

Defence Committee

Oral evidence: Domestic Threat of Drones, HC 180

Tuesday 29 October 2019

Ordered by the House of Commons to be published on 29 October 2019.

[Watch the meeting](#)

Members present: Dr Julian Lewis (Chair); Martin Docherty-Hughes; Mr Mark Francois; Mrs Madeleine Moon; Gavin Robinson; John Spellar.

Questions 204-311

Witnesses

[I](#): Gavin Wishart, Chair, Association of Remotely Piloted Aircraft Systems (ARPAS-UK), Professor Iain Gray, Director of Aerospace, Cranfield University, Tony Burnell, CEO, METIS Aerospace Ltd, and Paul Everitt, CEO, ADS.

[II](#): Giles York, Chief Constable, Sussex Police.

Written evidence from witnesses:

[Paul Everitt, CEO, ADS](#)

Examination of witnesses

Witnesses: Gavin Wishart, Professor Iain Gray, Tony Burnell, and Paul Everitt.

Q204 **Chair:** Good afternoon, and welcome to this session on the domestic threat from drones. This is an ongoing inquiry by the Committee. We are lucky to have four experts in this field on the first panel. Please introduce yourselves for the record, starting with Paul.

Paul Everitt: My name is Paul Everitt. I am the chief executive of ADS, which is the UK's national trade association for aerospace, defence, security and space.

Tony Burnell: My name is Tony Burnell. I am the CEO of METIS Aerospace. We develop both counter-drone solutions and new drone technologies. I am also the chair of the ADS drone platform and counter-drone group.

Gavin Wishart: I am Gavin Wishart. I am the chairman of ARPAS-UK. We ostensibly represent drone operators, but it is merging into the whole sector. I am a commercial drone pilot, and I am also an engineer.

Professor Gray: Good afternoon. I am Iain Gray. I am the director of aerospace at Cranfield University, but I am here today in my capacity as chair of the BEIS-sponsored Drone Industry Action Group.

Q205 **Chair:** What does that group do?

Professor Gray: The Drone Industry Action Group was established back in 2016 with the purpose of promoting, supporting and facilitating the commercial exploitation of drones for the economic benefit of the UK.

Chair: Thank you very much.

Q206 **Mr Francois:** We are tight for time, as there may be a Division, so I will not drone on. Professor Gray, how is the drone industry supporting the UK Government to assess the threat and risk of individuals using drones for malicious purposes in the United Kingdom?

Professor Gray: First, from a drone point of view, there are huge economic benefits to drone commercialisation in the UK. In identifying threats, we need a balanced approach, in terms of the risks identified with threats versus the significant commercial opportunities. I like the phrase in the recent Home Office report—the three Ds, which is about deter, detect and disrupt. In terms of deterrence, the UK Government have the drone code and the publication of documents, and registration technology such as electronic conspicuity is a good thing.

In terms of detecting, there have been significant advances in technology, such as sensors and equipment to identify drones. We need to contextualise the differences between rogue drones versus drones which have inadvertently got themselves into a difficult position versus the vast



HOUSE OF COMMONS

majority of drones, which are actually being used in a good and sensible way.

In terms of the last D—the disrupt—there are other people on the panel better able to answer that. Over the last 12 to 18 months, we have seen huge technology advancements in terms of disruption and anti-drone technologies. The key thing is how we keep the anti-drone technology moving at pace alongside the actual development in drone technology for good.

Q207 Mr Francois: Clearly, this Committee is most concerned with the security and defence aspects of drones, as you would expect, but in the interests of balance, could you give us some examples of the positive aspects of drones and how they are improving the lives of our constituents?

Professor Gray: There are some fantastic opportunities. We are familiar with the domestic opportunities around filming and things like that. What the public is not so familiar with are the opportunities around surveillance. There are offshore oil and renewable energy inspections in harsh environments. Drones are now regularly flying out and inspecting those bits of structure, keeping energy flowing.

Q208 Mr Francois: Can they do that in all weathers?

Professor Gray: Not in all weathers. That is one of the technology advances that we need to make. But offshore from Aberdeen—
[*Interruption.*]

Chair: There we go.

Mr Francois: We did try.

Chair: We believe there will be two votes. If there is only one, we will resume in 15 minutes; otherwise we will probably resume around the 25 or 30 minute mark. I am sorry about this. The session is suspended for the moment.

Sitting suspended for a Division in the House.

On resuming—

Q209 Mr Francois: When the bell rang, we were asking whether in the interests of balance you could give some positive examples of drones. You mentioned the monitoring of offshore energy facilities as one example. Can you think of any others?

Professor Gray: There are some great examples with search and rescue, over sea and over the mountains, of people's lives being saved through the use of drones. There are undoubtedly great things such as traffic surveillance and analysis of accident situations. On a daily basis, there are some really good stories.

There are also things from a public point of view, like the Notre Dame cathedral fire. If it were not for drones, the cathedral would be completely burned out and gone. There are also examples in the UK where drones



HOUSE OF COMMONS

have been used in emergency situations to save lives, real estate and properties. From my perspective, every day a really good drone story comes out.

Q210 Mr Francois: If I were to summarise what you have said, at the risk of putting words in your mouth, I think you are saying that when you need an eye in the sky in a hurry for the public good, a drone can be quite a useful thing.

Professor Gray: I think drones can be a really useful thing in that sense, and other commercial opportunities are being developed. The question was about what is happening now, but if you look to the future, there are lots of good applications moving forward.

Q211 Mr Francois: Thank you. Mr Wishart, can industry prevent recreational and commercial drones from being modified for malicious purposes?

Gavin Wishart: I am not a drone manufacturer, and I would not purport to be.

Mr Francois: But it tells me here to ask you that.

Professor Gray: That's good! Thank you for that.

The holy grail for anybody developing systems is that the system can be utilised for as many applications as possible, so if you are developing commercial systems, we would want people to take open architecture so that we can design and develop the drones into the future. There are obviously some safeguards that can be put in place to stop inadvertent—if not malicious—users. We have things like geofencing, where you can set areas that your drone will not fly into, and conspicuity, where you can tell other air users that you are in the environment so that you avoid air-to-air collisions and so on.

In line with any form of integration, it is important to have open architectures. Of course, that allows malicious users to use it, but you would not change the way you design computers based on the misuse of computers.

Q212 Martin Docherty-Hughes: Gavin, in your answer to Mark you mentioned malicious drones. Say someone makes a drone at home. How effective are the exclusion zones or restricted zones that are utilised around the national infrastructure for malicious home-made drones? I raise that point because we have already had one evidence session in which I questioned manufacturers. To take a very simple example, when I was taking my dogs for a walk into Ayrshire—

Gavin Wishart: It's a very nice place.

Martin Docherty-Hughes: It is indeed.

Gavin Wishart: It's my home.

Martin Docherty-Hughes: Your accent gave it away.



HOUSE OF COMMONS

I took my dogs down to Portencross, very close to Hunterston B power station, and somebody was using a drone 100 yards from the power station. How effective is that restricted zone?

Gavin Wishart: Clearly it was ineffective in that case. The capabilities of drones, like most things in life, are proportional to price. The more capable drones—the ones that fall across the amateur/commercial divide—have the sort of systems that have geofencing, so you would not be allowed to fly in those areas. I would not suggest that home-made drones are less effective than commercial drones, but normally they are quite small, they have low range, and because they are small they have little kinetic energy. Yes, the drone may have been doing something that it should not have, but what is the assessment of the risk of a 250g drone flying close to an area where it should not be flying?

Martin Docherty-Hughes: Thank you.

Q213 **Chair:** I invite anyone with a view on this point to come in. I raised it in a previous session as well.

In the days when I used to search for obscure documents in the National Archives at Kew, I used to see the airliners coming in to land—you almost felt that you could reach up and touch them. We all know that the greatest threat from the advent of drones in private hands is the thought that—either through malice or through incompetence and reckless irresponsibility—somebody could fly a substantial piece of kit, and it could get sucked into the engine intake of an airliner. Hundreds of people could be killed on the ground and in the aircraft. My question is why we have to wait for that to happen before the country decides that it needs to license these contraptions and put penalties into being to prevent unlicensed private individuals from having them. I think it is a fairly safe bet that if one or two disasters of that type happened, the pressure to bring in a regime of that sort would become irresistible.

Who would like to volunteer to discuss that scenario?

Paul Everitt: Should I volunteer, Julian? From an industry point of view, we are looking at striking an appropriate balance. I agree absolutely with what Iain has said. There is huge potential good from the use of drones and autonomous technology. However, there are some risks as well. We are in a moment when the Government, the state, are responding to the assessment of risk and putting in place measures that begin to address the risks that are there. In the Government's recently published drone strategy, enhanced registration is a key element, as are additional powers for the police and closer working with industry to understand the development of drone technology and what measures we can put in place to ensure that the manufacturers are including standards that make both accidental and malicious use much more difficult, but also that we have in place the technologies that allow us effectively to detect, track, identify and, if necessary, disrupt drones that we believe may be, deliberately or maliciously, in inappropriate places.



HOUSE OF COMMONS

We recognise that there is a threat from what has become, relatively quickly, a quite ubiquitous technology. It is clearly much more available today than it was five or 10 years ago. I think we are beginning to get an appropriate response from Government.

Q214 Chair: But in the scenario that I have outlined, the only way in which such an attack could be thwarted is some sort of system on the aircraft itself that could repel a drone being flown into one of its engine intakes, for example. I am not aware that such a system is in existence, so I come back to my scenario. Can you imagine what the demand from the public would be if an aircraft were brought down over a residential area on one or, at most, two occasions? I think they would absolutely demand that these contraptions should not be in private hands unless licensed in a system similar to that in which people who are .22 rifle target enthusiasts have to get a licence.

Paul Everitt: Colleagues may wish to add their comments, but since the unfortunate events at Gatwick last year, we have seen the uptake of detection, tracking and identification activities to identify more clearly whether there is drone activity in the vicinity of an airport. And obviously we have extended the area within which a drone is not allowed. So steps are being taken to ensure that, at the very least, we are able to identify whether there is something inappropriate in the vicinity of an airliner. It is very unlikely that an airport would be completely blindsided in this type of situation.

Q215 Chair: I will not press it more than this one last time, but the scenario that I am talking about is not in the immediate environment of an airport. It's in a suburb where the aircraft is coming in at a pretty low altitude, and I would have thought—please correct me if I am wrong—that it was well within the reach of a drone if someone were so minded. I fail to see how any sort of air control system, if someone were sitting in a back garden of such a suburb and about to launch a drone with that dreadful purpose in mind, could impede that. That is why I am putting the case, if only as devil's advocate, for a regime that ensures that people with ill intent would find it difficult to get their hands on the device that could cause such a disaster. Tony, would you like to have a go?

