HOUSE OF COMMONS

Defence Committee

Oral evidence: Domestic Threat of Drones, HC 2117

Tuesday 3 September 2019

Ordered by the House of Commons to be published on 3 September 2019.

Watch the meeting

Members present: Dr Julian Lewis (Chair); Mrs Madeleine Moon; John Spellar.

Questions 162-203

Witnesses

I: Dr Anna Jackman, Royal Holloway, University of London, and Arthur Holland Michel, Center for the Study of the Drone, Bard College, New York.

Written evidence from witnesses:

– Dr Anna Jackman (DTD0013)

Examination of witnesses

Witnesses: Dr Anna Jackman and Arthur Holland Michel.

Q162 **Chair:** Good afternoon, and welcome to our first public session on the domestic threat caused by drone technology.

We have two expert witnesses today. Although the Committee has had some roundtable private discussions before, because this is our first on-the-record session we will try to use the first part of the session, which we expect to last for about an hour, to set the technological scene. We hope later, not having been too finely drawn into the technical detail, to ask you about the broader policy issue and in particular about whether this is a problem that can be managed without a considerable restriction on the whole question of public ownership of drones, which can be bought off the shelf or by mail order. We will come to that later; it is fundamental to our inquiry, as the Defence Committee.

Can you both introduce yourselves briefly for the record, starting with Anna?

Dr Jackman: Hi, my name is Dr Anna Jackman and I am a lecturer in political geography at Royal Holloway University. I have been doing drone research for about the last seven years.

Arthur Holland Michel: My name is Arthur Holland Michel and I am co-director of the Center for the Study of the Drone, which is a research institution at Bard College in New York state. I am the author of a number of reports, including one on counter-drone systems.

Q163 **Chair:** Thank you both very much for coming here today. By way of background, can you briefly set out what the capabilities of commercial off-the-shelf—COTS—drones pose in terms of a threat to UK security? What should the approach of the authorities be to deal with bespoke drones, which may have been designed specially to pose a threat, or modified drones, which may have been bought off the shelf but altered to pose a threat?

Dr Jackman: Maybe I will start with a little bit on capabilities. The short answer on the capability question is that it is platform dependent, but the larger answer is that we should think about drones as part of a kind of ecosystem of platforms, with a real and growing diversity of platforms therein.

If we look at existing surveys of consumer platforms, we can see that they have really varying capabilities. Some of the lower-end platforms may have a range of only 100 metres, whereas some of the mid and higher-range consumer drones might have a range of 8,000 metres or 5 miles. They vary in the speed that they travel; they might be travelling at 10 kph or 90 kph, which is 55 mph. They also have really different carrying capacities. You might see drones carrying several hundred grams of

payload or up to a couple of kilograms. You also see things such as flight time varying a lot, between seven and around 40 or so minutes, and different capabilities on altitude or how far they can fly vertically. That might be 100 metres or up to nearly 5 km.

We see a lot of variation within the platforms currently available for you or me to buy off the shelf. That is complicated further by the growing context of racing drones, or drones that are used in the aerial sport of drone racing, which are smaller and can carry a lot less, but are a lot faster, travelling at between 60 and 160 mph. They are a reimagining of the low and slow drones. We also have, as you mentioned, drones built from kits or from scratch.

I will just talk a little bit about a couple of notable functionalities, and then pass over to Arthur to talk about future forecasting. A couple of really important functionalities, when mapping threats, are around things such as the autopilot feature. On many mid or higher-end commercially available drones, we might see that drones are able to follow predetermined flight paths, so that you set a flightpath up via GPS and the drone can then follow its own flightpath, as opposed to manual flying. There is also the issue of intelligent flight, which refers to a movement toward smart manoeuvring of drones.

DJI drones, the leading Chinese manufacturer of drones, has equipped many of its platforms with capabilities such as 'follow me', which means that the drone can lock on to an operator or to a moving target and follow that individual around. They also have capabilities that allow them to rapidly ascend or descend, or increase or decrease speed, which means they move in more interesting ways.

There is also a fundamental question about what you look for when you are visually IDing a drone. Smart capture features, which allow someone to use their hands to gesture—to take images, for example—mean that you are not necessarily looking for a controller or a smartphone anymore; you might be looking in a different kind of way for someone waving around.

The last current functionality I would like to mention is the live broadcast feature. Again, this is one that is commonly paired on DJI drones, but it allows a user to connect up their drone to their social media, be it Facebook or Twitter, and livestream the footage they are capturing, which, as we will likely go on to discuss, has propaganda implications as well. Huawei recently demonstrated a capability where a drone could livestream and make a video call to a smartphone as well, so we are seeing the broadcast capability coming into force.

Arthur Holland Michel: I just want to echo what Anna has said. I will start with a quick anecdote. A few months ago, Brian Harrell, a senior official at the Department of Homeland Security, set a task for two engineers to modify a drone to carry an explosive. They got a drone from Toys R Us and equipped it with a little claw mechanism that was Bluetooth activated and was able to drop a six-inch pipe from 35 feet. It cost $104

to put together, and the engineers were actually his sons, who were eight and 10 years old. They did that without any assistance. That just goes to show what the barrier to entry looks like.

That being said, that is a very limited capability. Those drones, as Anna mentioned, do not have a very extended range. They cannot fly very high and they cannot fly for very long. As you spend more on your drone, you get better capabilities, but to get one of those really dangerous drones is still quite a lot of money, unless you have technical expertise. There are two barriers to entry: you can either have financial resources or technical expertise.

Q164 **John Spellar:** If I can interrupt, do you see the greatest risk of drones coming from carrying explosive capability or from their kinetic impact?

Arthur Holland Michel: It depends on the size of the drone and the size of the explosive. In the case of these small hobby drones that would carry a six-inch pipe, they could only really carry maybe a pound of explosive, if that, so you might be able to achieve much more kinetic effect with a much larger drone that does not have any explosive on it. That being said, a much larger drone could also carry much more explosive, so it depends what you have available to you. That is what I will say about current capabilities. If you want me to comment on future forecasting—

Q165 **Chair:** Let me give you a little bit of in-flight refuelling, as it were, before you proceed. The sort of thing that we as the Defence Committee are interested in is the capability of drones, possibly bought off the shelf and/or modified. They can do surveillance; they can do propaganda, as you say; and as we saw at Gatwick, they can certainly do disruption, but the most important feature we are interested in today is destruction.

