COUNTERING DRONES

THE LATEST INSIGHT INTO
COUNTER-UAS SECURITY EFFORTS

SEPTEMBER 2016

GLOBAL LAWS

HOW NATIONS ARE ADAPTING LAWS TO CONTROL DRONE USE

SURVEY RESULTS

FIND OUT WHAT BUSINESSES THINK OF COUNTER-DRONE TECHNOLOGY

NEW COUNTER-UAS RESEARCH FROM MITRE

CORK AIRPORT'S AWARENESS EFFORTS

COUNTERING DRONES

The Emerging Threat: identifying, measuring and preparing for the security implications of civil and commercial drones

Estimated at around $127 billion, the 'drone revolution' is booming. But amongst the optimism is a creeping concern about the security and safety threat that this technology presents to critical national infrastructure, homeland security and a range of commercial sectors.

In response to this threat, various counter-drone defence systems are being developed by government and industry and it is predicted that this technology will begin to play a significant role in facility security systems as the use of civil and commercial drones becomes commonplace. But, for now, there remains a great deal of known knowns, known unknowns, and unknown unknowns for security professionals and sectors most vulnerable to drone attack or intrusion.

It is in this context that *Defence IQ* will host its inaugural **Countering Drones** conference this December to provide an opportunity for a security experts from a diverse community of sectors to ensure that they can guarantee the security of their assets and public safety for the future. This special edition magazine offers a look at some of the latest research and insight into the efforts being made worldwide., all of which will be discussed at the event..

CONTENTS

NO DRONE ZONE

When ignorance becomes a threat to security

WORDS RICHARD DE SILVA

It seems safety and security incidents involving drones are now a weekly – if not daily – occurrence in the press. August, for example, saw a reported 'near miss' of a commercial UAV and a Flybe passenger aircraft carrying 62 people in Cornwall, UK, only weeks after a report revealed a similar incident at Stanstead Airport in May involving a Boeing 737 and a privately owned drone. The same month also saw 'the first fatality linked to the non-military use of drones' in an incident at Wandsworth Prison in London.

The risk is not just a problem for the UK. There have in recent days been reports of a drone crash at the Koeberg Nuclear Power Station in Cape Town, and a near-collision between a drone and a police helicopter in Edmonton, Canada.

While this year's **Countering Drones** forum will be providing a dedicated focus on the technologies and legal implications surrounding drone countermeasures for at-risk sites, it will also be offering scope on the efforts to raise public awareness on drone regulations so as to lessen the risk of negligent incidents. After all, massive financial and

'Massive financial and physical disruption can occur even when an operator is not actively trying to cause chaos'

physical disruption can occur even when an operator is not actively *trying* to cause chaos, as some of these latest cases can attest.

Taking, as example, the situation of the commercial aviation industry, an incident involving an aircraft could indeed be catastrophic, while the wider impact this would have on an aerodrome and the industry would be considerable.

"If we were to focus on rogue drone users – drone users unaware of regulations, training, and so on – these type of reported incidents at airports are proving to be more of a nuisance," says Nathan Wall, the Airside Safety Lead at Cork Airport.

"For the aerodrome or airline it means that if a drone is reported within a 'NO DRONE ZONE', close ➡

to an airport or approach/departure route, aircraft could be advised to go into a holding pattern until the area is deemed safe for the aircraft to travel through. This has a financial and economic impact, because the aircraft has to use more fuel while more time is required from the crew due to the delays, therefore possibly costing the airline more. For the aerodrome, you are looking at further flight delays due to aircraft being unable to take off or land. There is also the factor then of a bigger workload on ground staff, ATC controllers and airline crews.

"Take a recent incident in Dubai airport in June: the airport was shut down for an hour and a half due to drone activity near the aerodrome. The impact on flight operations to an airport the size of Dubai is huge, as well

'Dubai had 90 minute schedule delays on their operations due to drone activity shutting the airport down'

as the impact on the airlines. They had 90 minute schedule delays on their operations due to drone activity shutting the airport down and impacting on passengers due to arrive and depart."

Wall is at the forefront of European awareness on the dangers of commercial drone use, spearheading a campaign to inform people that all drones over 1kg must be registered and that a ban now exists on drone use within 4.5km of Cork Airport – a campaign that will soon extend

Cork Airport is the first to see Ireland's No Drone Zone campaign

to the rest of Ireland's airports. Between January and July of this year, the Irish Aviation Authority (IAA), the body responsible for air safety regulation, has investigated more than 20 complaints about potentially hazardous drone flights.