Tony Burnell: Yes, I would like to answer that one. First of all, we have to balance the risk and threat with the likelihood of the sort of disaster that you are suggesting. Drones that can get up to the operating altitudes of airliners on an approach path, or in a hold, tend to be the more expensive commercial drones, which are in the region of £10,000 to £15,000, and up to £60,000. They are not usually within the pocket of somebody who is just trying to fly one in the back garden; they are more commercially available drones, so that would be unusual.

The industry has been looking at the problem for a while. Certainly, for the military requirements we have been getting an understanding of that. Industry has been independently developing systems that would support such a requirement. Gatwick is a catalyst. It has made everybody sit up and understand what the risk might be if something were to happen. We

have therefore been looking for a cohesive approach. The strategy that was mentioned earlier, released by the Home Office, is hopefully going to bring that cohesive approach forward to drive industry in that understanding, and industry is very keen to respond and to develop the systems that would be required.

We cannot have a sledgehammer to crack a nut. In other words, you don't want very high-end, £10 million to £15 million systems in an airport. You have to justify it against that risk. We have that understanding and strategy, along with the multi-Government agencies that will feed that back to industry. Suitable systems can be selected. They can be tested, and assurance given to the operators that use them that those systems are capable of doing the job. It is a process that we are going through, which is now accelerated with the requirements from the fall-out from Gatwick and your particular scenario. Obviously, there are other scenarios where counter-drone solutions may be required, such as nuclear power sites and prisons. Again, you have to find the right, effective solution for that risk; to cover off the threat.

Q216 Chair: Is there any practical objection if the Government decided that they wanted to introduce a system of licensing analogous to that for people who have to apply for a licence via the police for target shooting rifles? Is there any reason to believe that such a system would be impracticable? I anticipate people talking about the age of the internet, ordering things from abroad, and constructing things oneself. Also, there should presumably be a de minimis rule to say that it would only be for contraptions over a certain size and volume. Gavin, I see you straining at the leash.

Gavin Wishart: I like the word "contraptions". In terms of licensing, we already license. People who are commercial operators have what we call permissions for commercial operations from the CAA. Obviously, to get to that stage the individual has to go to ground school, so that he understands how drones operate. Met and all the other bits and pieces come together. They do an assessment at the ground school, as you would if you were going to be a commercial airline pilot. They do practical flight assessment to show that they are competent to fly their drone, and then they apply to the CAA for permissions.

We are not against licensing at all, but how effective a tool is it to stop people doing things? Guns are under licence, but we know that there are an awful lot of guns. You can 3D-print a gun, I believe. I don't know—I wouldn't try it myself. We are controlling drugs. That is not quite licensing, but it's the same sort of thing; some drugs are licensed and some are not. It does not stop people getting their hands on them.

Q217 Chair: But we still think it worth having the system, don't we?

Gavin Wishart: How effective is it? That is what I am asking.

Q218 Chair: Are you saying that we, for example, should do away with the system of licensing guns?

Gavin Wishart: No, I think what you need to do is have a proportionate approach to how you introduce legislation, and make sure that whatever you are doing to stop the malicious actor does not have a detrimental effect on the commercial operators.

Paul Everitt: We have a form of licensing for commercial operators and for larger drones, as has been said. The strategy that the Government have introduced is creating a registration system for, as I understand it, most drones. You begin to put in place a structure that allows the Government and authorities to identify the legitimate users and, therefore, narrows the target that we as an industry are working on from a counter-drone perspective, so that we can more easily identify things that do not comply with the regulation that has been created. Rather than trying to protect ourselves against the whole of the drone community, we are trying to focus on physical areas and numbers that are more manageable, in terms of the risks we face and the scope of operations we need to put in place, to ensure that some of our critical national infrastructure is appropriately protected.

Chair: Martin?

Martin Docherty-Hughes: I will come in on a later question.

Q219 **Chair:** Okay. Moving on fairly quickly in the light of your answers, how would you rate the Government's efforts so far to address the domestic threat from drones? Do you think it is proportionate, and effective as far as it goes? Who would like to have a go at that?

Professor Gray: I will give it the first go. In the past 12 to 18 months, the issue of reports through the Home Office and DfT has seen significant steps in terms of the Government putting systems in place. What continues to need to happen, however, is a much more joined-up approach across different Government Departments. MoD, DfT and the Home Office all have respective interests in this. What is absolutely paramount in terms of making sure we have a good, consistent approach is that there is good join-up between different Government Departments.

Paul Everitt: I think we have made a good start. The key for us is about ensuring that we continue to make appropriate progress. There are some areas for us that are still challenges. One is the legal framework in which we are operating, particularly where we are looking to counter drones. In the context of the Air Navigation Order 2016, drones are aircraft, so only limited action can be taken against them. Also, the Wireless Telegraphy Act means that some of the technology we might deploy to disrupt drones is currently only deliverable by the police or by the military acting in support of civilian activity. That legal framework still needs to be looked at to ensure that it is fit for purpose and to see whether it is suitable, depending on the scope of the national infrastructure that we are looking to protect.

We have been talking about airports, but, as Tony said, there is a range of other locations. Clearly, it may not be possible for the police or the



HOUSE OF COMMONS

military to be available to take disruptive action at each and every one of those at all times of the day, so we may need to look at some flexibility around that, to provide the right legal framework for qualified private sector operators, where that is deemed to be appropriate.

There is also a challenge for us in terms of testing and validating our drone and counter-drone technology. Ofcom are quite restrictive in what you can and cannot do, and most of what we would need to do to test some of our technology is ruled out of bounds by Ofcom, so there are relatively few, if any, places where we can test and validate equipment and potential threats from drones and drone technology. Those are areas where we think we can do more more quickly.

At the moment—this reflects a bit of the question Mark asked earlier—we have a regular dialogue with the Centre for the Protection of National Infrastructure, the Home Office, the office for serious crime and counter-terrorism, and the police around a range of threats, including drones, but we do not have a structured mechanism that allows industry and Government to work together, on the one side sharing the technology developments that might go into new drones and, on the other side, sharing their understanding of what they are seeing in terms of malicious actions or actors, which might help us to either build appropriate measures into our equipment or to ensure that we have the right countermeasures available.

Chair: Any other contributions on that?

Gavin Wishart: It depends on your definition of effective. I have a feeling that a drone is, by its very nature, quite an asymmetric threat. It is small, it is pervasive, it can be cheap and it has a low signature for many sorts of detection. That comes back to my earlier point about proportionality. What risk are you trying to prepare yourself against? Whatever the technology that these gentleman here can come up with—there are a lot of things in the pipeline—you can spend an awful lot of money on an awful lot of systems, but you would not be able to say that you have effectively, 100% stopped the drone threat. Proportionality is what is required.

Q220 **Chair:** Before I bring in Iain, I note that the department store chain John Lewis has recently decided to stop selling drones, in part due to fears over their misuse. Is there a case to be made for banning hobbyist drones entirely?

Professor Gray: I want to make a point in answer to the previous question. We have talked a lot about technology solutions. From a governmental point of view, one key thing is around establishing proper communication protocols in the event of incidents. That, again, is about working across Government.

To answer the question about John Lewis, it is a favourite store of mine and I would definitely go there if I was looking for a washing machine, a bed, a television or something like that. I cannot speak on behalf of John Lewis, but I am quite sure that, while the Gatwick incident may have



HOUSE OF COMMONS

prompted a discussion around this issue, the decision they made was based around their overall product portfolio. I am not 100% convinced that you cannot still buy drones from John Lewis online, as opposed to in-store. I cannot go to John Lewis to buy a model plane or railway or things like that. For me, it is not too much of a surprise that John Lewis have reviewed their product portfolio based on their business requirements. To not have drones in-store is a decision they have chosen to make for business reasons, in my view.

Q221 Chair: Does anybody think that there is a case for saying that hobbyists should either be excluded or, as we discussed earlier, licensed before they can acquire these devices?

Gavin Wishart: Once again, I am happy with the proportionate amount of licensing that is required to make sure that people fly safely. However, the—

Q222 Chair: It is also a question of flying responsibly. At the lowest level of this—I do not mean in altitude terms—you perhaps have people using cameras on drones to spy on their neighbours or to cause major nuisances to other people.

Gavin Wishart: That is an offence.

Q223 Chair: Right. So we are bringing in a whole new capability—a whole new dimension, really—of people being able to cause considerable distress to other people. Do we really want this to be on a completely commercially anarchic basis, or do we feel that the risk is significant enough to have a regulatory regime?

Tony Burnell: I think we have to balance this. When the motor car came out, we had to have somebody walking along in front of it with a flag for fear of running people over. People still get run over today. We did not ban the motor car, despite us sitting here and saying how much pollution it causes. We always find reasons why we should not have combustion engines—

Q224 Chair: Although drivers have to pass a test and get a licence for the motorcar.

Tony Burnell: We do.

Chair: So not your best analogy, if I may say so, Tony.

Tony Burnell: The strategies we have at the moment are out there to educate users of the drones and to have a basic type of training, so that when people get a drone, they have to go online to log on and understand where they can and cannot fly drones. I go around a lot of facilities, and where there is a risk that flying drones would be a criminal offence, there are a lot of signs up. You also find that around a lot of prisons. We are educating for that.

Some of it comes down to education. We have to understand that drones have a lot of good uses and that there are a lot of advantages for us, so



HOUSE OF COMMONS

we do not want to stifle the development. Some of those developments are coming from our 10-year-olds getting a drone to fly in the back garden. It is a great technology. They will then take that and develop themselves into new technologies for the future. We just have to understand the threat and that is probably the 0.5% who have a malicious drive to do something illegal—something they should not be doing. Therefore, we just have to ensure that we have the technology that protects the rest of us if that happens. We have to balance that threat.

Q225 John Spellar: Can I direct this one to Paul? What is the scale and make-up of the counter-UAV sector in the UK? How does that feature in international comparisons?

Paul Everitt: It would be fair to say that the counter-drone marketplace is emerging and developing quite rapidly. The UK is very well positioned. If I reflect back probably a couple of years ago, it would be quite—I say this in the nicest way—niche capabilities: relatively small businesses with niche capabilities in particular areas, which were half-seeing an opportunity and developing product. Over the last couple of years that has developed and we are now seeing some of the larger and major players in our sector—QinetiQ, Leonardo and others—bringing together a range of technologies to provide a more rounded solution for the customer. so not just a specific technology for disrupting a drone but a whole solution that allows you to detect, track, identify and ultimately deter.

Q226 John Spellar: Deter or eliminate or immobilise?

Paul Everitt: All those options, I believe, are available.

Tony Burnell: Sorry, I missed that question.