You made the point about youngsters fitting up a drone with a claw. Dr Dunn of Birmingham University, who I believe will give us evidence in a later hearing, published an article in *International Affairs* in which he says, "even drones without a payload represent a potential threat that is as yet unaccounted for in conventional risk assessments. Their size, cost and ease of use make small drones ideal devices to be swarmed against vulnerable targets. By virtue of either their kinetic energy alone or their ability to function as mechanical bird strikes, drones pose a significant threat to commercial airliners." In separate written testimony, he said, "The existence of drones uncontrolled and unregulated makes it possible that an aircraft can be brought down as easily by an 11-year-old child as by a terrorist."

Arthur, I see you are smiling at that point, but I think it underlines the point you made earlier. Just to help both of you, this is particularly the sort of abuse on which we would like to focus today. We are interested in what can be done to have a safe environment for the legitimate use of drones, but that is more for other Committees. Our concern is the person who doesn't give a fig about the legitimate environment but is out there because they want to wreak mayhem and cause destruction. You may like to proceed a little bit along the line you were going about the sort of

threats we might be facing and how adaptable drones are to inflict them.

Arthur Holland Michel: Absolutely. I hope later in the session we will have an opportunity to speak about the technical capabilities of counter-drone technology—

Chair: Yes, that is coming up.

Arthur Holland Michel: But I think it is important to do a little forecasting at this point as to what we can expect coming down the near-term pipeline in commercial COTS drones that anyone could buy on Amazon. Everything that I am about to describe is pretty near term.

You are going to see range improving, largely because of improvements in communications technology—the RF link. LTE mobile phone communication is also becoming a communications modality for drones, and that could essentially enable someone to fly a drone from anywhere in the country, because it is like making a telephone call. That is also very difficult to jam, because in order to jam that connection you also have to take down mobile phones in the vicinity of the operations area.

Not only that; there are a number of features that are intended to make commercial drones safer for regular operations in airspace that will inadvertently make them harder to defend against. One example is frequency hopping. You want to have a very robust radio link with your drone so that it doesn't go AWOL. That means that the drone will hop through the frequencies to ensure that you get the best connection at all times, but if a drone is hopping through the frequencies very quickly it will be hard to jam it.

A security researcher at an American firm called Red Six Solutions told me a couple of days ago about how commercial drones are having their GPS receivers positioned in such a way as to minimise interference from ground clutter. That is to give you more satellites to have better accuracy, but that also gives you better accuracy if, say, you are trying to use the drone as a rudimentary cruise missile.

Drones are getting larger. Thanks to a number of improvements in motors and things like batteries, they are getting faster. Some of the racing drones that Anna spoke about can hit maybe 80 mph and Red Six Solutions, the firm that I mentioned, has tested drones at 200 mph, using technologies that they are able to assemble DIY-style. The sensors themselves are getting smaller. If you are trying to do surveillance of a facility, you may not need a very large drone to carry a very powerful sensor. A British firm, Horizon Technologies, has developed a sensor for listening in on satellite phone communications. This is a very high-end sensor and it fits on a DJI quadcopter.

Then there is autonomy, which can be in the service of making these drones safer for use in the airspace, but there is a flipside to that. I will give you an example. Researchers in Switzerland recently developed a drone with a very agile obstacle avoidance system. That may be very good

for avoiding an airliner that is in the flightpath of the drone or vice versa. They demonstrated it by throwing a soccer ball at the drone in a very confined space. The drone was autonomously able to avoid it, but some of the main counter-drone systems are net-based. That same drone would in theory be able to avoid such nets that are thrown at it.

I will say two last things. The first is on swarming. There is a lot of talk about swarming and we can talk a bit later about how swarming makes the security challenge even more complex.

Q166 **Chair:** Before you do, that was going to be my next question, so I will just interject at this point. The approach at the moment seems to be to have what might be called a de minimis rule and basically say, "We will regulate drones above a certain low level of weight and size, and we will not regulate drones below that level." In your remarks on swarming, can you explain the extent to which such a division is unsafe, given the prospect of swarming large numbers of small drones? If they swarmed in such a way that they clog the engines of an airliner taking off or coming into land at a couple of hundred feet, could that bring the airliner down?

Arthur Holland Michel: That question is dependent on doing some thorough simulations of the actual dynamics at play. As yet, there have been no engine ingestion tests of drones. We don't actually know what happens when a drone goes into a jet engine; all we have are very sophisticated simulations that give us an idea that it is probably a very bad thing. Again, you have a trade-off. The drones that fall within the weight threshold, which you described, are very small, so you would have to have a very large number of them in order to achieve that kind of kinetic effect. That is probably quite far down the line, because at this point it is quite challenging to scale up the size of your swarms.

Also, the smaller a drone is, the less onboard processing power it can have and the less endurance it will have. That also creates limiting factors for your swarm. That being said, a study commissioned by the US army, by the National Academy of Sciences in the United States, estimates that by 2025 swarms of up to a few hundred drones—I am not saying that those are below that weight threshold—will be eminently accessible. That gives you a sense of how soon that is coming. That being said, you don't even need a true swarm, where the drones are actually collaborating with each other in a dynamic way, to achieve your effect. You may be able to launch 10 drones today, set each on an independent GPS waypoint and achieve the same sort of effect, and really you only need 10 drones to do that with existing technologies.

The last thing I will say is that we have to bear in mind that the knowledge behind the malicious use of drones will also become more readily accessible in the years ahead. There are lots of online forums and DIY spaces where technical capacities are experimented upon and knowledge is shared. That is not only for malicious purposes, but largely for a very positive purpose among the hobbyist community. However, that knowledge becomes more and more available with each passing year.

Q167 **Chair:** Anna, would you like to take it a step further? By all means refer back to some of the points that have been raised since you last spoke, but would you also like to set out your assessment of the vulnerability of the UK to the malicious use of drones by people trying to cause maximum damage? And, apart from the very obvious weaknesses of airports—both to disruption and, heaven forbid, to the bringing down of an aircraft—are there any other parts of the national infrastructure that you regard as particularly vulnerable? Arthur, I may come back to you afterwards on that.

Dr Jackman: Yes. If you'll permit it, I would also like to speak to part of your previous question, which was about the mapping of threats and risks themselves.