"The Drone Awareness campaign has been a huge success," Wall says, citing the fact that the method of placing signage around the airport that advises the public that the area is a NO DRONE ZONE has spread wider across the Cork community, even forming discussion among people not involved in aviation. Social media has also played a useful role in promoting the cause. The success surrounding the campaign was a joint effort between the airport authority, Irish Aviation Authority and based airlines at Cork Airport.

Since this campaign was launched on 26 July, three incidents have been reported by members of the public and by light aircraft training pilots of drone activity within the controlled airspace. Wall and his colleagues aim to assist the IAA in extending the visibility of these regulations. He sees the biggest security gap to be ignorance: people buying or operating a drone without knowing the regulations or the impact on safety and security if trying to fly one near to an aircraft or airport.

Indeed, _Defence IQ_'s research has indicated a distinct lack of communication and understanding surrounding these regulations at a global level, in spite of many countries having introduced drone rules (even within the past year).

"We are getting there but it will take time," Wall admits. "I would like to see every civil aviation agency produce an IOS or Android App in regards to Drone awareness 'dos and don'ts'. This app could include the NO DRONE ZONE in each country and regulatory information. I don't think the communication piece is failing, I think the fact that the drone market has increased so much over the past two years, that we have simply seen a huge increase on the numbers of drones being purchased."

Awareness action may well make a difference in the coming years. However,

'The question is whether technology or procedure can do a good enough of a job on this front before a serious 'attack' is launched'

beyond the problems relating to simple ignorance and negligence, there of course remains greater security concerns surrounding those who will look to actively break the rules with malicious intent. When it comes to a site like an international airport, a number of measures are currently being considered to counter these vehicles quickly and safely when regulation alone fails. The question is whether technology or procedure can do a good enough of a job on this front before a serious 'attack' is launched.

"From purely a safety point of view, Cork Airport personnel are testing a drone watcher app on Android," Wall says. "We have made our staff more aware about drone activity and we have completed a drone escalation SOP (standard operating procedure). Counter-drone technology is evolving monthly, so airports will have to look at these options, but the high cost of

some of the equipment or solutions remains a huge concern for airport authorities."◾

Nathan Wall will be just one of the speakers at this year's Countering Drones conference, taking place in London, UK, on 6th-8th December 2016. Also among the panel will be: the Deputy Commissioner for Intelligence and Counter-Terrorism New York Police Department; the Secretary General of Defense and National Security for the French Government; the Commissioner for the Correctional Service of Canada; the Aviation Security Operation Centre Manager from the Israel State Security Division; and the National Coordinator for Security and Counterterrorism for the Netherlands Ministry of Security and Justice. More information is available at www.CounteringDrones.com .

COUNTERING DRONES

US grappling with counter-UAS technology challenges

WORDS RICHARD DE SILVA

As *Defence IQ* has recently reported, the rising number of criminal and negligent incidents involving civilian unmanned aircraft systems (UAS) is pushing harder on the need for a greater awareness of the potential dangers to the public. However, in many cases, awareness is just not enough. The progress of UAS technology requires a tandem attention to the progress of counter-technology – effective and safe methods of neutralising these vehicles when they become a threat, particularly to vulnerable civil sites.

Much of this process is being made in the United States, where the Federal Aviation Administration (FAA) has, as of August 29, released a rule to allow for the use of small UAS within national airspace. To get a better perspective on how this technology is moving forward, we caught up with Andrew Lacher, UAS Integration Lead and Research Strategist at technology R&D centre the MITRE Corporation, ahead of his brief at the **Countering Drones conference** (08-09 December; London, UK)…

Defence IQ: Mr. Lacher, let's look at the real threat situation as far as commercial unmanned systems are concerned. Are drones a serious concern at the moment? Or is it more a growing problem that hasn't yet seen a need for serious 'countermeasure' technologies?

Andrew Lacher: Well, it's being taken seriously but I don't think the answer is that simple. It's a complex situation because the threat ranges from inadvertent operators –who may create a nuisance or a hazard with their operations – to a malicious actor who might be intending harm. Now, there have been no significant incidents among domestic UAS in terms of malicious actors intending harm, but there have been incidents where people have been using UAS for criminal purposes, such as smuggling items across a boundary, whether it be across a border or into a prison.

There have also been a number of unauthorised UAS systems blundering into areas and creating unsafe situations. So I think what the community is seeing are indicators of a troubling trend, and they're trying to get ahead of that trend. So, yes, people are taking it very seriously.