Paul Everitt: I think the first question was more about how the market has developed and where the UK sits from a competitive point of view.

Tony Burnell: The last five or six years' development was very much experimental, with a number of companies that got involved. About three years ago, a lot of companies saw a need for counter-drone so there was a rapid expansion of companies offering counter-drone capabilities. Following on from that and from Gatwick and with CPNI now carrying out testing, we are seeing what I would say are solid capabilities now starting to come to the fore for offering.

To understand the capabilities, as Paul said, there is not one specific system or one capability that solves the problem. It has to be a multi-layered approach. For instance, you may use an RF sensor that will detect 80% of the drones and you may have a radar that will, again, detect 80% of the drones. Putting them together, they will detect about 92% of the drones. Electro-optics in cameras will increase that again.

You look at your risk and what is acceptable for you. You also look at your costing, because these systems will be anything from a commercially-based system that is off the shelf to a military-specified system. Your



HOUSE OF COMMONS

purchase could be anything from £50,000 to £2 million to £3 million per system. You have to balance that.

Paul Everitt: What we see in the international market is that the UK is doing reasonably well. Many companies are finding international buyers, be those Governments or airports in other countries, which are more proactive in determining what they want and are prepared to invest in it. In the UK, up until relatively recently, there was a—I wouldn't say reluctance, but it was relatively slow to get purchasers or customers to identify what they did want and to take the decision to put something in place.

Q227 **John Spellar:** That clearly is a role for Government or the CAA to provide a bit of drive. Ultimately, it ends up being Government. Shouldn't Governments be getting together the various establishments that could be considered vulnerable and the various industries, driving towards a common view and doing that in conjunction with industry in order to build British industry for our own requirements, but equally significant, in order to establish a strong presence internationally?

Paul Everitt: Yes. Again, the strategy that has been published is steps along that journey. The Centre for the Protection of National Infrastructure—we call it a piece of MI5—provides advice to the owners of national infrastructure about the technology that is available to address their broader security concerns. They are now doing work with industry, both to identify and test—

Q228 **John Spellar:** Is there sufficient drive and energy in this? What you are describing seems to me largely like a traditional procurement. Is it not actually that there is an urgent operational requirement here?

Tony Burnell: For quite some time, industry has been looking for that cohesive approach. Within the last 12 months there has been a much better drive from Government to start looking at what industry has. Until 12 months ago, they were very much looking at what the threat was with a drone and then looking to see if industry was going to counter that threat. By the time that had been tested and analysed, the threat had changed. Therefore, in Government quarters, there would always appear to be the reluctance to buy a solution here and then, to see where the new counter-drone technology was going to counter that new threat.

Looking forward, with this new strategy that has been pushed out—and hopefully it is going to be decisive—what we need to do is have defined requirements for industry so that industry can drive and provide a solution now that can be bought, tried and used, not to wait for it to catch up with where the next threat might come from. We need to have evergreening in the technology and the move forward. There is a risk that the technology you buy today will be obsolete in six months' time because a new technology comes out that we have to counter. You cannot change that risk.

Q229 **John Spellar:** My final question then, is to ask which entity or which Department should be providing this driving force?



HOUSE OF COMMONS

Tony Burnell: I don't think it is for me to state which Department it should be, but it needs to be a single Department. At the moment a number of Departments have their own areas of responsibility. For instance, CPNI does the testing and the technical requirements of it. JSaRC deals with the industry facing and the Home Office has come up with a strategy to lead on it—

Q230 **John Spellar:** But everybody's problem is nobody's problem.

Paul Everitt: It is a national security issue, but it is appropriate for the Home Office, given the spread and scope, to be the home for the co-ordination and direction of this issue.

Q231 **John Spellar:** That answer fills me with trepidation. Let us move on.

Tony Burnell: Can I just add one thing? Recently the RAF announced a project, which is going to be an evergreening project, through the UAS CDC, which is going to be the technical body looking at solutions that are readily available and will fit the bill for UORs, as you put it. They have taken the risk to buy, to then develop and look at other solutions, do a comparison and move their game forward. I think that sort of model is probably a good model that would work very well for the Government and civilian requirements.

Q232 **John Spellar:** Are a number of providers within this industry jumping on a bandwagon, proffering solutions that are not really effective? In other words, is a system of proper accreditation needed—I do not mean going over years, but a sort of rapid accreditation—and therefore the development and implementation, again rapidly, of industry standards?

Tony Burnell: Yes. As I mentioned, CPNI is carrying out testing and calls are already running for those and equipment is being tested, so to they get a baseline standard of what capabilities the systems can do. That will then go into a security catalogue, which those that have requirements for it can read and see what is approved and what the performance in the system was. The Air Force is doing the same thing with its programme through the UAS CDC. They will look to ensure that when somebody puts a call forward, the equipment that is proposed actually has the certifications it says it has. It will be up to the Air Force, which does its own trials, to test its performance, but before it gets to that point, it knows that the system has the environmental certifications and does what it says on the tin prior to that stage.

You are right that there are probably quite a few—I don't have a percentage—snake oil salesman out there, who will sell you the widget that will solve your problem. They come and go in time, but with the right processes and the right agencies doing the work, we can ensure that those will not get through and the systems that do what the end user needs will be selected.

John Spellar: Thank you.

Q233 **Martin Docherty-Hughes:** How does existing regulation limit the use of unmanned aerial vehicle technology? Are there any exceptions, and



HOUSE OF COMMONS

should there be more?

Professor Gray: I am not sure exactly that I understand the question.

Martin Docherty-Hughes: In term of countering UAV technology. For example, if you are Hunterston B nuclear power station and you are looking to counter unmanned aerial vehicles, how good is the existing legislation around that?

Paul Everitt: There are restrictions.

Martin Docherty-Hughes: There is a difference, I think, between legislative restriction and an act of effective implementation of the legislation.

Paul Everitt: Okay. I will pitch out and we'll see if I have answered your question. Because a drone is classed as an aircraft, you cannot just take it out of the air; only certain people can take it out of the air and only when there is risk to life. That is a legislative restriction that limits your power station's ability—

Q234 **Martin Docherty-Hughes:** Forgive me for intervening. I can see Iain's perplexed look and I may come back to him in a second. In the Gatwick incident, if you are Gatwick airport and you want to counter unmanned vehicles, does the existing legislation limit your ability to do that?

Paul Everitt: Yes. What they can do and are doing is detect, track and identify something in their airspace, but they cannot remove it or disrupt it themselves; only the police or the military working in a civilian context can do that.

Q235 **Martin Docherty-Hughes:** Are you on the panel quite happy with that existing legislation?

Paul Everitt: I think we have said that there are some challenges around that. The other part that goes alongside that, which I referred to earlier, is the Wireless Telegraphy Act. Some of the technologies that we would use to disrupt a drone are RF or GPS-blocking signals that are not exactly the same but are similar to the sorts of things that might be used to monitor your telephone or intercept your telephone calls and that kind of stuff. Again, only certain people in certain circumstances are allowed to do that. Therefore, we can identify it and track it, but only certain people can take action against it.

Martin Docherty-Hughes: Iain, do you want to come back in?

Professor Gray: It comes back to the balance of risk and threat. On whether we have got everything right, we have just seen in the last couple of weeks the Home Office report; there are some recommendations in there that are still to be implemented. We saw the Science and Technology Committee report earlier in the year; there are some recommendations in there still to be implemented. We have the upcoming aviation strategy report, which I am sure will have some recommendations. De facto, have



we got everything in place now? No, we need to implement some of those recommendations.

In terms of getting the right balance of risk and threat, the Chair proposed one scenario and asked some questions about it. It is about understanding the risks against an evolving technology scenario, and having a dynamic process to allow us to understand those risks and threats. I believe the recommendations in the reports I cited are good recommendations and should be implemented.

Q236 Martin Docherty-Hughes: That is what I heard earlier, in terms of the benefits of drones. As a Scottish constituency MP, I have noticed recently that NHS Scotland are doing their first pilots for the delivery of medicines in the Western Isles and the islands of the NHS Highland structure. Na h-Eileanan an Iar is doing deliveries, as well as Highland piloting them—I definitely get that. What I want to go on to is, how effective are the counter-drone capabilities of critical national infrastructure companies—this is a long question—and are they legally compliant? I would also put national infrastructure bodies in there. For example, in Scotland water is not private; it is owned by the state. So there is a range of national infrastructure in both the private and public spheres. How effective are counter-drone capabilities, and are they legally compliant?

Tony Burnell: A number of very, very effective capabilities are available on the market and have been implemented when needed. For example, some of those capabilities were deployed at Gatwick. For a very short period, they were given access so if the drone entered the Gatwick area they could be utilised.

There is still some understanding and education to come on both sides. Where these technologies have been used overseas, they have been used in military environments, and they work very effectively. We have to look at the policies and procedures in the UK, and we need to move those forward quite rapidly to allow legislation for these technologies to be used.

The industry also needs a proving ground to try these out. We need access to test ranges to take these counter-drone technologies on, fly drones, prove their capability and look at the effect they have. For instance, one of the systems is RF jamming. At the moment, the capability is out there—we jam the whole band, across 2.4, that drones operate on. When they do that, they jam all the other frequencies that operate on there as well, so you are losing Bluetooth, your wi-fi connections and maybe other data, so you have to have an understanding of what they do. In the future, there will be new technologies that are able to carry out surgical jamming, but again we have the question, “Okay, we jam the drone. What is the legality under the Air Navigation Order, now that we are affecting a platform?” We have to have that legality in there.

Professor Gray: I think it is about that balance of risk and threat. By the way, I love the example of health deliveries in the Scottish islands. That is a really good example of drones used for good.



HOUSE OF COMMONS

In terms of getting the balance of risk and threat, the conversation starts to focus on not just the rogue drone operator but somebody who has real malicious intent to do something. In the balance of risk and threat, you have to ask yourself whether the drone is actually the device—the solution—that somebody would choose to use if they had real malicious intent.

Q237 Martin Docherty-Hughes: In terms of malicious intent, everyone keeps talking about the Gatwick incident—I will talk about that more in a wee bit—but if there was malicious intent at Gatwick, would the drones that were used have had any impact on aircraft at all? I see some shaking heads in the back.

Professor Gray: I think that investigation has closed, from what I understand, without any significant conclusions.

Gavin Wishart: The point you make—

Q238 Martin Docherty-Hughes: The reason I ask—forgive me, Gavin, for coming in—is that, where some people talk about the Gatwick incident, I have what we call the Clydebank incident. I don't know if many of you know Glasgow Airport very well. It sits to the south of the River Clyde, and it is not in Glasgow; it is in Renfrewshire. Its northern take-off zone goes across my constituency at a very low level—in fact, the other month, we had a vortex over the community of Whitecrock, and Glasgow Airport has had to pay for roof repairs on houses in my constituency. I have had two incidents with drones. I do not think they are malicious in any shape or form. Somebody has got a drone for Christmas, probably from John Lewis—there are other providers available—

Gavin Wishart: Not now.