Chair: Please do.

Dr Jackman: I am sure that we will come on to discuss further non-kinetic issues, but as kinetic issues are your focus, within battlefields themselves, we have seen kinetic drone deployments in a growing number of ways. These have surrounded the obvious dropping of explosives, particularly 40 mm grenades. Arguably, that is led a lot by IS—Islamic State—actions. But we have also seen the non-state actor groups getting a bit more creative, for example by embedding explosives in drones so that when they are grounded and forensically inspected, they explode. People are really tapping into the existing history of IEDs and thinking about how they can be made airborne. In 2016, there was a case where Islamic State killed two Kurdish soldiers by doing this—by embedding explosives in that way.

We are also seeing a change on the battlefield in terms of kinetic uses linking to frequency and to what Arthur was just talking about—rudimentary swarms and, even if they are not all in collaboration, seeing drones in volume. We see journalists reporting in Iraq instances of 10 quadcopter grenade attacks in an hour, or three-to-five-drone swarms. So you are seeing this kind of volume amplification and the idea that drones above you can cause harm below but also just cause confusion and muddy and complicate a scene.

Q168 **Chair:** Would it be fair to say that, given what has already been achieved in the development of drone technology, we have to work on the assumption that if we are simply talking about certain limitations in range, endurance or capacity, it is only a matter of time before "improvements" allow those limits to be breached? In other words, ought we to be working on the assumption that even if certain drones—off-the-shelf-type drones, however modified—can only keep up in the air for a quarter of an hour at the moment, in a couple of years' time you will probably be able to multiply that by a significant figure?

Dr Jackman: That is a fair statement. We are seeing the battlefield context as a crucible. It is a space for experimentation around improvising innovation, and it's reasonable to expect that some of the wins that the non-state actors have will be attractive to other groups.

There are a couple of things, as a sort of caveat, on that. The first is the fact that there are ideological issues here. Some researchers, such as Ash Rossiter, have written about the way not all non-state actors will necessarily find these platforms ideologically attractive. There's a need to be attentive to the ideological interests of different groups and some of their desires.

Q169 **John Spellar:** Sorry, what does that mean?

Dr Jackman: There might be particular reasons why, for example, a non-state actor group does not see the drone as a very attractive device. It might be the question of martyrdom—the way in which, for example with suicide vests or bombs, the act of killing oneself in the action is an important part of the desire to use that weapon of choice. I think that is a consideration.

Q170 **Chair:** On the other hand, there have been cases, such as the Times Square case, where the idea of using a drone was particularly attractive because it was seen as some sort of payback for the use of drones to eliminate individual terrorists.

Dr Jackman: Absolutely. That was the second point I was going to make, which is about symbolic value. The icon of the war on terror is the armed drone, so in many ways, using a consumer drone to subvert or challenge this asymmetric war is actually a massive symbolic win.

Q171 **Chair:** You can argue it either way.

Dr Jackman: Yes. It's a tricky thing to talk about, but there is also a question that Arthur and I have discussed around resourcing. The Islamic State is not necessarily a typical non-state actor organisation, in terms of the resourcing that it has for this issue. They pioneer a lot of the kinetic drone use on the battlefield and there has been some excellent work, for example, into the supply chains that they use, their makeshift factories, the drone units that they have pioneered and their very elaborate procurement system, which consists, as drone researcher Don Rassler mentions, of 16 companies in seven countries, from which they have sourced consumer drones. However, they also have resourcing that many other organisations may not have, so that is also an important consideration when we think about this issue.

Q172 **Chair:** And some more vulnerabilities, other than airports and airlines?

Dr Jackman: Yes. One important vulnerability is around big political gatherings and events. So, in terms of non-battlefield kinetic drone instances, as we saw in Venezuela in August last year, the President was speaking at a military parade and a C4-laden drone was released and remotely triggered and it was widely reported as the first assassination attempt by a drone using a commercially available platform, albeit an expensive one, and a second one was then detonated nearby.

So I think these sorts of sites, where we see political or military leaders, are a very obvious kind of—

Q173 **Chair:** Large numbers of people.

Dr Jackman: Yes, and I think that crowds are a really important thing to think about. For example, we have seen drones fitted with nationalist banners over football matches. At the Serbia and Albania qualifying football match in 2016, a drone was released there. And that can cause aggravation and chaos below. Although we can talk about payloads and what we might put on to a drone to cause fear, with even an ambiguous payload if you are not sure what is coming out of it and an agent appears to be released over a crowd or large event, that could cause a stampede, which could cause chaos below and all kinds of injuries.

Q174 **Chair:** Shall I move to Arthur now? How big must a drone be to be involved in spraying liquid, like crop-dusters for example?

Arthur Holland Michel: It depends how much liquid you want to spray.

Q175 **Chair:** Enough to terrorise a crowd and make it think that something terrible was happening.

Arthur Holland Michel: In theory, you don't need a very large drone to achieve that effect; you have a small spray system. The crop-dusting drones that exist commercially are very large, very expensive and very much controlled, but I don't really believe that you would need something of that level in order to achieve that effect.

I will just add on the threats front that while we are focusing on drones in the kinetic sense, they have also proven to be very effective in Syria and Iraq, in the hands of ISIS, for battle management. For example, ISIS has used drones to guide vehicle-borne IEDs more accurately to their targets.

Q176 **Chair:** So the drones actually control the vehicle?

Arthur Holland Michel: No. There is an operator who's over the city; they have direct eyes on the target and they can communicate with the driver. ISIS has also demonstrated a capacity to use drones for battle preparation. There was a successful assault on a refinery, for example, and in the days leading up to it there were a number of drones doing reconnaissance. They achieved great kinetic effects, thanks to unarmed drones.

Q177 **Chair:** In terms of hardening the UK against the use of drones by terrorists or other disrupters, what do you regard as the vulnerable points here, other than the ones we've discussed?

Arthur Holland Michel: Any facility that is accessible from the air, that is in the open. I have heard threat analysis that if you have an F-35 fighter jet on the deck of an aircraft carrier, and a small drone with a small explosive payload lands on one of the wings and detonates, you may not cause any human harm but you have certainly caused a great deal of property damage. I would not rule out any facility that, as I say, is visible from the sky.

That is very much democratising, in a sense, because I would not say that there are some facilities that are visible from the sky that are more

hardened than others, if that makes sense. That is a common vulnerability across the board.