I believe there is a notable demand in the community for counter-UAS technology to address the potential growth in unauthorized UAS operations. There are lots of vendors developing solutions in anticipation of this interest. The community itself consists of organisations worried about their own security and private security organisations as well as government agencies from local law enforcement, federal law enforcement, and the U.S. military for force protection, both domestically and overseas.

DIQ: That's okay, there seems to be enough taking place just in the civil airspace… ➡

'The boundary between a safety and a security concern is hard to draw'

Andrew Lacher

AL: And the civil airspace is a real concern. The boundary between a safety and a security concern is hard to draw. When you have an unauthorised UAS flying near an airport, it could be somebody who simply doesn't know any better or it could be someone who is intending harm. We don't know. In either case it's an unauthorised operation that raises concerns because of the many things at risk.

DIQ: I understand MITRE is focusing primarily on the situation in the United States, though correct me if I'm wrong…

AL: Right. MITRE's work in this space is primarily focused on the missions of federal agencies in countering civil UAS-related risks which include aviation safety/security, civil infrastructure protection, homeland security, and military force protection. We're also working with local law enforcement. Our work with

the Department of Homeland Security certainly brings us into contact with that element and with the first responder communities.

But we are actually thinking of solutions that may be arising from anywhere in the world. For example, we sponsored a challenge in August that had eight participants with systems we were evaluating in flight, using live airborne *simulated* threats. Those vendors came from all over the world – mostly Europe and the United States, but we also had participants from other regions. So, while our day-to-day work concerns the problems faced primarily from a U.S. federal government perspective, we're looking at a solution space that is worldwide.

DIQ: Obviously the solution space always needs to be cost-effective and while this does seem to be a fledgling market, is there a sense that the solutions being tabled currently are in fact cheap to run? Is that aspect progressing at the ideal speed?

AL: I would have to say there is no silver bullet technology out there, whether it be cost-effective or not, especially when you're considering a solution that will mitigate the operation of a UAS without interfering with other activities in a civil setting. There's no

'The concept of "cost-effective" is in the eye of the beholder with regard to what is at risk'

perfect solution. As part of our recent challenge, we were specifically looking at cost-effective solutions. But clearly, the concept of 'cost-effective' is in the eye of the beholder with regard to what is at risk. If you're worried about protecting a large high-risk area from intrusion, cost-effective means something different than if you're worried about protecting

a small facility where there's little risk. Depending on the importance, you may be willing to expend by quite a large amount of money. So it's all relative. There are some things that work, but they don't mitigate the most sophisticated threats.

DIQ: As you said earlier, in terms of those problems, at least when we look at the civil space, there's a need to ensure that any counter-UAS technology doesn't endanger the people it's trying to protect, or the assets it's trying to protect. Is that the biggest concern at the moment in regards to something that could affect how this technology is absorbed?

AL: Well, you want your solution to not create other problems whether it be a hazard to the same people you're trying to protect or whether you're using a solution that creates a widespread effect, such as jamming GPS. That could create a whole host of other problems for safety. In other words, we have to think of the trade-offs. We're worried about that, and there are a significant number of policy concerns, especially in the United States, where it concerns jamming and the authority to actually jam communication signals. That's a policy issue.

Even the notion of interfering with an aircraft in flight – that's against the law. Who has the authority to do that? Can federal law enforcement? Local law enforcement? Private security companies? Private citizens? Determining who has that authority means we have to work through some of those issues.

DIQ: At the most recent Farnborough Air Show, *Defence IQ* asked an FAA representative whether the desire to get regulations in place and ensure commercial opportunities for unmanned systems are moving forward would, in effect, outpace the ability to ensure we have the right security and countermeasures in place.

Do you think that's a risk?

AL: Well, one thing to consider is that new technologies enable a lot of things, positive and negative. Using an analogy, the internet is used by bad actors. Everything from child molesters to drug dealers use the internet for illegal purposes, but we don't ban the internet or stop its development.

'We shouldn't let the potential of bad things unduly constrain our ability to embrace the good'

The same thing is true with UAS. We shouldn't let the potential of bad things unduly constrain our ability to embrace the good. We do need to make sure that we can operate UAS in a safe manner and that there may need to be policies and procedures in place so we can ensure a high standard of security, but we shouldn't lock progress down because of that. As we do with the internet, we should prepare for the bad actors as well.

DIQ: And on the subject of the good things, where do you see the next few years in terms of the positive changes that will be made in this market? What's your ideal vision?