Martin Docherty-Hughes: Not now, unless it is online. With someone at a very low level—this is not Heathrow or Gatwick—across a high conurbation in the greater Glasgow area, and I am talking maybe 400 feet from the roof of someone's house in a community of 50,000 people, what kind of problems should we be thinking about in terms of trying to block or limit use in those areas? I don't hear anyone talking about the Clydebank incident, even though this has happened twice, in two consecutive years, but it happens once at Gatwick and the whole world pays attention. My community are left thinking, "Well, what happened to us?"

Paul Everitt: Part of the challenge here, certainly for us in responding, is that I am not sure that there is a source of advice from Government to airports or other positions of critical national infrastructure on what their approach to assessing risk should be, or what mechanisms they should put in place to protect themselves.

Q239 Martin Docherty-Hughes: From your expertise, what happens if a plane is at 400 feet above a huge conurbation, landing, and a drone hits it?

Professor Gray: I think, from a speculative point of view, you are conceiving a scenario. The industry and the aircraft manufacturers themselves look at all sorts of different scenarios in aircraft design, such



HOUSE OF COMMONS

as bird strike or other kinds of failure scenario. The manufacturers of large civil aircraft are certainly looking at, and are live to looking at, these kinds of scenarios. From an airport point of view and given the kind of legislation that we have just talked about—the 5 km exclusion zones, the registration of drone users—the fact that it is a criminal offence is designed to deter and to make sure that those incidents do not happen. It is the most safety-conscious industry there is, in my view. In terms of people exploring those scenarios, they are looking at ways in which we can mitigate against them as best we can. There are no two ways about it, this industry, whether it be the aircraft manufacturers, the airport operators or the aviation sector, takes safety extremely seriously. They would overlook no steps with a view to ensuring overall safety.

Q240 Martin Docherty-Hughes: Finally, are some critical national infrastructure sectors better prepared than others?

Tony Burnell: From my perspective, a number of sectors have looked at the issue with drones. In prisons, for instance, it has been quite high profile, and work has gone on in that area. I cannot answer as to where the Ministry of Justice is in its process at the moment, and it would not be for me to comment in this forum on some of the things in my knowledge, but work is going forward.

A number of sectors are looking for the Government to provide the education for them, so they can understand what they need to mitigate their risk. That is going forward. With this strategy, it is very important that it is not one that we spend the next 12 or 18 months putting together and understanding; we need to be looking at moving it forward in three or four months, to gain understanding, and then industry can help to support it—it can have industry behind it. We know that about 11 or 12 CNI areas could have a drone risk, and that needs to be supported.

Professor Gray: Last week, I had the good fortune to spend some time in Singapore at an international transport systems congress. Singapore is a country that has recognised the economic value of drones. It is a country that has got its own legislative procedures. The good news for us is that many UK companies are out there trying to get economic benefit for themselves and this country by putting things in place over there. I got the distinct impression over there that the UK is well placed in terms of its understanding of the technologies and what we need to do. The UK is providing the advice and industrial business support to countries like Singapore. It has the right approach to that risk and threat.

Gavin Wishart: When you are commercial drone buyers, whatever you are doing, you look at risk as two elements: probability and severity. I do not know what the probability is of a drone being on the threshold of a runway, but you could probably do some research to find out what that might be, taking into account the efforts we are making to reduce that threat.

The second point is about the severity. Iain makes a good point that the airworthiness of aeroplanes has been the lifeblood of this country and



others, making airlines and flying as safe as possible. Aeroplanes are designed to take birds. Unfortunately, birds sometimes bring aeroplanes down on an international basis. We do not hear about that quite so often, but it happens. Equally, engines are designed to take catastrophic failures without throwing turbine blades and affecting the passengers.

Personally, I would like to see some real research into this that we could all get behind. There has been some research, but where it came from and who did it is questionable. I would like to see some real research done so that we can understand it. There are things that the drone industry can do to help. In the research that has been done, there was some discussion about the impact of the motors on an aircraft's perspex displays. Obviously, an aeroplane on the approach is going quite slowly because it is going to land, so it is not at its highest velocity, and the kinetic energy of the impact would be less. However, drone manufacturers should understand that putting a shroud around the engines may actually improve its impact potential.

I fly a small 2-metre drone that is made of plastic. With the downwash of an aeroplane, it would not get anywhere near an aeroplane—or a helicopter. I would like to see some really good research into this, so that we understand what the risks are and can try to design to reduce those risks.

Martin Docherty-Hughes: Thank you.

Q241 **Mrs Moon:** Gentlemen, I get the impression from listening to you that the evolution of drones is moving fast, but the counter-drone technology is moving at a snail's pace. How great is the gap?

Tony Burnell: Actually, I cannot agree with you on that. From the industry perspective, many industries are working very fast and are actually looking at what the next threat is. For example, this morning I was looking at the 5G technology, and I had a meeting with a company about where they thought they were going to go in developing the technology for drones and looking at how to counter malicious or rogue drones that may occur with that technology. So that is being thought of.

I mentioned earlier that the industry is really keen to get defined requirements from the Government on where they want to go. I mentioned that we are looking at evergreening. We will never catch up and get ahead. We will try to get ahead of what the threat will be, but it is very much like explosive ordnance devices: you are always trying to be ahead and to counter the threat. We learn from that. Many of the companies that worked in RF jamming with EOD are looking at counter-IED, have very good capabilities and are spending a lot on research and development to get ahead and to be able to offer the best solution out there for counter-drone.

It is important that we stay ahead of the game. It is a partnership between Government and industry to do that. It should not be for industry to try to second-guess what the threat will be. Industry struggles at times



HOUSE OF COMMONS

to get the leadership that it needs on the direction it should go in, so it is second-guessing—that is important. I hope that that will come out of the strategy and will happen.

Q242 **Mrs Moon:** So you are telling me that we do not have to worry, that we have the counter-drone technology to deal with the problem that Martin outlined and with Gatwick, and that it is on the market and operational today?

Tony Burnell: It is, yes.

Q243 **Mrs Moon:** So why is it not working? Martin has had two incidents.

Tony Burnell: I understand that drone detection, tracking and identification capabilities are working in Gatwick.

Mrs Moon: I was not talking about Gatwick.

Tony Burnell: Well, it is working.

Paul Everitt: It can only work where it is in play, and we are not responsible for decisions about putting in place those appropriate technologies either in airports or in other parts of critical national infrastructure. Things are available and, as Tony said, the Government's strategy hopefully provides us with the opportunity to rapidly develop and respond to emerging threats, but we will need our Government partners to be able to share that information with us so that we can adapt.

As Tony indicated, in other parts of some of the work we do, we have well-structured relationships and mechanisms for that information and intelligence sharing, and in the drone and counter-drone area, that is where we hope the strategy will provide us with the right kind of mechanisms so that we can respond swiftly.

Q244 **Mrs Moon:** So the counter-drone technology is in place—

Paul Everitt: Is available.

Q245 **Mrs Moon:** Right. It is available, but the problem is that the Government have not insisted that it needs to be in place to protect critical national infrastructure?

Paul Everitt: Yes. There is an open question about the advice that is being provided about what should be in scope—what facilities and at what level. Again, that is part of the debate and discussion about what the actual risks are. We are not suggesting that absolutely everybody needs absolutely the highest level of protection, but there needs to be a debate within Government and within that critical national infrastructure community about how they determine what is the appropriate level of protection and whether protection is required. Then we can work with them as a customer.

Q246 **Mrs Moon:** How far away do you think that is? How long before we have that? Does anyone have any ideas?



Tony Burnell: I am expecting that, within the next few months, CPNI will start reporting on the systems that they are recommending putting into their catalogue, and that will be in there, so that CNI sites can then purchase those systems. I would think that list will start coming out before Christmas. It is an ongoing evaluation for companies that will take place over the next two or three years, but as companies put their kit forward, it is being tested, and that will be available. It is then really down to the policy of the CNI sites to look at the risks and decide what they have and what they want to put in place. Budget will obviously be one of their concessions on what they can fit in. I expect that to be available.

Q247 **Mrs Moon:** Will that include things such as some of what I think they call built-in safety mechanisms—it seems a bit counterintuitive to call them that—such as collision avoidance, which could limit the effectiveness of counter-drone technology? Are you including that in your description of how prepared and how available the counter-drone technology is?

Tony Burnell: Sorry, I don't quite get—

Paul Everitt: I think Madeleine is saying, what if a drone has anti-collision or anti-avoidance technology within it and is therefore more agile and able to avoid some of the mechanisms that we might deploy?

Tony Burnell: In terms of the capability of the drones that we would be looking to defeat, which are the threats at the moment, the counter-drone systems out there, if we are looking at RF mitigation, will jam and stop all but the drone that has fully autonomous capability. If you have a drone that is fully autonomous, that is on a flightpath, that is not expecting to have a heartbeat with a controller—if it loses the heartbeat, it would have to stop or return back home or to a set destination—and that is not receiving any mid-flight guidance, you will need to look at a hard kill type of mitigation. There are some capabilities out there in different guises. There are net capture systems available out there, which I know are being tested as we speak. There are laser systems, although obviously the use of a laser system is much more questionable, and that has to be studied. In terms of the capability of those sorts of technologies, we are still six to 12 months away from a real understanding of those capabilities, but they are available in other countries.

Q248 **Mrs Moon:** I understand there are also birds of prey available, but there we go.

Paul Everitt: We would assume that systems of that level of sophistication are not the sort of things that would be being casually used—

Q249 **Mrs Moon:** On the general market.

Paul Everitt: Those are the kind of high-grade technologies that one would expect to be either very sophisticated players or state actors, as opposed to malicious people—people who are either casually or inadvertently creating a problem, or even those with a reasonably sophisticated approach. That is a different order of threat.



HOUSE OF COMMONS

Q250 Mrs Moon: To avoid the time lag, do the drone technology developers and the counter-drone technology developers talk to each other? Do they say, "Right, this is our new product. What can you do to bring it down?" Is that conversation taking place, or is it that it comes on the market and then you have to catch up?

Tony Burnell: The short answer, in the majority of cases, is yes. The counter-drone technology manufacturers and developers are talking to the drone technology developers to find out what they've got.

Q251 Mrs Moon: What about the use of swarms of drones? Is there technology available to deal with the issue of swarming that we have heard so much about?