Q178 **Mrs Moon:** Could you both expand on the issue of the non-kinetic malicious activity that drones can undertake? You talked about the concept of the banner, and of looking ahead and seeing what the reconnaissance information is, but what other threats can they pose non-kinetically and how big is the threat that comes from them? Can you expand on that a little? I think we focus a lot on the kinetic threat and are perhaps being a little naive about the non-kinetic side.

Arthur Holland Michel: Certainly. I will give you another non-kinetic example. Russia has used small drones in both Ukraine and Syria, equipped with jammers, and cell-site simulators if you will, to not only interfere with communications among their adversaries, thus causing chaos and confusion, but also to disseminate false text messages directly to the cell phones of say, Ukrainian soldiers, saying, "You should defect. Your superiors do not care about you." That is another example of the sort of non-kinetic effect that could be very effective.

As Anna mentioned, you could land a drone with some political or terrorist messaging in a very prominent location and there would be significant public panic as a result. A good example of that that I would use is that in the lead-up to the World cup in Russia ISIS released a very rudimentary video of some CGI drones dropping bombs on some of the World cup stadiums. This looked like a high school computer graphics project and yet it made global headlines—people were talking about it. I can assure you that Russian security officials were talking about it, and factoring it in to their threat analysis. ISIS achieved that effect with a simple video. It is drawing on what I guess you might call the advertising power—the psychological power—of the drone.

One other non-kinetic effect that I might speak to is interfering with law enforcement operations. There is a precedent for this. There was an FBI operation in the United States where a group of agents who were conducting surveillance suddenly found themselves under a small swarm of drones that were both conducting surveillance of the FBI operatives and disrupting their operation. As I understand it, those drones were also live streaming the video they were collecting to the criminal organisation—

Mrs Moon: So, surveillance of the surveillance.

Arthur Holland Michel: Exactly. Sousveillance, if you will.

Q179 **Mrs Moon:** Anna?

Dr Jackman: We are seeing drones in surveillance capacities increasingly used by different protestors in different kinds of operation. We saw this as far back as 2013, when the German Pirate party flew a drone towards Angela Merkel in protest at her surveillance policy, but we are also seeing a resurgence more recently.

With Extinction Rebellion, earlier this year leaked documents showed that the climate activists were planning to fly drones around Heathrow airport in a sustained form of disruption, echoing the incident that happened at Gatwick. More recently, we have seen a splinter group, Heathrow Pause, arguing that they will do the same thing this month. We have yet to see whether that will materialise, but it is definitely something that is gathering attention. Previously, we have seen Greenpeace fly a Superman-shaped drone over a French nuclear plant and we have also seen the use of drones over a range of types of sensitive site to capture and communicate sensitive imagery. It might be politically sensitive sites such as the White House, the Colosseum and the Eiffel Tower, but also security-sensitive sites. In 2014, we saw 37 security breaches via drone over UK nuclear, naval and submarine bases, and embassies as well. You are seeing a changing way in which people are trying to use these platforms.

Also, I think it is useful, potentially, to flag racing drones using these small platforms in non-kinetic ways, just to complicate and confuse security at an event for example. It might be to divert attention, so you saturate the airspace above security at an event and then something else happens elsewhere on the grounds—that is to divert attention—but also, leading on from Arthur's point about the cyber area, we might see that cyber threat evolve and take a changing place in the discussion soon. The Department of Homeland Security in the US recently issued a factsheet on the UAS challenges to critical infrastructure, which speaks directly to many of the concerns that you have raised today, in which they talk about drones as a threat to intellectual property—they say that drones may be used to capture sensitive information.

As Arthur talked about, there are already companies that make drones designed to conduct a cyber-attack. We see these in the UK and in Israel as well—drones to conduct active cyber-attacks to intercept phone calls and data from smartphones.

But one of the more interesting things I wanted to raise was a scale question and an accessibility one. Some of the cyber-capabilities are not readily accessible or available. They are quite limited in who might have access to them. What we are seeing, as in the wider drone landscape, is a kind of DIY response, where individuals are building their own takes on these capabilities. There is one project, Project Cuckoo, that is an off-the-shelf-parts wi-fi sniffer drone. An individual has essentially said that he built the platform using freely available parts and put together a drone that he could place where it shouldn't be to, in his words, "conduct electronic surveillance or even active attacks" of a wi-fi network. What we are seeing is that, while some of the capabilities are more readily accessible and others are not, there are DIY responses that are important.

Q180 **Mrs Moon:** In terms of disrupting a wi-fi network, would that be over, say, a building like this one or GCHQ? Is that what you are thinking of?

Dr Jackman: The factsheet from the Department of Homeland Security identifies particularly commercially or politically sensitive sites where interception of the data might be more desired, but those are arguably

some of the sites that counter efforts will be focused on, so I think it is a wider question than that. We have seen drones flying over commercially sensitive sites to gather information from the air, and there is no reason that they might not want to do that with this sort of wi-fi sniffer or hacker drone as well. That is definitely a discussion that is going on in those circles.

Q181 **Mrs Moon:** I think you underestimate how proactive the House of Commons can be at times, but there we go.

Can we talk about terrorist groups and what they have developed and how they have deployed drones in conflict areas? What can we learn from that? What have they done? How have they utilised them? And what do we need to learn about how they might use those in a civilian sphere? Are there lessons to be learned there?

Arthur Holland Michel: In answering your question, I would point to the threats that we have already enumerated, in terms of serving as a rudimentary cruise missile, a booby trap, dropping small munitions, propaganda, surveillance for battle space preparation and battle management and, perhaps in the near future, electronic warfare.

There is an important point that I want to make with regards to the terrorist use of drones, specifically as it relates to the domestic terrorist use of drones, if you will. The drone emerged as a favoured tool among international terrorist groups with the demonstrated capacity to have attacks within Europe about half a decade ago. Yet, to date, we have not seen one of these groups attempt to use a drone in a terrorist attack in the EU or in the United States. Why is that? I think that is an important data point. It would serve us well to spend a little time thinking about that.

My personal theory is that, while the drone is a very formidable and powerful technology, there are other tools for causing chaos, panic and death that are, at this point, more accessible, more effective and potentially cheaper.

Q182 **Mrs Moon:** Such as?