AL: In the United States, the first specific aviation regulation that enables the operation of unmanned aircraft has gone into effect from 29 August. It will enable small UAS – less than 55 pounds – to be operated in relatively rural areas – away from people but in line of sight of the operator. That opens the door to a whole range of potential applications. There's a lot of excitement now. Early on, I was personally involved with the development of that rule and I'm very pleased by its publication.

However, we in the US have much more progress to make. We need to find ways that we can expand the access of operating unmanned aircraft. We're opening the door now, but we need to enable access of UAS at night-time, near to people, and in urban areas. We need to extend the operational range beyond the visual sight of the operator on the ground. Things like that are the next steps to enabling even more applications. MITRE, as an organisation, is working very closely with the FAA on mechanisms to do that safely.

DIQ: Given that you'll be speaking at the Countering Drones conference (06-08 December; London, UK), is there anything that you're particularly interested in hearing from our audience on the counter-technology end, particularly as we'll have a lot of European perspective in the room?

AL: Firstly, I'm looking forward to sharing our work. I'm going to talk in general about our perspective on the challenge of countering unauthorised UAS operations but then specifically talk about the challenge we sponsored and the results from it. We'll in fact be announcing the results on 8 September.

I hope to get more information about other possible solutions out there, and what other organisations and oversight entities are doing to deal with some of the policy challenges with UAS operations. I'm looking for ideas and best practices from a policy standpoint, but also looking for technology solutions. About half of the participants in our contest were European, and I think there are a couple of reasons for that. For one, they may be able to test and develop technologies with greater ease because of different policy and regulatory environment. That may be one reason we're seeing great innovations coming out of Europe.

# 'I'm looking for ideas, best practices and technology solutions'

Andrew Lacher will be just one of the speakers at this year's Countering Drones conference, taking place in London, UK, on 6th-8th December 2016. Also among the panel will be: the Deputy Commissioner for Intelligence and Counter-Terrorism New York Police Department; the Secretary General of Defense and National Security for the French Government; the Commissioner for the Correctional Service of Canada; the Aviation Security Operation Centre Manager from the Israel State Security Division; and the National Coordinator for Security and Counterterrorism for the Netherlands Ministry of Security and Justice. More information is available at www.CounteringDrones.com.

COUNTERING DRONES
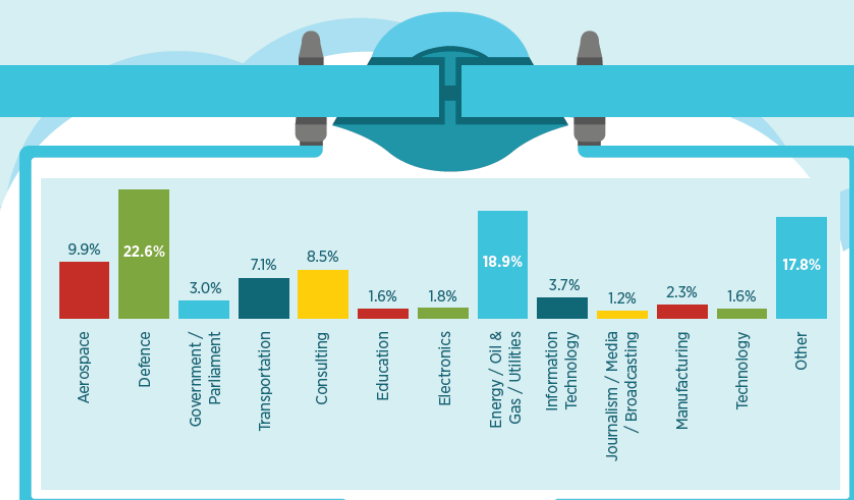
ARE YOU PREPARED FOR THE THREAT OF DRONES?

Defence IQ surveyed over 430 people with an interest in unmanned aerial vehicle/counter-drone technology developments. We asked them whether they believed the threat is really as serious as many suspect and if the commercial sector is ready for major security incidents resulting from drone-use...