Tony Burnell: Some technologies are available, yes. Again, you are looking at high-grade military systems that have the capability to look at swarms and then define a swarm. Is it 20 drones? Is it 100 drones? Where are we likely to see a swarm of 20 drones in the UK? It would be state actors, I suggest, that would be behind something like that. If we were going to the Middle East, there may be a high probability of that. If you look at the threat balance, it is not likely to be seen in the UK at this time.

Q252 Mrs Moon: What about the use of drone technology as a cyber-security attack weapon? Is that something that is feasible, and have we got mitigation measures against that?

Chair: For example, taking over radio and telephone communication masts and misdirecting messages and calls, which I believe is technology that is available.

Tony Burnell: They would be capable of carrying technology, but that technology is normally available only to agencies. If you were looking into that sort of technology—I will be careful in what I say here, because we are bordering some issues that may be sensitive—it is possible but highly unlikely. If you were looking at commercial espionage, that is possible. Commercial espionage can be done with a telescope out of a high building through another office window; a drone could be used for that. Again, that is a malicious use and is therefore against legislation—we have laws to stop that. If you want to counter that, you have to consider technologies that are out there and available with counter-drone technologies to be able to do it. I would not suggest that you would want to be attacking and jamming, but you would want to know if something has detection capabilities to say, "Yes, we have a drone in the area."

Q253 Mrs Moon: But we are the Defence Committee; we are not the Department of Culture, Media and Sport. We are not looking at hobby droning; we are talking about serious threat droning. Our concern is about the high-level technology, the new emerging technology and the new threat technologies. What we are looking for is your assurance that here in the UK we are on top of that, that we are aware of the threats, that we are developing the technologies to deal with those threats, and that—it might not be necessarily in the hands of the hobbyist—it is something that the military and security forces are dealing with.



HOUSE OF COMMONS

Tony Burnell: There are technologies available today to counter that threat.

Q254 **Chair:** How difficult would it be to import from another country some complex drone that has been adapted to be used in a malevolent way? Are our customs arrangements sufficiently well briefed and robust to monitor this?

Tony Burnell: We are probably the wrong panel to talk about the customs and security arrangements for that. What I can say is that there are components available on Chinese markets that allow you to modify drones in the UK and that may give you extended range capabilities and that sort of thing. But the capabilities that are available—actually, they are quite cheap—will be detected by the industry's systems, which will give you an element of countering.

Q255 **Mrs Moon:** One of the things that worries me about this is that, in terms of cyber-security, we learned very quickly that, sometimes, it could be the lone young person in their bedroom who could actually be one of the biggest threats against even the state and high-end, security conscious parts of the state. I cannot see that a young person who is interested in drones would not also keep themselves abreast of the latest drone technology and seek to achieve it themselves. That is my concern and, I think, the concern of this Committee.

That is why we are seeking the assurance that the technology is there to counter those drones that might not necessarily be in the hands of a foreign agency or state, but that might get into the hands of a keen hobbyist who could then be used by someone who wished to attack the state. Are you confident that that technology is there?

Tony Burnell: We have to be clear on one thing: nothing is 100% guaranteed in life. The counter-drone capabilities that are out there in the UK, made by industry, will tackle—I would put my Air Force pension on this—99.5% of the drones that are out there. There is still the 0.5% of drones that you do not know about and that you will be keeping up to understand.

I explained earlier that, with each technology that we have in the layered approach, you will probably cover about 80% of drones per technology. They will overlap to give you that higher 98% or 99% detection and the ability to mitigate them with what is available today. Can we get to that 100% with other technologies? In EOD—explosive ordnance devices—can we guarantee that we will always stop every bomb or know where it is? No, we can't. We have to balance that, but what is available today will cover most of what is out there in terms of commercial, off-the-shelf drones—even the modified ones.

Q256 **Martin Docherty-Hughes:** Following on from Madeleine's line of questioning, do you agree that the majority of commercial off-the-shelf drones sold in the United Kingdom are made in the People's Republic of China?

Gavin Wishart *indicated assent.*



HOUSE OF COMMONS

Martin Docherty-Hughes: Some nodding heads there. Like most pieces of technology that we use today—whether it be in a commercial or leisure process—those pieces of technology will require software updates on an irregular to regular basis, which would require those drones to be connected to a PC, a laptop or so on to download the recent updates to the programming.

Tony Burnell: Just the middle-of-the-range and high-end drones. Some of the cheaper off-the-shelf drones do not require an update. They are very basic.

Q257 **Martin Docherty-Hughes:** They might not require it, but they might be able to access it. They might have a USB port to connect to.

Tony Burnell: They are likely to have a port to connect to a camera.

Q258 **Martin Docherty-Hughes:** Most of them will have a USB port, and you might be able to access that. Given that most of those drones are built in the People's Republic of China, and given that the companies that make them are mostly registered Chinese companies, the point I am trying to make is that it is not just when they are in the sky that there might be a cyber issue; there is, basically, what some would call data-mining by the People's Republic of China of all the information that those drones have. That was not denied when a major manufacturer came to this Committee in the last evidence session. I must say that that manufacturer is based in the People's Republic of China.

Tony Burnell: I would say, on the technical side, that it is highly possible. Likewise, we probably all have something in our pocket that has the same risk.

Q259 **Martin Docherty-Hughes:** But most of those do not fly over national infrastructure on a regular basis.

Gavin Wishart: Neither do drones—come on, that is unfair. There are probably more telephones in your national infrastructure than there are drones.

Martin Docherty-Hughes: I am just making the point about drones.

Gavin Wishart: Well, I'm just talking about telephones.

Q260 **Martin Docherty-Hughes:** Well, look at telephones: we have iPhones which, even though the United States might not like it, have some components that are made in the People's Republic of China. The F-35 programme even has elements made in the People's Republic of China. That is an important part of the discussion, as Madeleine said, of the Select Committee on Defence. As members of the Defence Committee, what we are trying to understand is the risk. It is the same with iPhones, but we are not discussing iPhones or any other piece of telephony; we are discussing drones. You do agree that data-mining is a possibility from third-party nations.

Tony Burnell: I think we could not disagree.



Professor Gray: We cannot discount it.

Q261 **Gavin Robinson:** Good afternoon. Apologies for not joining you at the start—there are a few other things going on at the moment. I’m going to get a drone home, I think.

In addition to developing counter-drone technology, could you give us a sense of how useful industry can be in ensuring the effectiveness of authorities in responding to the malicious use of drones, and incident response in particular? Tony, you have outlined how there is sometimes a struggle and you are not getting the right guidance from Government; and Paul, you indicated how in other aspects of the ADS sector it is not as ingrained or co-operative. How ingrained is industry? How co-operative can industry be in assisting authorities when they have to respond to the malicious use of a drone?

Paul Everitt: We have strong relationships with a range of organisations. Within Government there is the Centre for the Protection of National Infrastructure for parts of the Home Office and indeed the police. We have a regular dialogue around a range of issues, which includes drones and counter-drones, but it has not been specifically structured around that conversation. Again, the Government’s strategy certainly indicates a willingness to put a little bit more structure around that sort of dialogue so that we can have a much more ongoing discussion both in sharing what we know and the technology we have available as well as taking from Government some of the insight they are getting on some of the intelligence they may be gleaning about either particular types of malicious use or adaptations that we might need to be more proactive in trying to develop responses to.

Q262 **Gavin Robinson:** When it comes to critical incidents and how useful industry can be at any given point in time, is the industry engaged in exercises, for example, and running through and testing what you do?

Tony Burnell: Yes. I mentioned earlier an RAF programme that is running at the moment that is engaging with industry through the UAS CDC. I understand that programme has been running for about five years in the background; there has been some R and D development and understanding in that programme. That programme is now open to industry, in an evergreening process, to look at new technologies and how industry can offer to bring those to the Air Force’s project. The project is called Project Synergia.

Q263 **Gavin Robinson:** You sometimes see guys walking through the streets in their white suits, acting out chemical or biological warfare and the response to it. Are we doing the same with critical incidents involving drones? Is industry engaged in responsive exercises and planning out what the problem is and how best to deal with it?

Tony Burnell: Not so much in responsive exercises. As I understand it, Government agencies such as CPNI are carrying out testing at the moment and understanding what the capabilities are of each different solution so they know how they can use those solutions.



Q264 **Gavin Robinson:** Is industry ingrained?

Tony Burnell: Yes, industry is very keen to be involved. I am chair of the drone platform and counter-drone group. We have 55 companies engaged, the majority of whom are in counter-drone. We meet every four months for workshops and presentations with the major groups such as CPNI, members of the police, JSaRC and the Defence Science and Technology Laboratory to talk about what the issues are and what we can do. There are trials held biannually, called the Bristow trial, where industry is open to take technologies along. We in industry would like to see a more cohesive approach, working closer and sharing the problem with Government—they share the problem with us—so that we can help solve that problem for them.

When there are incidents or requirements, industry are happy and have stood up to the plate many, many times before, often at short notice—within six hours.

Professor Gray: My day job is at Cranfield University. My role here is predominantly about promoting drones for good capability. Cranfield University has a global research airport and a defence arm at Shrivenham. We at Cranfield work with the Home Office and industry, and we play out the kind of scenarios that you are describing. To my mind, on the one hand you have capability developing solutions that can realise the economic benefit, and on the other there is very clear evidence of industry and Government working together on anti-drone capabilities.

Q265 **Gavin Robinson:** If there is a willingness from the Government to work more closely with industry and you see that relationship evolving, what do you feel it would be best for us to crystallise in our mind in terms of recommendations for what the Government should be doing as they seek to build a better relationship with industry?

Paul Everitt: Any strategy needs to be implemented, at pace. There is a piece, which was mentioned, about making sure that the owners of critical national infrastructure have good advice on how they should go about assessing the threat and what their options are for countering that from a drone perspective. Again, I am not trying to suggest that everyone needs the absolute level of protection, but they should think about what they do need. The third thing, which was also touched on, is that to be ahead of the game we need to be able to test and evaluate, and we need facilities available to us at a reasonable cost in order to be able to do that. That is a combination of access to facilities that the state may own and a regime that Ofcom controls that is sensible and appropriately structured.

Tony Burnell: We have talked very much about the limitations we have on using, say, RF mitigation, and that is down to Ofcom. There are many things that we can learn from other areas. I go back to the RF jamming, which is very similar to counter-IED or explosive ordnance device. If we have an EOD incident in the UK, we do not question, and Ofcom does not question, the use of capabilities to ensure that nothing can be detonated by remote control. In simplistic form, that is exactly the same as what we



HOUSE OF COMMONS

are trying to do with drones. We could look to that community and say, “How are you doing this? What’s the effect when you turn on your jammer across the whole of the bands?” If it has a very limited effect, how can we take that and bring it very rapidly into the counter-drone environment to use the same processes and procedures and to get legislation in place so that can be used?