Arthur Holland Michel: An assault rifle, a vehicle—you rent a van—or a group of people with knives. If you try to get inside the psychology of a would-be drone attacker, you can kind of imagine the thought process: "Wouldn't it be great to use a drone to disperse a chemical agent over a stadium?" Then they see that actually, it may not be quite as easy as they thought, especially if they have no technical capacity and especially if they do not have the supply chains that we were talking about. But they could just rent a van and ram it into a soft target. That is going to change, no doubt, especially as our responses to those other types of attack become more robust, but it is something to think about. It speaks to where the drone is today. It does not speak to where the drone might be next year, the year after that or 10 years from now, but it is an important part of the threat assessment at this moment.

Q183 **Mrs Moon:** We have tended to talk in terms of the threat of drones that have the capability to carry some sort of payload. What about the microdrones that are being developed? What is the threat from those, particularly from a terrorist organisation perhaps operating in the UK? Instead of the larger drones, what about the very small ones? What is the threat there? Is it a realistic threat now or is it something for the future?

Arthur Holland Michel: That is still a pretty deep future capability. The British Army actually has a microdrone—it is called the Black Hornet. They cost $50,000 each as I understand it, if not more. They are pretty capable, but they cannot carry explosives; their range is fairly limited compared with a larger drone; and it is very difficult to buy them, even if you have the money. There are very few militaries that use them. They have not been incredibly widely adopted, which I think you can read between the lines of to say something about their capabilities, how effective they are and perhaps how reliable they are. That gives you a bit of a timescale, I think, as to when we may see them trickle down into the civilian domain.

If we wanted to get very sci-fi about it, potentially you could imagine someday using a drone to fly inside a building. Maybe it has a small tiny little explosive payload on it, so when it lands on someone's head, it kills them. That is the kind of thing that very much exists within the sci-fi domain. I do not think it has much bearing on the discussion that we are going to have about CUAS policy. It is perhaps a different security challenge, but you are right to be thinking a little deeper into the future.

Q184 **Mrs Moon:** I am thinking deeper into the future, because I have actually seen them operating in US development sites, so I know they are out there, and I know how small they can be. I am not a sci-fi reader; I am someone who has actually seen them in use.

Arthur Holland Michel: Keep in mind that if there is a strong gust of wind, they are susceptible to that. Their communications links are not going to be very strong. We have a lot of talk about them flying indoors or—I don't know—sneaking into Parliament, but RF links do not go through heavy thick walls, so they will not have a communications link; they will have to be autonomous. Well, autonomy is difficult. There are limitations there, as things stand today.

Dr Jackman: Many of the sensors that you need for those types of manoeuvres are weight-adding to those devices, and obviously, being so small, they can carry only a certain amount of weight. So there is a temporality issue there, as well as a more fundamental accessibility one.

Looking a bit further forward with those microdrones, one area that I think will make this an even more interesting conversation in the future is bio-mimicry—bio-inspired drones. We are seeing many research institutions, military and otherwise, investing in and developing bio-inspired drones that look like birds or insects, and that function and move in different ways. They are inspired by different sets of design principles. These, I think, will sit differently in our environment. You don't necessarily know what you are looking for if a drone appears to look like a bird or a small

insect, so this is something that will change the appearance or morphology that we might expect to be associated with a drone.

May I return to your previous question about kinetic threats? One point that I really wanted to make today was around taking seriously the DIY space and people who modify drones in their garages and homes. We are seeing a lot of weapons-based modification in the United Kingdom, the US and beyond. People are adding flamethrowers, semi-automatic handguns, paintball guns, BB guns, functioning chainsaws and 80,000 V tasers—all those types of weapons—to drones. While many of these experiments are done playfully—people make YouTube videos about them, just to see what's possible; they are attracted to that spirit of creative experimentation—there is a growing online resource to suggest, "You could add this chainsaw on to a drone and it works", or "You could 3D-print a gun and add it on to a drone and it fires." I just wanted to flag that, and the resourcing online that goes with it, because I think the online space is one that we should pay a lot of attention to, in terms of mapping out our threats, and we should keep an eye on how these ideas travel.

Q185 **John Spellar:** Presumably, all of those are added weight, so you require a steady growth in the size of the drone to carry that.

Dr Jackman: Yes.

Arthur Holland Michel: There are advances in carrying capacity as well. A research group from Stanford released footage last year of drones that can carry 40 times their weight—a drone about this large that can open a door. That, again, gives you a sense of how that barrier is also falling.

Dr Jackman: The people who add these sorts of things to drones often build the platforms from scratch. You see people who have a certain level of technical literacy and expertise building drones that can carry people, huge crates of beer—all kinds of things. It is possible to make these things with commercially available parts, so it is a question of building your own platforms or modifying existing consumer ones.

Q186 **John Spellar:** True, but they all require a power source to be able to do that, which is surely a limiting factor.

Dr Jackman: The battery life is another barrier to entry, or a limiting factor, but again, as Arthur says, in the same way that you see developments in carrying capacity, battery life is a really investment-rich space; industry, universities and others are always trying to increase battery life. We are seeing some quite big advances there as well.

Q187 **John Spellar:** Where I am trying to get to with this line of questioning is whether there is a size at which it may be possible or sensible to impose restriction—to say, "You can have the smaller drones with much fewer restrictions, but if you go above this size or weight, there are a lot of prohibitions." That will not stop everybody, but it does narrow very much the availability of these. As you add these various capabilities, they add weight and therefore require extra power, and that adds weight as well.

Arthur Holland Michel: My sense is that things are moving in the opposite direction, and that every advanced airspace authority in the world is exploring ways to bring larger drones into the airspace system, because that will enable a growing number of applications, including long-range inspections, cargo, emergency, medical deliveries, and let us not forget Amazon deliveries. The economic push to integrate the largest possible number of drones, and eventually drones of a larger size, is so strong that it would be difficult to push back against that.

Q188 **John Spellar:** True, but we have a large number of automatic weapons in this country, licensed, in the hands of the police and the Army. We also have enormous restrictions on their ownership by anybody else. That does not mean that there are no automatic weapons, but unlike in the United States, for example, they are much more limited. Is that where we ought to look?

Arthur Holland Michel: Automatic weapons cannot be used to deliver emergency kidney transplants. That is something that I think the drone industry might convey to you as the flipside to that argument. The discussion that you are seeing happen about larger drones is that if the industry can prove that large drones can be integrated into the airspace in a safe way, the airspace authorities will allow that to happen.