Regions In Which Respondents Are Based

- 7.8%
- 14.1%
- 44%
- 0.9%
- 3.2%
- 12.0%
- 6.5%
- 8.5%
- 3.0%
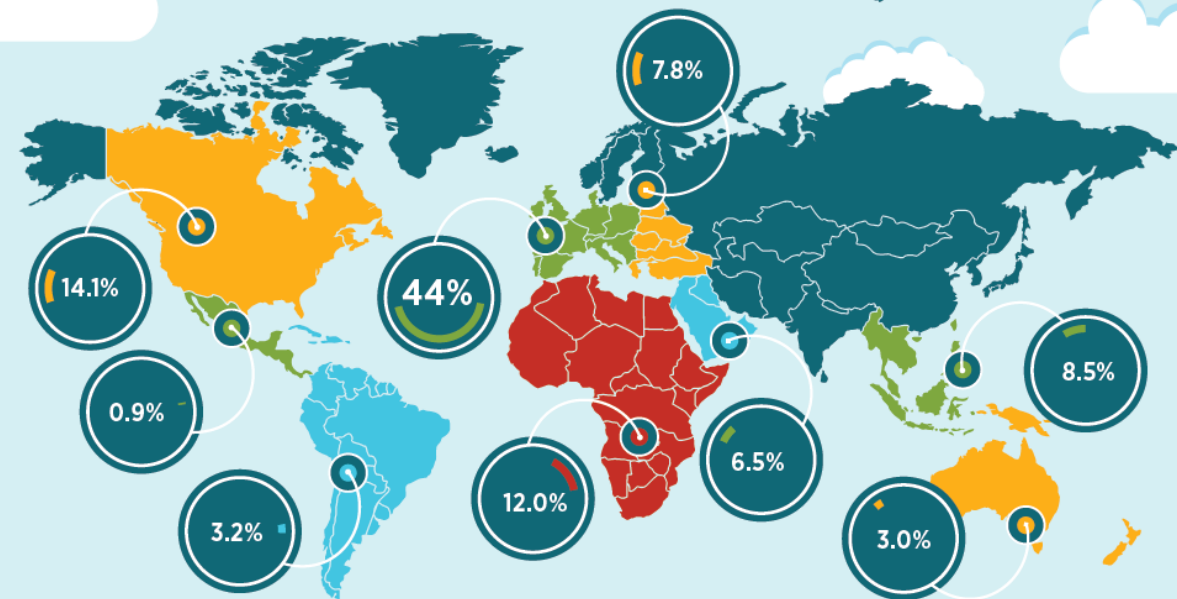
Those surveyed are primarily from Western Europe, but all regions are represented.

Sectors In Which Respondents Are Based

Aerospace	Defence	Government / Parliament	Transportation	Consulting	Education	Electronics	Energy / Oil & Gas / Utilities	Information Technology	Journalism / Media / Broadcasting	Manufacturing	Technology	Other
9.9%	22.6%	3.0%	7.1%	8.5%	1.6%	1.8%	18.9%	3.7%	1.2%	2.3%	1.6%	17.8%

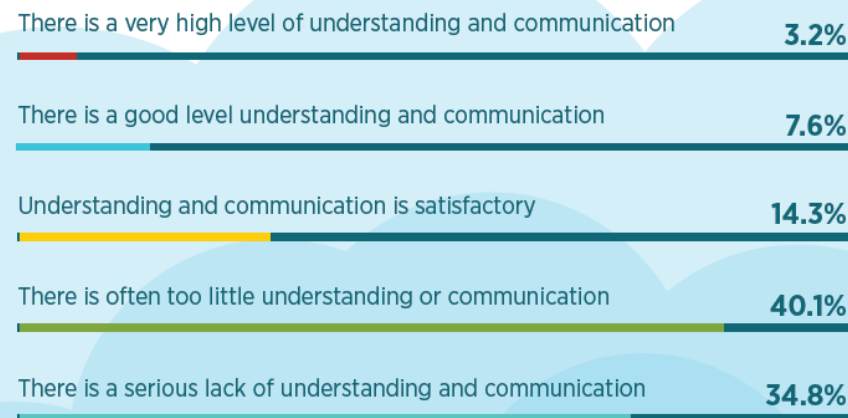*Those surveyed are primarily involved in the defence, aerospace and energy/oil & gas utilities sectors. Other responses primarily consist of security, law enforcement and legal services.*

Does your industry or organisation face a potential threat from malicious or negligent drone use?

The majority of those surveyed identify a potential threat of drones to their own organisation or sectors.