Gavin Wishart: To reiterate, to do proper testing and evaluation of drones and counter-drones—it is a unique thing—you need airspace and you need to be able to control the RF environment you are in. It would be really nice to see something set up, if there is not already. There are a lot of air ranges in the UK that are run for the MoD by QinetiQ, I guess, through the long-term partnering agreement. It would be really nice to see one of those opened up—perhaps Spadeadam, which used to be an RAF resource; I don’t know whether it is now—so there was somewhere people could bring their good ideas. There are issues with IP—let’s not pretend there aren’t—and with how you deal with multiple groups of commercial actors working together for the better good. We do it in other areas, so there is no reason we shouldn’t be able to do it in this area. That would be a great idea.

Professor Gray: I echo what Paul Everitt said. A series of recommendations have been made; let’s implement them at pace. Let’s get the right balance between risk and opportunity, because there are real UK economic benefits to come through drones. A lot of the conversation today has focused on technology, but let’s get some fundamental communication protocols in terms of how we work in the case of incidents. It is not just about technology; it is about being joined up in understanding what the responsibilities and communication protocols are.

Chair: I thank the panel very much indeed. I am sorry we were interrupted by a vote, but it was well worth the wait and we are very grateful to you all for sharing your expertise. We will now swap over panels. Gentlemen, if you are inclined to sit in for a bit longer, you are welcome to do so, but, in the meantime, thank you.

Examination of Witness

Witness: Chief Constable Giles York.

Q266 **Chair:** We resume with a panel of one. Chief Constable, thank you for waiting so patiently. I am sorry that the vote, and our own natural inquisitiveness with the previous panel, led you to have to wait longer than planned. We are grateful to you for being here today. Can you say a few words of introduction about yourself, your role and your involvement with the past incident that was of such interest to the nation?

Chief Constable York: It was not a problem; I found the previous session incredibly edifying and you were flexible enough to accommodate me being allowed to do a meeting over in the City before coming here, so I am grateful to you for that.



HOUSE OF COMMONS

I pass on apologies on behalf of Lucy D'Orsi, the deputy assistant commissioner who is the national policing counter-drones lead. This week is half term and she made a judicious, and probably very good, decision to be with her daughter this week. I have had a brief from her but ask your pardon if I am not fully up to speed with where we are nationally around counter-drones.

I have brought a small contingent with me, should any of the panel like to talk to me informally afterwards. I have Andy, Lucy D'Orsi's staff officer, who is working in the area around national counter-drones. I also have Justin Burtenshaw, who is the commander at Gatwick airport, and Marc Clothier, who was the commander who dealt with the incident and was at Gatwick airport at the time. Through George, we have extended an invitation to Committee members who may wish to visit Gatwick, to see it and to have a presentation from them or for them to answer any other questions about it. I would be more than grateful.

I am the chief constable for Sussex police. I cover all policing from Chichester to Hastings, for those who know the coastline, and up to Crawley, including the policing of Gatwick, which is done in line with the policing of many airports across the country, working incredibly closely with Gatwick Airport Ltd as partners in trying to police that place.

Chair: Would it help you if your three colleagues joined you at the front?

Chief Constable York: I think they would rather sit where they are, to be honest.

Chair: They should feel free to pass the odd little note to you.

Chief Constable York: What we will probably get from them is the feedback of nodding and shaking of heads. That is more feedback to me that I can't see, but it is guidance to you.

Chair: I shall study the physiognomy with interest. Gavin will start us off.

Q267 **Gavin Robinson:** It is good to see someone leading from the front. I will let you know if there are any crooked smiles or nods of the head.

Could you help us understand how drones, and the threat and risk that they pose, have become an increased workload for you in your constabulary? How have your thought processes evolved around the threat of drones since the incident at Gatwick? Was it a previously important part of your overall work or is it a new and emerging issue that you are having to deal with?

Chief Constable York: If you permit me, I will speak quite broadly to begin with and then narrow down to try to answer your question in a coherent way.

I sometimes talk about social media; there is nothing wrong with social media, but there is something really wrong with the way some people choose to use it. You might be able to use that as a parallel with drones. There is nothing wrong with drones per se. We have already heard some

fantastic examples of where they do good; there are just some awful ways in which some people use drones.

There is another whole group that sits around the police use of drones. I had a demonstration at my own headquarters in the last two to three weeks. They are a phenomenal tool for finding missing people, finding burglars on the run, or looking through the windows of the third storey of a building so the firearms team knows the safest time to go through the door. There are exceptional and positive uses for drones.

The airport environment itself faces many risks. Gatwick Airport Ltd has its own security measures in place. Policing is there because it is part of the national infrastructure as well. Drones are part of the threat that we face together in and around that. Before the incident in December last year, there had been a lot of planning around what a threat from drones at the airport might look like. We had been through different scenarios of how we thought people might use drones to threaten the airport in different ways. The reality that we saw in December was exceptional; perhaps my sitting in front of the Committee demonstrates quite how exceptional that attack was. It was a criminal use of a drone. It was a sustained attack on the airport. It appeared to come from a person or people with good knowledge of how an airport operates and of drones and how to be able to use one under those circumstances. It was the sustained element that was quite unique to what we saw in Gatwick on that occasion.

We had a drone response plan, which was enacted. It had been tested by CPNI, which we have heard referenced many times here today, and it had been shared across the country as well. There was clear thought before the attack happened. I absolutely think that the attack at Gatwick, for whatever reason, has acted as an immense catalyst, to pick up on your point, to speed up the thinking around what counter-drone activity should look like. It is fascinating that, for all the evidence the Committee has heard in previous sittings and today, it is not necessarily the catastrophic, mind-stretching uses of a drone that can cause such disruption; it is the mere presence of a drone itself in the first instance.

I will finish by saying that, throughout this process, preservation of life was at the forefront of our minds. Many lives, holidays and families were disrupted because it was Christmas, but life was preserved.

Q268 Gavin Robinson: Having had an operational response plan to an attack from a drone, how has your understanding emerged or developed since that incident? How have you reflected on your plan, its effectiveness and what is required today?

Chief Constable York: There are two critical things around it. One is that it has expedited the sharing of what that looks like. There is a long and established national group of airport police commanders. During the incident, in the immediate wake of the incident and since the incident, all that learning has been learned and shared across that group. That is one thing we have learned as a result of the incident. Another thing is that there is now a national protocol that says, "Should this happen, here is a



HOUSE OF COMMONS

list of what can happen for you." That was not necessarily in place as fully as today when the incident happened.

Relevant to the Committee, I put on the record my thanks for the speed with which defence colleagues moved in order to be able to assist us. They were able to bring in equipment that was not on any notice to move. It involved characters who had already started their Christmas leave, but who willingly came out of their homes and deployed incredibly quickly, without necessarily having been part of anything warned about, planned or anything else in place there. Some things that we did in order to be able to stand up and react happened incredibly fast, without a clear blueprint in place beforehand.

Q269 **Gavin Robinson:** Do you feel that you have the necessary resources and expertise at within your constabulary should an attack like this happen again?

Chief Constable York: A recurrent phrase in pretty much any hindsight commission or inspection report is, "You could have done more." I think that we are much better prepared today than we were at this time last year. I think we have much better technology in place than we had at this time last year, and much greater expertise in place. Should anything happen again anywhere, I am fairly sure that any inspection team coming in will say, "You could have done some more."

Q270 **Gavin Robinson:** Have you increased your resource dedicated internally in your constabulary's budget to equip your force should there be another attack? Has the resource remained the same? Have you been granted additional resource from the Home Office?

Chief Constable York: The resourcing of the specific threat to the airport is more complex than just me increasing the resource; it is about Gatwick Airport Ltd increasing its investment and resource into this. I do not have a word of criticism for the way that it reacted to this; I have only praise for what it did and how fast it responded and brought in equipment as a result of this incident. It has invested really heavily in equipment; it has also invested in skilled staff, in order to be able to operate that equipment. Equally, we have increased our training for our staff, so they can understand what the conversations with the airport are about when they talk about the equipment and all that goes with that, and also so they understand the whole layered approach of protection. That is what you heard from the previous session.

The new strategy that has been released, either rightly or wrongly uses the phrase, "there is no silver bullet in this." There is a layering of protection against where people may launch a drone from, on identifying and detecting where it is, and being able to track it and identify it. Those are some of the key changes where we have been able to invest as a force and as an airport. Equally, we have had a bid through the Home Office, and I think it has funded about £1.3 million for investment into this area.

Q271 **Gavin Robinson:** Is that for Sussex?



HOUSE OF COMMONS

Chief Constable York: No, it is for the national capability. I think we could probably spend three times that to be able to stand up a national capability, which is what we are trying to do. This is more Lucy's world than my world now, because it is around the national response. I believe her ambition and agreement is to try to set up regional capabilities, because there is no point having Heathrow and Gatwick fully protected if Edinburgh and Glasgow are not. We need to buy enough sets of this equipment so we can have regional teams who can deploy. It is not only about deploying to airports, but necessarily about deploying to events as well, should that be necessary. It is about having skilled teams of officers who can intervene.

Q272 **Chair:** Before we move on, could I explore one aspect of what you said earlier, Giles? You said that there is much more capacity for protection at Gatwick than there was a year previously—in other words, before this incident. Is that right? You are saying that there are systems in place now, following the incident, that were not in place before the incident.

Chief Constable York: That is right.

Q273 **Chair:** Because you—or rather Gatwick—has seen what this incident can do and, therefore, it has decided to move in systems that had to be got in very urgently last time when the incident happened, and not in time to prevent huge disruption. Does that not betray an attitude of mind that you may have heard me mention earlier at the beginning of the previous panel? There seems to be a tendency as far as the threat from drones is concerned, that people wait until some sort of incident happens, and when the worst has happened, then they make the deployments of equipment, whereas it must have been possible to imagine that someone might use a drone to cause disruption at the airport.

That is why, coming back to the catastrophic scenario, which is the one that, as the Defence Committee, has to worry us most, I put to you the question that I put to the earlier panel: do we have to wait for an aircraft to be brought down in a populated area by a drone before it will be the right time or there will be the motivation to bring in a system of regulation and licensing for the ownership of these devices? Can we not anticipate that such a disaster will happen before it happens, and therefore try to bring in some form of control on the accessibility of these devices that could be misused in that way, in the same way that we have strict control of firearms in this country?

Chief Constable York: I understand all that you have said. There is something about hindsight, which we see time and time again, around what we could, should or might have done in many different circumstances. Absolutely, the success of policing is when something does not happen. It is so often the way, and it is really difficult to count what that means. The really challenging decision, which is probably more with you than with me, is on proportionality, because as we have seen there is an awful lot of good use of drones. There is a really positive and productive social emergence around them as well, and we are now working with a lot of our local drone clubs—we found any number of them



HOUSE OF COMMONS

in the wake of this. The registered drone clubs are working really constructively and positively with us. Absolutely at the heart of this, the really challenging piece of it, is proportionality and what that looks like.