Q189 **Chair:** I don't think that is the end of the spectrum that we are so worried about, because those would be primarily, if not exclusively, in the hands of legitimate enterprises. What we are trying to get at is: is there any way in which people with malicious intent can be carved out from getting access to these potential delivery systems of disruption and destruction? Would size would be a relevant factor in that, or would one need to have a more across-the-board ban that says, "You can only have access to these things if you are licensed to do so"?

Dr Jackman: That is an excellent question with a tricky answer. Some of the threats and risks we have talked about show that drones of different sizes can be used with different purposes. It may be that smaller drones are used together to try to overwhelm the space, or to confuse—just to buzz around someone's head. If you have ever had that happen, it is really annoying, so you can imagine that if you are a security force member, that is a tricky issue. It is not necessarily a size issue, but it does not stop it from being used in a threatening or risky capacity.

The issue of access is a second part to that; there is a supply chain question. The drone researcher Don Rassler has done some excellent work looking at supply chains. While the current UK initiatives that are publicly discussed are predominantly focused on providing regulation information at point of sale in certain high street shops, there are many other ways that you buy drones—predominantly online, but also the second-hand drone industry is massive. I buy most of my drones second hand, because I crash them quickly. I am not a very good flyer—that is not necessarily something I should admit here.

Those sorts of avenues are under-appreciated as potential ways for people to access these platforms. The UK Government are doing things around registration, to try to help with identification, but this is a question for people who just do not comply, which makes it more complicated. I do not think that size is everything.

Chair: We promised that we would go into the question of counter-drone technology. Madeleine, I think you have another question on that.

Q190 **Mrs Moon:** I wanted to ask about the current capabilities to detect, track and identify counter-unmanned aerial vehicles technology. Is it adequate? What do we need to do to improve it? What are the glaring gaps?

Arthur Holland Michel: I will speak to that. I think it is safe to say that countering drones remains a technical challenge that has not been completely overcome by anybody.

I will speak to the detection and tracking element and the identification element. Very briefly, if you wish to detect a drone, you have a number of avenues available to you. Radar is a common one; cameras, either daylight or infrared; acoustic sensors—they are basically microphones that listen to the specific acoustic signatures that drones emit. Radio frequency sensors detect when a drone is emitting a particular type of communications signal. Electronic ID depends on drones being co-operative in broadcasting who they are, where they are and who the operator is. The combination of systems—that is, counter-drone units that have a radar, a radio frequency sensor and a camera—is popular, because no single detection system will be failsafe in every single environment. That speaks to the key challenges.

False negatives and false positives are a big problem. You are talking about the airspace, which is very crowded. There is a lot of interference, and you cannot necessarily have 20 people vetting a system every time it buzzes. There is radio interference, particularly at airports; if you are trying to sniff out the radio emissions of drones, airports are very spectrum-busy environments. Even something such as the weather can make it more difficult to track a drone. Then there is the question, once you have seen the drone, of how you know whether it is malicious. As we will see when I speak to the interdiction elements, sometimes a drone is safer in the sky than it is when you are trying to shoot it down, because it has to go somewhere.

Not only that, but how do you decide how to respond to the drone with enough time? A drone that is available today can fly at, say, 25 metres per second. If you have a detection range of 750 metres, which is pretty good, you will have 40 seconds—or less, 30 seconds—until that drone is right over your head. When I say detection, I really mean detection and identification, so you detect it, you know that it is there and is a drone, and you have a lock on its position. In that time, you have to make what is, in some cases, a very high-stakes decision, especially if you are talking about a large crowd. That is a drone that flies at 25 metres per second.

What about a drone that flies at 90 metres per second? That challenge is all the more difficult.

You cannot necessarily tell where the drone operator is with all these systems, which is a challenge if you want to catch them and put them through a judicial process. That was certainly the case at Gatwick; we still do not know who the operators are. Drones can be flown in certain ways to make them more difficult to detect. If a drone is hovering, it might be harder to detect with a radar, for example. There is also the privacy element; there may be limitations in terms of the kinds of sensors that you can use with drones, because they could collect personally identifiable information.

I will speak briefly to the interdiction element—taking the drone out of the sky. You have a few options: jamming the communications link, nets, spoofing, which is somewhat similar to jamming but allows you to redirect the drone, lasers, microwave, projectiles—shells, bullets, things of that nature—collision drones, which are drones that you fly kamikaze-style into the offending drone, and dazzling systems, where you dazzle the sensors with a very bright light source, so that the drone is essentially blinded.

What are the interdiction challenges? Generally, the more effective a system is, the less safe it is. It would be nice to shoot lasers at every single drone that appears over Gatwick, but those drones have to land somewhere, and that is very dangerous in a congested area. Not all the lessons that we have learned from the battlefield deployments of counter-drone systems, which have been extensive at this point, are directly transferable to the domestic space. There are certain things that you can do in the battle space that you cannot do here. The MoD has a system, the AUDS, that has actually been installed at Gatwick. The company claims it has had 2,000 successful drone intercepts in battlefield use, but I can assure you that not all those intercepts would be viable at Gatwick airport, because you are talking about a civilian environment and you cannot interfere with all the communications that are happening.

I will make a last couple of important points on this. There have been a number of exercises, and the people I have spoken to who have seen those exercises have said that the counter-drone systems are really good at addressing a small number of scenarios that they have been designed around—say, a single drone coming at you with explosives on. But the second that you get creative and expand the variety of scenarios—this is all speculation, but say the drone is flying at very low or very high altitude and coming down at you, or there is a change in the number of drones—the market really starts to show its immaturity.

Then there is the fact that this is an immature market, and there are a lot of people trying to get into the market. When I started doing research about drones, everyone who called me up would say, "Arthur, what can we use drones for? Can they do deliveries? Can they walk my dog?" Now, everyone calls me up to ask, "Arthur, how do we shoot them down?".

As there is so much interest in the field, there are hundreds of products on the market. When I did the report that I mentioned earlier, which came out last year, there were 230 products on the market. I am coming out with a new edition of that report in the next couple of months, and I would say that there will be close to 400 systems on the market—not that all systems are created equal; there might even, dare I say it, be some snake oil in the market.