55.1% YES
30.6% NO
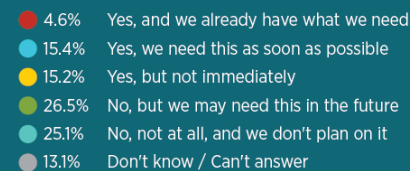**14.3% I DON'T KNOW**
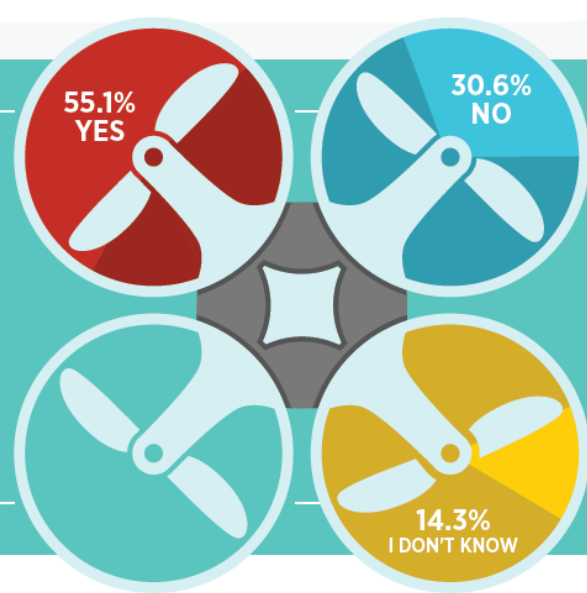
How well do you believe current legislation and guidance on civil air space drone use within your country is understood by the public and communicated by the authorities?

- There is a very high level of understanding and communication — **3.2%**
- There is a good level understanding and communication — **7.6%**
- Understanding and communication is satisfactory — **14.3%**
- There is often too little understanding or communication — **40.1%**
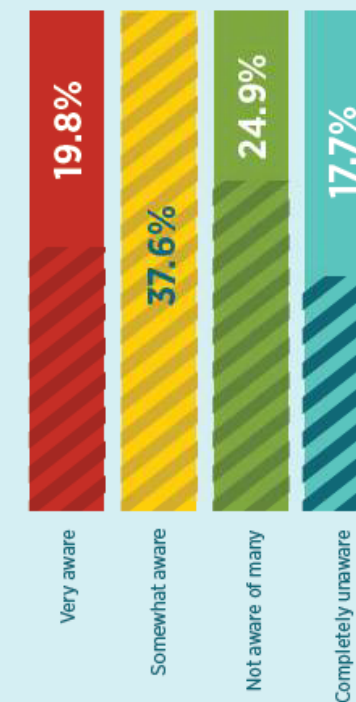- There is a serious lack of understanding and communication — **34.8%**

Over 74% of respondents believe there to be too little understanding or communication when it comes to drone regulations in the civil air space, with almost half of these identifying the deficit as "serious".

Does your organisation / site require a counter-drone strategy or counter-drone equipment?

- **4.6%** Yes, and we already have what we need
- **15.4%** Yes, we need this as soon as possible
- **15.2%** Yes, but not immediately
- **26.5%** No, but we may need this in the future
- **25.1%** No, not at all, and we don't plan on it
- **13.1%** Don't know / Can't answer

Almost half of our respondents are relatively satisfied with current levels of safety at their own sites and organisations without counter-UAS technology. However, many of these respondents identify as solution-providers and/or UAS operators or manufacturers rather than at-risk parties, while many also foresaw a potential need for these solutions in the future. Over 35% of respondents see an immediate need for fielding counter-drone technology at their place of work.
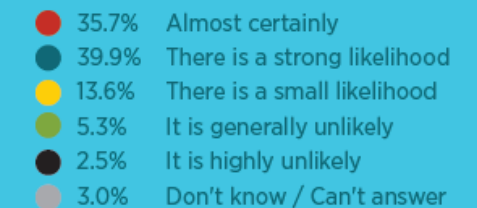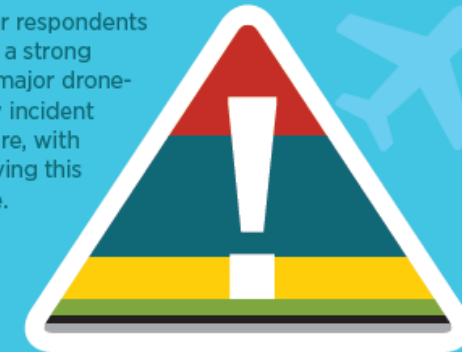
How aware are you of current commercial / civil counter-drone solutions available on the market?

- Very aware — **19.8%**
- Somewhat aware — **37.6%**
- Not aware of many — **24.9%**
- Completely unaware — **17.7%**

The level of awareness about commercial counter-technology on the market today is mixed. However, at least 42% of respondents admitted a significant lack of knowledge.

Generally speaking, and as regulations stand, do you believe drones in the civil air space are likely to be involved in the cause of a major security incident within the next 5 years?