Q274 Chair: I am president of a registered target rifle club. The fact that we have to have police checks and get our gun licences does not in any way impede our activities. In your opening remarks, you mentioned the good things that drones can do in the hands of the police, such as looking through windows, which can be of great value in an operation, but the police are appropriately authorised to use drones in that way. What happens if a great many unlicensed drone users start to look through the windows of their neighbours with these things? Then their neighbours might take some sort of direct action to try to protect their privacy, and it turns out that the neighbour is the one who has broken the law, rather than the drone user. The question of proportionality comes into it, but the question of regulation as a way of reducing the likely consequences of misuse is something on which I feel you ought to have an opinion that you might share with us.

Chief Constable York: In the example that you use, in honesty, if neighbours want to upset each other—we see that time and time again—there are much easier ways of doing it than necessarily through that mechanism. Again, that is why I say it comes down to proportionality. As has been said here, and as you have said, this Committee is minded about the most disastrous. That is where there is the spectrum of the completely lawful to the merely annoying, right up to the wilful and unlawful criminal intent around them. It is about the proportionality across that spectrum of how we choose to use regulation and legislation.

Q275 Mrs Moon: The sorts of threats that we may see in mainland Britain have probably been experienced in theatre, because there you often have adversaries who are constantly probing a higher level of support and protection. How much—not necessarily you, Chief Constable, but the officer you have designated to focus on this in particular—are you kept up to date with the sorts of uses that drones are being used for in theatre, so that you can explore the feasibility of that being a threat in the civilian world? Do you follow what I am saying?

Chief Constable York: Absolutely, I do. One of the things that has changed in the last year is the sharing of that information. Different groups are working together. Lucy D’Orsi has brought together a counter-drone working group within policing. That has a very broad membership working with them. It has CPNI, DSTL and the military on there, so there is the forum by which that information can be shared. On the example you used of use in other theatres, another word that we use around here would be “collateral”. You may be trying to have an effect on a drone, but what other effect are you having on many other things that depend on radio frequencies? If you then put that into an airport environment, the collateral of some of the options available to us is a significant consideration either for the person authorising that or the person who will take effect with it.



Q276 Mrs Moon: But our military also manages airports around the world. Those airports are under attack and threat for totally different reasons, but they are a testing ground, often used by groups who would wish to harm and attack us, for trying out new technologies and ways of using, for example, drones. Having tested in theatre, they think, "Let's take it to a softer target in the UK," which will not necessarily have the technological sophistication that you need to protect you in theatre.

Chief Constable York: One of the key bits of work that Lucy D'Orsi has done is to engage with DSTL and the Home Office, which can commission work there. The previous panel talked about having a clear operational requirement from policing. We have been working on that during this year. A clear operational requirement is now in existence. We are looking for the resourcing for that with the Home Office, to be able to commission it and ask how we can meet this operational requirement. DSTL has absolutely been part of that process and is working with Defence on that.

Q277 Chair: To finish off our earlier exchange, may I check one point? Why is it that the equipment, which has now been permanently installed at Gatwick as a consequence of the incident there, was not installed by the airport before the incident?

Chief Constable York: I am not sure that I am best placed to be able to answer that on behalf of the airport. There is something around—again, it came through on the previous panel—the effectiveness and the testing of the equipment, as well. It is a broad market. I think one person said he has 55 members of his group. Part of it would necessarily have been a procurement process, to say which is the best equipment to have. It was not that there was no equipment there at all, but that they have been able to enhance their equipment since then.

Q278 Gavin Robinson: You mentioned that one of the learnings and outcomes of your appraisal of the incident at Gatwick was that you now have a codified list of resources available to you and the other authorities that you can engage with and draw support from. Could you give us a sense of the relationship between yourselves and other police forces, yourselves and Government, and yourselves, Government and critical national infrastructure? Are there any breakdowns in that tripartite relationship?

Chief Constable York: To answer your last question first, I do not think there is any breakdown in the relationship. There is a coherent approach to finding a solution, because it is seen as a priority. For myself, in the middle of the incident, I spoke to Assistant Commissioner Neil Basu, most days, even when he was off for Christmas. Another confusing thing in this situation was that it was during Christmas, not only for the public, but for the police. My deputy would have been speaking to Lucy D'Orsi most days. We had Metropolitan police officers on the ground within hours of asking them to get there. We had something like over 800 officers from seven different police forces respond in order to help us respond to this incident.

This incident affected policing not only in the UK, but around the world, and the policing of airports particularly. Justin Burtenshaw, who was the commander at Gatwick, has been to a number of conferences and had



HOUSE OF COMMONS

even more visitors come to Gatwick to do learning around that. The coherence across police forces is positive. Lucy D'Orsi met with the Home Secretary recently. That was incredibly positive for making changes. There is a real desire to do this. One bit that could shift a little bit is the scale of investment that we are able to put in, to be able to move forward the regional teams with equipment that is effective, and to be able to move forward the operational requirement and get the responses from industry around that.

Q279 Gavin Robinson: It does not sound too considerable. You have mentioned £1.3 million and that you could spend three times that.

Chief Constable York: Between £4 million and £5 million was requested.

Q280 Gavin Robinson: You may be able to answer this only from your constabulary's perspective rather than the national picture, and fair enough if that is the case, but how do you feel the threat of drones is best considered within counter-terrorism policing?

Chief Constable York: Neil Basu leads the national counter-terrorism approach. Certainly, my personal experience with him during and since this incident would say it is incredibly positive. It is about airports and national infrastructure, and there is also really clear consideration about set events, such as football matches, concerts and other things. That is absolutely on their agenda.

Q281 Gavin Robinson: So the threat of drones is not separate and distinct but is considered as a counter-terrorism aspect of policing?

Chief Constable York: Yes.

Q282 Martin Docherty-Hughes: From a police perspective, what are the challenges to detecting, tracking and identifying malicious drones? You talked about financial resources a moment ago, but are there any other challenges in detecting, tracking and identifying malicious drones?

Chief Constable York: The most difficult bit about it is your adding of the word "malicious", because it adds a mental intent of the person who is flying it.

Q283 Martin Docherty-Hughes: And most of the time it is not?

Chief Constable York: Most of the time it is not. To be able to find that malicious element, you could only do it by interview and by the person telling you what was in their mind at the time. I am sorry if that sounds a trite answer; it is not meant to be.

Q284 Martin Docherty-Hughes: No, it does not, because my next question was about whether technical solutions are available to officers who need them. It seems to be that you need more police officers and a hell of a lot more time if you are to interview a lot of people who might unintentionally have a negative impact using drones. As a Scottish constituency MP, I will leave that up to you and your colleagues at the Home Office because it is completely devolved.



HOUSE OF COMMONS

Are local forces being provided with operational advice and guidance from national policing leads and what is the role of the NPCC? For a point of clarity, can you advise whether the National Police Chiefs' Council covers England, Wales and Northern Ireland only or all of the United Kingdom of Great Britain and Northern Ireland?

Chief Constable York: It covers England and Wales. It does not cover Scotland, but I think it covers Northern Ireland as well.

Martin Docherty-Hughes: That then is a question that I will take back to the Chair and the Clerks.

Chief Constable York: You asked a question before that.

Q285 **Martin Docherty-Hughes:** My question was whether in your perspective, local forces are being provided with operational advice and guidance from national policing leads, and is there a role for the NPCC in that?

Chief Constable York: Absolutely. Lucy D'Orsi's role as the national counter-drones lead is an NPCC role. She wrote to all forces in March with really clear directions, support and help, to say, "These are the considerations you should have around counter-drone capabilities within your force area." That is why I stressed previously that you cannot say, "I haven't got an airport; this isn't for me," because every force area will probably have a large gathering of some people for something at some point. Even though the NPCC does not cover Scotland, there is absolutely sharing with the Scottish police force when it comes to something as serious as this.

Q286 **Martin Docherty-Hughes:** As Scottish constituency MP, my request is—through the Chair, of course—that there is a letter off to the chief constable of Police Scotland, if not the police authority of Scotland, because, in terms of the questions that we were asking Giles, there is important critical national infrastructure in Scotland—huge oil refineries, Dounreay, the nuclear deterrent, and so on. Those are important issues, Chair.

How can you disrupt, disable or destroy malicious drones when you have identified them? What is your perspective? You may feel that that is not within your remit to answer. Are there technical solutions available from a police perspective?

Chief Constable York: I will take it at quite a generic level, for two reasons. One is not to belie what we do and can do, and what we necessarily cannot do. The other is that if I go into a technical space, it is probably not for me to be speaking there. The obvious thing is somehow to physically intervene with the drone and take it out of the sky in some way—that would be one way to do it. The other way, as we have heard from the previous speaker, is to engage somehow with what is controlling the drone, and to be able to do that as well.

Q287 **Martin Docherty-Hughes:** Through your experience of the Gatwick incident, are you happy with the decision-making protocols that are in place to deal with the eventuality of disabling or destroying a malicious



HOUSE OF COMMONS

drone?

Chief Constable York: I am much happier today than we were before, because the law is much clearer. We were absolutely trying to establish authorities during the day of what we could and could not do. In fairness, the Home Office and the Minister were incredibly helpful and moved incredibly fast in order to be able to help us with that. If there is one slight loophole that I would like to be able to move to, it would be that—for example—should Gatwick have and maintain the equipment that can detect, track and identify, and if we license an effector on the end of that that can say, “Yes, we can now do something about it,” at the moment the authority to use that effector sits at chief constable level, which I am happy with. However, the only person who can effect the effector is one of my staff. I cannot give an authority that allows Gatwick Airport Ltd, with all its expertise in using the equipment, to use that final bit of intervention. That would be one bit of the law that we would like to see changed.

Q288 **Martin Docherty-Hughes:** That is the division you would like to see of the existing legislation.

Chief Constable York: Yes, and I hope Andy is nodding behind me.

Q289 **Martin Docherty-Hughes:** I see a lot of vigorous nodding going on behind you, and I’m glad you mentioned it.

Chief Constable York: There’s quite a nuance to it, Martin, so if you want written confirmation of what that actually means, I am really happy to follow up on that.

Q290 **Martin Docherty-Hughes:** That would be good, because it is the kind of detail that we are looking for. Talking about effective technology, has there been an experience of it being deployed during an exercise in situ that you are aware of?

Chief Constable York: I am not aware of where we have done it in situ. We have certainly done a lot of table-top exercises that include it.

Q291 **Martin Docherty-Hughes:** Are you sharing that table-top exercise information with other forces?

Chief Constable York: Oh, absolutely. And with other airports.

Q292 **Mrs Moon:** We are all looking forward to meeting Lucy D’Orsi at some point, because you have mentioned her so often. She might not be here, but by golly we know what she is up to. You mentioned that she had given you a briefing before you came. Is that something that you would be able to share with us?

Chief Constable York: It was on the telephone. Apologies.

Q293 **Mrs Moon:** Okay. I wonder whether you could take us back again to when you were actually facing the challenge during Operation Trebor—as in mints, I take it. What were the key challenges that you were facing then? As it evolved, was the level of co-ordination with central



HOUSE OF COMMONS

Government good enough, and do you think it has improved?

Chief Constable York: The primary thing that we were facing, as I said, was the safety of the public. That absolutely had primacy for us. In facing that, we were working incredibly closely with Gatwick Airport Ltd—we were sitting in their control room and they were in our control room. There was minute-by-minute, if not hour-by-hour, engagement with Gatwick Airport Ltd. We had an incredibly positive relationship. Alongside the public safety bit, there were the detect, track and identify elements that were going in, so we were getting equipment arriving from the military and others during the period of what we were facing. Then there was the piece around trying to kick off an investigation that sought to identify somebody who may have an intent or want to be able to do this, or any intelligence that existed. The engagement with other forces—the Metropolitan police and several others sent us resources—was really positive. Equally, the engagement with Government was incredibly positive. If there was potentially one thing that could have been more streamlined, it would be which ministerial meeting we should be going to, because naturally in this space, the Home Office was incredibly interested and so was the Department for Transport. There was something about working for two masters in that space.

Q294 **Mrs Moon:** Do you know whether Cobra was ever called?

Chief Constable York: Cobra was called, and I think it was chaired by the Home Secretary when it was called.

Q295 **Mrs Moon:** That would have solved the problem. Rather than different Departments holding individual meetings, it should have been an overall Cobra response, surely?

Chief Constable York: In the heat of what was going on, Cobra was called, and then in the following week, as the airport had been reopened and we were in recovery and reinforcement, when Cobra did not sit it was accountable to both of the Ministries in turn. As a result of it, Marc, who is here, went up and sat within the Home Office counter-drone team to share his expertise with them in the immediate light of it, so he spent the first two or three months of this year working out of the Home Office from Sussex Police.

Q296 **Mrs Moon:** Let's talk about when the military came in and the capability that they brought. It was the RAF, I understand? I want to make that plain, because everybody refers to the Army and it was the RAF. I only say that as chair of the RAF all-party parliamentary group. Why did you need military capability, and could that have come more quickly? Were you left without that crucial extra expertise or kit for longer than perhaps you should have been?

Chief Constable York: From my experience of calling on military aid to the civil power, considering that it was not on notice to move in any way, it arrived incredibly quickly for us, and it arrived with the right people to make it operate. I think, given the circumstances we faced at the time, I



HOUSE OF COMMONS

was summarily impressed with how quickly the RAF were able to get their equipment and their personnel there.

Q297 Mrs Moon: I assume that within your police force area you must have a number of places that involve critical national infrastructure. As it happened, it was an airport, something that is very visible, with lots of people tweeting out, "Oh my God, we're not going on holiday!" It is very immediately accessible and public awareness-raising. How do you think it might have played out if it had been, for example, a threat to a water treatment works or to electrical supplies? Do you think the response would have been different? Would it have been handled differently? Would it have been a slower response? Have you even played that scenario out?

Chief Constable York: We have certainly played them out nationally, but there is something about the immediacy of the effect. If there was an attack on another part of the infrastructure—speaking from public knowledge as opposed to any police knowledge—you have contingencies that can kick in and can supply your water, your electric or your gas from somewhere else, should that be the case. That is not the case when you have an airport and people waiting to get on to aeroplanes. You are absolutely right that it could and would play out very differently. We have seen that play out differently as well.

Q298 Mrs Moon: Are you happy with the skills training and transfer between blue-light and military expertise and knowledge? Is that being shared? Is there a more open and willing transfer of skills and expertise, working alongside each other, following Gatwick, so that at least we can say, "That was a really positive outcome"?

Chief Constable York: I sat with the officers from the RAF as they were operating their system, and the generosity of what they shared with people from Gatwick who were adopting the system was testament to the heart of what you are saying. Policing now gets its science and technology from DSTL, and we have access to an awful lot of what DSTL are doing. The police are benefiting hugely from what the military have learned, and I am not aware of anything that is standing in their way or any hindrance to accessing what they are doing.

Q299 Mrs Moon: One final question. You heard the evidence that we took about the time lapse between drone technology and anti-drone technology. Given the restrictions on police forces' budgets, are you confident that you are able to keep abreast of the new technology—both the drone technology and the management of it—that you need to protect places like Gatwick?

Chief Constable York: I don't have enough knowledge of the type of technical advances that are being made and what we need to stay abroad of in order to try to stay ahead of them. We have very positive relationships with the drone manufacturers but, from a conversation over here, I think it is much more difficult to keep up with people who may choose to build their own or others. Essentially, at the moment, counter-drone measures are physical or electrical. Those elements of the

technology aren't necessarily changing dramatically, so it is about trying to refine what we have and make it safe to use.

Q300 Chair: We are on the home straight now. To wrap up on the Gatwick affair itself, after 10 months and a reported cost of £800,000, the criminal investigation into the incident has been closed. Can you tell us why that is? Presumably it is because we haven't been able to find the perpetrator.

Chief Constable York: We have exhausted the lines of inquiry that we had. We have had any number of persons of interest who have come to our notice. We have investigated all of them and cleared all of them, based on what we know to date. We have looked at a huge amount of data to try to identify the drone and other things like that. Those have been explored as well.

The vast majority of the £800,000 for the total cost of Operation Trebor was spent in the first couple of weeks of trying to react and respond. The investigation will absolutely be opened in a flash should somebody want to come forward and give us information, or if there is a new angle that we can take on the investigation.

Q301 Chair: One of the most curious parts about it was that there was no filmed imaging at all of the drone, even though so many people thought they had seen it. Isn't it rather strange that no CCTV system and nobody with a mobile phone camera managed to pick up this device when it was causing such disruption?

Chief Constable York: I am not surprised. We had, I think, 109 credible confirmed sightings. When you consider what it looks like and how fast it moves, trying to capture that on anything is fantastically challenging. Should you wish to come and visit Gatwick Airport to have a look, I would welcome you there, because why it wasn't captured kind of feels obvious. Gatwick Airport—I am looking behind me—is a huge area. You try telling me what a drone half a mile away at the other end of a runway looks like from here, film it on the best phone that you have got and show me the footage that says, "Undoubtedly, this is what we have got." This is one of the fascinating things for us. We feel that we have seen so many pictures, videos and whatever of drones in flight, but considering the length of the runway, the width of the airport itself and the distances concerned, personally, having been at the heart of it, I am not surprised we haven't had any.

Q302 Chair: On the basis of our former discussion about the extent to which the airport did or did not think in advance—I appreciate it is for Gatwick Airport Ltd to respond to questions about that—did the police never ask Gatwick Airport Ltd to have stronger countermeasures in place? Was there never any discussion as to whether or not they were adequately protecting the airport facility against interference of this sort?

Chief Constable York: Absolutely, we have those conversations.

Q303 Chair: You have them now, but did you before the incident?



HOUSE OF COMMONS

Chief Constable York: No, before the incident we were having those conversations. Now, of course, the catalogue that was described by the previous panel is a lot fuller, with a lot more confidence, than at this time last year, because there is an imperative.

Q304 **Chair:** But you are not aware of having made any representations to the airport that perhaps they needed to have more countermeasures in place.

Chief Constable York: Again, I think there is more of a partnership in how we approach the protection, rather than us making representations about what they should or should not have in order to protect it.

Q305 **Chair:** Let me put it another way. In the discussions that you had with them about the possibility of drone problems before the incident happened, was there no feeling that perhaps the methods that they had permanently in place were insufficient to prevent disruption, as turned out to be the case?

Chief Constable York: I think there may well have been, but I was not party to those discussions, so I cannot say whether there was or was not.

Q306 **Chair:** Would there be a record of that anywhere in your archives?

Chief Constable York: I don't know.

Chair: Perhaps you could look into that and let us know.

Chief Constable York: We can follow that up afterwards.

Q307 **Chair:** What lessons do you think have been learned from this whole rather sorry incident? The good part about it is what you have said to us today about the way in which the military reacted, and the effectiveness and speed of that. However, it should not have got to a position where the airport was disrupted so badly. What lessons have been learned locally and nationally? Did you contribute, given the experience that you all went through, to the counter-unmanned airport strategy that has just been published?

Chief Constable York: Some of the critical lessons that have been learned are about "detect, track and identify" and about having a really clear strategy in place. The counter-drones working group has been fundamental in developing that strategy. Sussex Police has a seat on that, and Justin is my representative on that strategy. Absolutely, yes, we are contributing to it as a national response.

Q308 **Chair:** Are there any specific recommendations that you want to highlight as a result of the experience of that disruption?

Chief Constable York: It was unprecedented, pretty much anywhere around the world, to have a sustained attack in that way. I think that Gatwick Airport was as well prepared as any other airport at the time, which goes to your question of whether they should have had more. I would say that they had as much as anybody else.

Q309 **Chair:** So they would all have been disrupted in that case.



HOUSE OF COMMONS

Chief Constable York: Yes, absolutely.

Q310 **Chair:** Finally—from me at any rate, unless there are any last-minute bits from my colleagues—I have a couple of questions about police powers.

Again, referring to the counter-unmanned aircraft strategy document, do you feel that this strategy, if it comes into force, effectively gives you the powers and technology you need to address the threat—I should say the range of threats—from drones? Do you think it is sufficiently funded?

There is going to be a Bill called the Air Traffic Management and Unmanned Aircraft Bill that has some police powers outlined in its provisions. Do you think that those powers are sufficient to enable the police to address the threat from the malicious use of drones?

Chief Constable York: I believe that the new powers will put us in a much better position to address it. Should all of this sit on policing's shoulders, or should some of the enforcement necessarily sit elsewhere as well? We will need some clarity on that.

As for the resourcing element, I commented earlier about the immediate resourcing in place here needed for policing to put out regional teams that can respond and, equally, to respond to an operational requirement that needs to be put out for the benefit of the suppliers.

Q311 **Chair:** Is there any last comment that you would like to make before we wrap up?

Chief Constable York: No. I would just like to thank you for the opportunity to come along today.

Chair: Thank you very much, and thank you to your team for supporting you with vigorous nods of the head. I did not notice too much wild shaking in a negative fashion, so I think you must have stuck to the brief that was so ably supplied.