Then there are the countermeasures to the countermeasures. You start deploying a counter-drone system, and your adversary wants drones so badly that it will start innovating to get around your system, finding the vulnerabilities. There are ways to do that as well. That is a quick survey of where I think we stand.

Q191 **Mrs Moon:** You were going through jamming, nets, lasers, microwaves, collision and dazzling, but maybe we should think satellites. Those are all words used when talking about management of satellites and satellite weaponry. Is there any link between those markets and the technologies that they are developing?

Arthur Holland Michel: For countering satellites?

Mrs Moon: Yes.

Arthur Holland Michel: As far as I understand it, no, except perhaps with regard to directed energy and lasers. There has been some talk about countering satellites with lasers, but you need a much more powerful laser to reach those kinds of altitudes, and directed energy is very much still an emerging technology and somewhat untested. But that is the extent of it—I could not speak to any other connections.

Mrs Moon: Thank you.

Q192 **John Spellar:** When we write our report, we will make all sorts of recommendations to Government. What areas in the counter-technology should they focus on developing in order to advance it?

Arthur Holland Michel: What you hear in the world of counter-UAS is that—this is a cliched term—there is no silver bullet. No single system has yet proven itself to be the one that we should put all our chips on. Jamming is the most popular technique at the moment, and it has proven to be one of the most effective ones, but as soon as drones do not have a communications link, your jamming systems will have no worth against them.

The strategies that I have seen are very much multi-tiered, with a diversification of approaches. You see that, for example, in the NATO strategy. It is funding not just one type of technology, but a number of parallel initiatives. In a way, throw a lot at the wall and see what sticks. There are historical parallels for that. We saw that in the early years of anti-aircraft warfare, for example, when there were all sorts of things—the parachute and cable, or the barrage balloons—and more recently in the counter-improvised explosive device efforts, when a lot of technologies

were tested. As you iterate, some technologies start percolating towards the top, but I am still not at a point where I think we can make bets on which technology will do that now.

Q193 **John Spellar:** We have talked about a number of the technical challenges, but are there any issues with the legal environment? Are there areas in which we ought to suggest a revision of legislation, whether to prohibit or inhibit activity, or to enable counter-activity? Do we have any artificial inhibitions to our abilities in the legal system?

Arthur Holland Michel: A European Commission-funded programme called ALADDIN 2020 is developing a counter-UAS system. It did an analysis of European countries' laws with relevance to CUAS, and that included the United Kingdom. It identified a number of laws that could be used as both legal cover for CUAS activity and, as you say, to inhibit use of CUAS, including the Wireless Telegraphy Act 2006 which bans jamming, the Electromagnetic Compatibility Regulations 2016, and the Investigatory Powers Act 2016.

What you will notice is that all of those laws generally precede the widespread dialogue that we have seen in the last couple of years on countering UAS, which means that they do not have provisions specifically relating to CUAS and, also, the exceptions that those laws carve out—for example, the exceptions to the Wireless Telegraphy Act 2006 that say you can't jam unless you are, for example, involved in some kind of law enforcement operation—have not yet been tested legally against CUAS operations. We are operating a little bit in an unknown space and it is a little hard to tell at this point whether that provides sufficient legal latitude and cover for CUAS operations, in my opinion.

Q194 **John Spellar:** That's quite helpful. Could you send us a bit more detail on that?

Arthur Holland Michel: Certainly.

Q195 **John Spellar:** You seem to be nodding at us, so do you want to cover that?

Dr Jackman: Yes, I think Arthur did an excellent job of summarising that. One thing to add is that the MoD is clearly doing really excellent work here through the launching of their £2 million fund into the counter-drone space.

A couple of recommendations that spring to my mind from that are around it being a multi-pronged approach that isn't just about the technology itself. While I think it is really important to invest in testing facilities where you see technology undergoing testing in our weather conditions and environments, and to have some transparency about what the results of those tests are, because it is actually very difficult to find lots of data around many of the counter-drone systems and how effective they are, we should also be learning internationally, for example from the US, about communications initiatives. The Federal Aviation Administration, the US airspace regulator, recently issued a statement around the adding of

weapons to drones, saying that this clearly contravenes a particular section of the FAA Reauthorization Act of 2018. This type of communication addresses this issue in a different kind of way, taking a communications approach.

Lastly, we should be thinking about the mapping of risk and threat as something that is really important and informs how we see the counter-technology. As Arthur said, if you test counter-drone technology with a very prescriptive set of scenarios—you assume that this is the way the terrorist or the non-state actor will use the drone to inflict harm—you just need to get a little bit creative and use different emerging capabilities to test in different ways to realise that a differently-thought risk assessment, which pays attention to DIY actors and creative actors as much as to existing battlefield and wider kinetic issues, is really helpful. The Department of Homeland Security runs a kind of initiative that is as interested in risk mapping as it is in the counter-technology itself. I think that is something that we could learn from.

Q196 **John Spellar:** You mentioned the work that the MoD has done and we are very much aware of that. In your assessment, is Government joined up enough to actually use that in real time? The experience of Gatwick would seem to indicate some weaknesses in the emergency operation of Government and, indeed, of Cobra. What is your assessment of it?

Dr Jackman: Completely coming at it as a researcher and an outsider to that environment, in undertaking my own research into the future drone city, which is a research project I am running, I work with police officers, different types of security practitioners and the commercial drone industry to understand how our airspace is changing. In that capacity, I have had different conversations with a lot of different organisations and individuals around drone threat. Many of them are very quick to talk about the risk that they see, but it does appear at times that some of the efforts are a bit piecemeal and are not necessarily best connected. There are some really interesting things that the UK is doing—both the MoD but also the Ministry of Justice, through its prison drone squad, which is looking at the issue of smuggling into prisons with drones—all of which I think could be better centralised and connected, perhaps through a more centralised working group, for example.

Q197 **John Spellar:** Okay. This is my final question. You mentioned the work of the Federal Aviation Administration and the Department of Homeland Security in the US. Are there other countries where we ought to be looking at the work they undertake in this field?

Arthur Holland Michel: There are a couple of other places where work is happening in this space. I should add a caveat to all this, which is that there is an abysmal lack of transparency with regards to CUAS. I have gone to so many manufacturers and said, "Has your system been used for any successful intercepts in real operations?" They say, "Yes, of course." I say, "Can you give me an example?" They say, "No." That hinders information sharing, and our sense of what works and what doesn't.

Having said that, NATO has a working group specifically focused on these issues. The FBI has done several CUAS deployments. Again, it has not released information publicly about that, but any large, prominent event in the US now will have a presence by the FBI CUAS team. Israel is at the forefront of the deployment of CUAS. There is little public information about this, with one notable exception. During the recent Eurovision contest in Tel Aviv, the Israeli police had an extensive deployment of a CUAS team, involving hundreds of people, which gives you a sense of the labour-intensiveness of the technology. They had a number of successful detections and intercepts. They used Chinese Hikvision jamming rifles and they seem to be disposed to speak publicly about that operation. That is one good place to see what works and what does not.

However, I should note that in conversations that I have had with people who work on this, one of the problems that even operational folks are coming up against is that there is a dearth of information, because there has not been a terrorist attack with a drone in one of these environments in the west. Whereas we are pretty well prepared to deal with suicide bombing attacks—because many have happened in the past, so we have a wealth of data as to what works and what does not—we have not had a single UAS attack that we can draw upon. Gatwick is a notable exception, but, of course, it was not a kinetic terrorist attack. That leads to a scary conclusion: this will get better once there are attacks. Of course, we want to prevent them before they happen. That is the paradox that we are operating within at the moment.

Also, the European Commission is doing quite a lot of work on CUAS. They have a high-level conference on CUAS in October in Brussels. I can pass you information about that, if it is of interest.

Q198 **Chair:** But we know that the British Airline Pilots Association, for example, has long been worried about the capability—I think we can say unique capability—of drones to bring an aircraft down, in a way that other systems could not. Of course, the technology to do what al-Qaeda did on 9/11 existed for a long time before they actually did it. Presumably you are not suggesting that we have to wait for a disaster of that sort before we try to head it off.

Arthur Holland Michel: No, I am saying that that is a headwind to work against and the policies have to keep that in mind. I think that workarounds to that are, for example, thorough technology forecasting and thorough technology literacy—knowing how the technology works, and what it is and is not capable of—so that the policy is well directed at the technology as it exists today and is also future-proofed against future iterations of the technology. Those are the kinds of measures that I think could get around that.

Chair: I am trying to understand the way in which the terrorist mind works, as well.

Arthur Holland Michel: Absolutely. A good CUAS team knows all the scenarios that the adversary has in mind for how to use a drone, plus one.

Q199 **Chair:** Finally, Anna, I have one last question. Is there sufficient danger in the malicious use of drones in the UK to justify restricting their use to licensed operators? By all means, take the opportunity in your closing remarks to address any questions that you think we should have asked but did not, which you would like to put on the record.

Dr Jackman: To briefly add to your previous point, in thinking about previous modes of attack that did occur and the question of whether a drone attack will occur on a certain scale in Europe, a Met police officer was quoted in a *Financial Times* article earlier this year as stating that two potential attacks via drone in an unspecified European country had been thwarted by the security services. While they may not have been actualised on that scale, there is information that suggests that they could have been.

When we think particularly about the risk of drones near aircraft, the way that hobbyists and other individuals think about drones is changing. You are seeing that, in people's appetite to test and see how far those platforms can be pushed, hobbyists, for example, are flying drones at record heights. We have videos on YouTube that suggest that they have been flown nearly 10,000 feet in the air. There is a way in which our imagination around what drones can do, or even just in terms of testing them, could be dangerous, and that should be considered.

In terms of your question about sufficient danger and licensing, that is a really tricky one, because the steps towards drone registration in the UK are important. Trying to increase visibility and knowledge of what is in the air and where is really important, and I absolutely support the Government's position on that. The question of danger and licensing comes down to conformity and adherence to the law. If I was going to use a drone in a malicious way, I would not particularly care if there was a licence or not—it would not be a question that entered my mind; I would simply not license the drone. The issue then becomes how you tackle the non-conformity—

Q200 **Chair:** Sorry, I should have refined that question. Basically, it would say that you could not own or possess a drone without a licence. Does that make it—

Dr Jackman: I think that makes it a more interesting question. It is also then about how you actually enforce it. For example, the reason I pointed to those second-hand drones that you can access on Facebook Marketplace and on Gumtree—

Mrs Moon: Or car boot sales.

Dr Jackman: Yes, or car boot sales—all sorts of things. In spaces that are less visible in terms of point of sale initiatives, you would still have the same issue. There is, for example, the analogy that cars are licensed but are still used as weapons or weaponised in different ways. Licensing can help, but the issue of non-conformity, to a certain extent, makes that redundant.

Q201 **Chair:** Arthur, do you have any final comments or any comments on that particular issue? For example, a strict licensing system, as in the case of a firearms licence, would presumably make it an offence to pass a drone from a licensed holder to an unlicensed one.

Arthur Holland Michel: I guess it comes down to an analysis as to whether there are threats inherent to the drone that are not inherent to other technologies that are eminently accessible or regulated under different regimes and modalities.

Q202 **Chair:** That is why I have been focusing so strongly on the bringing down of aircraft, which is the thing that drones can do much more easily than anything else.

Arthur Holland Michel: I think it remains an open question. It is a question that should really be answered only through a collaborative multi-stakeholder dialogue. The groups that are involved, for example in the integration of drones into the airspace, are vital to the counter-UAS discussion. While they are talking only about co-operative drones, that is still part of the full ecosystem of how to keep airspace safe. The industry is also very valuable, because it has the technological expertise. I believe that all those groups have more in common than they would perhaps initially let on.

Q203 **Chair:** Are you saying that if we reach out to the hobbyists and the enthusiasts, they would actually co-operate in trying to work with the Government to ensure that terrorists could not get hold of drones?

Arthur Holland Michel: Absolutely—by all means. Not to speak too much on their behalf, but seeing a devastating terrorist attack with a drone will have a tremendous whiplash effect that will be harmful to the drone industry and to all the hobbyists as well who have only positive intentions for the technology. It has been my experience that they are all eminently willing to participate and contribute to the discussion. I always encourage discussions to be as diverse as possible.

Chair: Very good. Any final comments or is that it?

Arthur Holland Michel: No, I think that is everything.

Chair: I thank you both for an extremely well-informed session. We have learned a great deal from you, and we will proceed with our inquiry in a far stronger intellectual position than we were in an hour and a quarter ago. Thank you both very much indeed.