Over 75% of our respondents believe there is a strong likelihood of a major drone-related security incident in the near future, with over 35% believing this to be inevitable.

- **35.7%** Almost certainly
- **39.9%** There is a strong likelihood
- **13.6%** There is a small likelihood
- **5.3%** It is generally unlikely
- **2.5%** It is highly unlikely
- **3.0%** Don't know / Can't answer

Interested in learning more? Involved in this market?

Join us at Countering Drones 2016

(06 - 08 December, 2016; London, United Kingdom)

www.counteringdrones.com

Civilian Drone Developments
New Rules and New Fears

The civilian use of drones presents homeland security, critical national infrastructure and commercial industries with a myriad of safety and privacy challenges. The growing number of incidents in just the past year involving drone intrusions into high-security areas such as airports, nuclear sites and government buildings, have done little to satisfy concerns for public safety. Many analysts have predicted that a major criminal or terrorist incident caused by a commercial drone is a case of "if", rather than "when". In efforts to mitigate the risk of serious incident – be it malicious or negligent – many countries are now scrambling to introduce effective regulation regulatory frameworks, and most of these are in their infancy. Here, we look at some of the major developments in international drone laws and the latest incidents causing concern for domestic security forces…

AUSTRALIA

Australia became one of the first countries in the world to regulate RPAS with the first operational regulation set back in 2002. The country's the Civil Aviation Safety Authority (CASA) governs UAS/RPA rules and regulations.

In recent years, to fly an RPA of any size for commercial benefit required a UAV controller certificate and an unmanned operator's certificate (UOC) for the business. Additional ratings have included a flight radio operator's license and experience on the type of UAS operated.

However, due to new regulations expected to come into effect in late 2016, anyone will be able to fly a drone under 2kg for profit in Australia. This relaxation of the laws is designed to cut red tape and thousands of dollars from the cost of using drones commercially. However, critics – particularly in the security arena – have warned that this will pose new dangers, such as in an increased risk of espionage and terrorist attacks.

Regardless, CASA-approved RPA training schools will remain available, offering drone pilot training packages and assistance on the certification process. Pilots will still need to register with CASA and describe the areas in which they plan to fly. They will also need to comply with the mandatory conditions that apply to amateur drone users, including flying below 120m in the air, only during the day, more than 30m from other people, away from emergency situations, more than 5.5km from controlled air space, and within the visual line of sight.

In April 2014, at the Geraldton Endure Batavia triathlon in Australia, a drone was being used to photograph competitors when it crashed into one of the athletes, causing a head wound that required stitches. The drone operator claims that the drone crashed after someone in the audience stole control of it from him.

FRANCE

From 2016, new regulations have been introduced for drone use, although some operators have criticized them for being overly complex.

Aircraft must remain in line of sight and fly within a distance of 200m, or 50m out of sight. The drone should not exceed 2 kg. Flights programmed on GPS coordinates have a weight limit of 1kg and automated flight is limited to 8 minutes. Commercial drones must exhibit a license plate with the name of the owner and contact details. It is possible to obtain authorisation for a particular flight if you can demonstrate an acceptable level of safety.

Operators must obtain authorisation from the DGAC. Professional operators must have a manual for specific activities (known as MAP) and provide a declaration of compliance. Operators must undergo training and obtain a theoretical statement of skill level (known as DNC). Technical files for specific vehicle classes are also required. Applications must be sent to a regional CASD/IR.

Since 2012, four operational scenarios have been defined. Scenario S-1 defines a flight where the drone should not fly more than 200m from the pilot and only outside of populated areas. Scenario S-2 accounts for a distance of up to 1 km (potentially out of direct line of sight). Scenario S-3 allows for flying over a populated area but maximum distance cannot exceed 100m. S-4 consists of flight outside of populated areas not covered by S-1 or S-2

– requiring pilots to be fully certified and to have a plane/helicopter pilot license, logging at least 100 hours, and having flown at least 20 hours in the last 6 months. Larger UAVs see further rules that are more difficult to obtain.

Between October 2014 and February 2015, at least 17 drone sightings were noticed over nuclear power plants in France, putting the country on high alert.

In one day in 2015, at least five drones were sighted by police in the early hours of the morning over the US embassy, the Eiffel Tower, the president's official residence, the Elysée Palace, the Invalides military museum and the Bastille area, which is both residential and commercial.

INDIA

It is technically illegal for civilians to use drones in India, but enforcing this law is becoming increasingly difficult as many UAVs are being used for recreation and photography, while the costs of devices are rapidly falling. As such, most drone use in civilian areas, if done safely, ethically and responsibly – and away from high-risk or sensitive areas – is unlikely to lead to prosecution.

Recognising that an outright ban is unrealistic, India's Directorate General of Civil Aviation (DGCA) and interior ministries were meeting in 2016 to formulate acceptable guidelines for operation, but officials have anticipated "technological and administrative challenges."

In October 2015, it was reported that an unidentified person was spotted flying a suspected helicam in New Delhi, near the high-security Vijay Chowk intersection close to Rashtrapati Bhavan and Parliament. The UAV was spotted hovering around 20-30 feet above the ground and the operator was aid to have "fled in a car" when confronted.

UNITED KINGDOM

The rules governing use of drones are still evolving as legal implications become more clear. For example, the House of Lords EU Committee called for the compulsory registration of all commercial and civilian drones, amid growing concern over the use of drones by private individuals with little knowledge of aviation rules.

Currently, drones may be used for recreation and commercial purposes as long as the operation of the aircraft does not endanger anyone or anything. The aircraft must be kept within the VLOS (normally taken to be within 500 m horizontally and 400 ft vertically) of its pilot. Operations beyond these distances must be approved by the CAA (the basic premise being for the operator to prove that he/she can do this safely).

Small UAVs (irrespective of their mass) used for surveillance purposes are subject to tighter restrictions with regard to the minimum proximities from other people or properties. Special permission is required from the CAA before these operations commenced.

The aircraft must not be flown over or within 150 metres of any congested area, over or within 150 metres of an organised open-air assembly of more than 1,000 persons, within 50 metres of any vessel, vehicle or structure which is not under the control of the person in charge of the aircraft, within 50 metres of any person except during take-off or landing, or within 30 metres of any person except for the person in charge of the aircraft.

Careful note should be taken that the collection of images of identifiable individuals, even inadvertently, when using surveillance cameras mounted on a small unmanned surveillance aircraft, will be subject to the Data Protection Act (which legislates over requirements concerning the collection, storage and use of such images).

According to data provided by Freedom of Information, police forces around the UK dealt with 860 calls about drones flying over residential properties in 2015. Households in Greater Manchester suffered the greatest nuisance with 90 complaints regarding intrusive or disruptive drones.

Police in the UK have been provided document guidance on how to neutralize "negligent" use of a drone, which includes instructions that officers must not (unless under exceptional circumstances, such as terrorist activity) attempt to take control of the aircraft due to the risk to public safety and to the drone itself. Instead, officers may only instruct operators to land or wait until the battery runs out.

Drone use around prisons (such as those attempting to deliver phones and narcotics) is on the rise in the UK. No incidents were recorded in 2013, two were recorded in 2014, and 33 in 2015.

JAPAN

An amendment to the Aviation Act came into effect in December, 2015, prohibiting flying drones over residential areas, in metropolitan public parks or gardens, or areas surrounding an airport without permission from the Minister of Land, Infrastructure and Transportation. Flying drones during night time and during an event is also prohibited.

Drones must remain within VLOS, cannot transport hazardous materials and may not drop any objects. In addition, UAVs in unrestricted areas across the country are required to stay below 150 meters (492 feet), and also be kept at least 30 meters (98 feet) from people, buildings, and vehicles. If the rules are violated, the UAV operator is liable for a fine of up to 500,000 yen.

These requirements are not applied to flights for search and rescue operations by public organisations in case of accidents and disasters.

In April 2015, anti-nuclear activist landed a drone containing radioactive sand on the Japanese prime minister's office.

ISRAEL

Israel's security situation means that there are hundreds of areas – some quite small (the size of a military base) and others huge (the entire west bank and large areas close to the borders) – around the country where overflying with a drone would be very problematic. Authorities are likely to take a dim view of general civil drone use.

Even so, license and insurance is possible, which can be obtained automatically by paying for membership to the Israel Aero Club. A year's membership will provide an automatic license to fly up to 50 meters and will cover insurance. To fly at up to 250 m requires an advanced pilot license issued by the Ministry of Transport. Flights above 250m are forbidden without advanced approval.

Hezbollah is reported to have been violating Israeli airspace with commercially available drones – part of a fleet of an estimated 200 UAVs. A 2016 attempt to photograph IDF drills saw Israel launch missiles to intercept the aircraft.

CLICK TO VIEW THE FULL INTERACTIVE MAP: