International CBRNE Institute

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

CBRNE-Terrorism Newsletter

W O M D

August 2016

unmanned CBRNE aerial vehicles

www.cbrne-terrorism-newsletter.com

SPECIAL Collection

CBRNE Unmanned Aerial Vehicles

The war in Syria brought the problem with chemical weapons into surface and led to their destruction with the aid of the international community under the Organization for the Prohibition of Chemical Weapons (OPCW). The consequent involvement of the Islamic State gave rise to production and use of chemical weapons both in Syria and Iraq. Following the multiple terrorist attacks in France and Belgium alarmed the Western world to a possible chemical or radiological attack against soft targets mainly in Europe. In parallel the introduction of unmanned aerial vehicles (UAVs – drones and multi-rotors) in both military and peace-time operations and activities complicated further the threat of using UAVs loaded with explosives, chemical or radiological loads. This Special Collection of the "CBRNE-Terrorism Newsletter" provides an overview of current situation worldwide giving some insights of how serious the threat is and how these vehicles can be used to counter these threats. The main conclusion is that the threat is real and we need to be proactive in order to avoid the usual surprises.

The Editor

Drone vs UAV? What's the difference?

Source: http://www.ezvid.com/drone-vs-uav-whats-the-difference

Is there a difference or are these the same thing?

The Answer

In the last few years, the word drone is becoming synonymous with two things, a death dealing machine flying high above Afghanistan and hobbyist quadcopters that are popping up everywhere like the Parrot AR seen below. They are even delivering products for Amazon these days. It seems that one day our mailmen may even be replaced with flying drones. Science fiction here we come.

Back to the matter at hand. The difference between UAVs and drones.

Trying to distinguish between drones and UAVs is a little tricky. Mostly because the term "drone" is more of a media buzzword rather than a clearly defined machine like a UAV. Due to the increasing popularity of drones for domestic and hobby use though, the government has decided to put some effort into defining exactly what makes up a drone so that regulations can be put in place.

I would say that every flying drone is a UAV, but every UAV is not a drone. Let's take a deeper look to see what I mean.

What is a Drone?

A drone is any kind of autonomously or remotely guided vehicle whether on land, sea, or air. The main qualifier, and currently only agreed upon definition, for something to be a drone is that there is no pilot inside.

Hobbyist quadcopters are drones, remote submarines are drones, and even robotic bomb diffusers are drones. All of these can be considered drones in the most basic sense of the word because they are machines/vehicles that are piloted through pre-programmed computer software or a remote pilot.

Let's get more specific and just focus on flying drones for now, as I believe that is what your question is referring to.

In the simplest sense, even the 1917 Kettering Bug pictured below can be considered a drone. The "Bug" rolled off a larger aircraft and used electrical and pneumatic controls to guide it towards a target. Its flight pattern couldn't be adjusted remotely, it couldn't be recalled and, along the way down its engine would shutoff and wings would be released before falling out the sky and hitting the target. Not exactly what we think of today when we use the term drone, but by the only currently agreed upon definition, it is a drone. Currently the government is trying to create a more detailed definition for the word drone so that when regulations are put in place, they will be tailored specifically to drones and not all remote piloted crafts like RC airplanes. To clear up some of the confusion, some proponents are trying to add that in order for something to be considered a drone, it needs to have some form of autonomous flying software that allows it to function, adjust its flight pattern or return to its launch spot without human intervention.

What this basically means is that unless it has some sort of on-board autonomous flying system, it shouldn't be considered a drone even if there is no pilot in the craft. Of course nobody has been able to fully agree on this.

According to Chris Anderson, the former Wired editor who currently runs DIYDrones.com and 3DRobotics, drones include any remotely controlled flying object that is capable of switching to autonomous control at some point during the flight. He feels that a basic remote-controlled model aircraft wouldn't be considered a drone.

Ryan Calo, a Professor of law at the University of Washington, seems to agree in some sense. He feels that there are three qualifications that must be met to call something a drone. It needs to be able to fly, it must have some sensing capacity like a camera or infrared sensor, and it must be capable of some level of autonomous flight.

The military and the government on the other hand, don't seem to agree. They currently define any flying craft without a pilot inside as a drone.

What do you think? Would you consider the Q500 Typhoon Quadcopter which comes with a 1080P 60FPS HD video camera, 3-axis gimbal and personal ground station, a return to home feature, plus a transmitter that supports a 5.8GHz video downlink that delivers streaming video to the built-in screen of the transmitter to be the same as the E-flite 3100 Apprentice?

What if I told you that the E-flite has a "panic" control system that returns to, and maintains, level flight if the operator has trouble flying?

You can see why things begin to get a little tricky here.

Stabilizing flight could be considered some level of autonomous flying ability, but that's as far as it goes. It can't be programmed on a path or return to home if it loses radio control transmission. Due to the camera, return to home programming, and precision, hover style flight capabilities of the Q500 Typhoon Quadcopter it seems to me it should fall under different regulation. The Q500 could easily be used for snooping or video recording of neighbors while the E-flite's flying style would make that nearly impossible even if a camera was attached.

So how is a UAV Different than a Drone?

UAV is military or government speak for Unmanned Aerial Vehicle. Most often when the term UAV is used, they are referring to drones, but this is not 100% accurate. You see, an RC airplane is a UAV. It doesn't have a pilot on board steering the craft and it is controlled remotely, hence it is an unmanned aerial vehicle or RPC (remote piloted craft). According to the military, these would be considered drones, but since most RC airplanes don't have any kind of autonomous flying software though, should they really be considered drones? I feel the term UAV would be more accurate whereas calling an RC airplane a drone doesn't really seem to fit. Unfortunately, not every federal department agrees with this which is what makes distinguishing the two so difficult.

According to Les Dorr, a spokesperson for the FAA, "the Federal Aviation Administration uses the designation UAS (unmanned aircraft system) to describe anything from a remote controlled model helicopter to a passenger plane-sized predator attack craft."

The Department of Defense has slightly different wording in their definition of a UAV or UAS, but it seems to line up with what the FAA says. They apply the term UAV to any "aircraft or ballon" controlled by a person or software from afar.

Neither of these departments has a definition for drones.

So what's the Verdict?

If you are just interested in buying a drone for fun to fly around your neighborhood, then there is no difference between UAVs and drones. If you want to search on Amazon or some other online shopping site, I suggest you use the term drone as it is more popular and will bring up a larger variety of options.

If you are interested in the difference between the two for regulatory issues, then many more factors must be taken into account. If we look at these two descriptions and the input of various professionals and regulatory departments, we should all be thoroughly confused by now. As mentioned previously, the problem is a lack of a universally accepted definition. This muddies the water and makes it hard to make any kind of blanket statement about what a drone is or isn't and whether UAVs and drones are the same thing.

I tend to agree that RC airplanes and drones aren't the same thing and have very different capabilities. Because of this I feel that there needs to be some way to distinguish between the two. I agree that some form autonomous flying capability must be present for something to be considered a drone and I would go so far as to include some considerations regarding its flying capability. I would add that in order for something to fall under the regulations being enacted for domestic drone use, it needs to have the ability to hover in one place for an extended period of time.

Most professionals in the industry agree that the main difference between the two is the capability for autonomous flight. Following this line of thinking, **any flying drone has to be a UAV, but not every UAV has to be a drone.**

ISIS Wants to Carry Out a WMD Attack in Europe

Source: http://www.clarionproject.org/news/isis-wants-carry-out-wmd-attack-europe#

Dec 07, 2015 –"The European Union and its Member States must prepare for the possibility of a chemical or biological attack on their territory by the self-styled 'Islamic State'" warns a new European Parliament report.

The report states ISIS could carry out a future attack with an improvised explosive device (IED) packed with chemical, biological, radiological or nuclear (CBRN) material. It thought ISIS may already have CBRN material within Europe.

"ISIL actually has already acquired the knowledge, and in some cases the human expertise, that would allow it to use CBRN materials as weapons of terror" the Director of the Weapons of Mass Destruction (WMD) Non-Proliferation Centre at NATO, Wolfgang Rudischhauser, stated.

ISIS reportedly used chemical weapons in combat against Kurdish positions in Syria.

It is said to have seized chemical weapons from old bunkers formerly held by Saddam Hussein. Nuclear material was also taken from the research facility at Mosul University, according to the International Atomic Energy Agency (IAEA).

The FBI thwarted at least four attempts by ISIS to purchase radioactive materials smuggled through eastern Europe.

"We are dealing with a very serious, well-resourced, determined international terrorist organization that is now active on the streets of Europe," said head of Europol, Rob Wainwright. Europol coordinates between EU police forces. "This represents the most serious terrorist threat faced in Europe for 10 years."

The report recommended increasing training of security services to deal with a possible CBRN attack and equipping security at sensitive sites such as airports. It also advocated more intensive screening of potential returning foreign fighters to track those believed to have expertise in manufacturing WMDs.

The Jihadist CBRN Threat

By Scott Stewart

Source: https://www.stratfor.com/weekly/20100210_jihadist_cbrn_threat

Feb 2010 – In an interview aired Feb. 7 on CNN, U.S. Secretary of State Hillary Clinton said she considers weapons of mass destruction (WMD) in the hands of an international terrorist group to be the largest threat faced by the United States today, even bigger than the threat posed by a nuclear-armed Iran. "The biggest nightmare that many of us have is that one of these terrorist member organizations within this syndicate of terror will get their hands on a weapon of mass destruction," Clinton said. In referring to the al Qaeda network, Clinton noted that it is "unfortunately a very committed, clever, diabolical group of terrorists who are always looking for weaknesses and openings."

Clinton's comments came on the heels of a presentation by U.S. Director of National Intelligence Dennis Blair to the Senate Select Committee on Intelligence. In his Annual Threat Assessment of the U.S. Intelligence Community on Feb. 2, Blair noted that, although counterterrorism actions have dealt a significant blow to al Qaeda's near-term efforts to develop a sophisticated chemical, biological, radiological and nuclear (CBRN) attack capability, the U.S. intelligence community judges that the group is still intent on acquiring the capability. Blair also stated the obvious when he said that if al Qaeda were able to develop CBRN weapons and had the operatives to use them it would do so.

All this talk about al Qaeda and WMD has caused a number of STRATFOR clients, readers and even friends and family members to ask for our assessment of this very worrisome issue. So, we thought it would be an opportune time to update our readers on the topic.

Realities Shaping the Playing Field

To begin a discussion of jihadists and WMD, it is first important to briefly re-cap STRATFOR's assessment of al Qaeda and the broader jihadist movement. It is our assessment that the first layer of the jihadist movement, the al Qaeda core group, has been hit heavily by the efforts of the United States and its allies in the aftermath of 9/11. Due to the military, financial, diplomatic, intelligence and law enforcement operations conducted against the core group, it is now a far smaller and more insular organization than it once was and is largely confined geographically to the Afghan-Pakistani border. Having lost much of its operational ability, the al Qaeda core is now involved primarily in the ideological struggle (which it seems to be losing at the present time).

The second layer in the jihadist realm consists of regional terrorist or insurgent groups that have adopted the jihadist ideology. Some of these have taken up the al Qaeda banner, such as al Qaeda in the Islamic Maghreb (AQIM) and al Qaeda in the Arabian Peninsula (AQAP), and we refer to them as al Qaeda franchise groups. Other groups may adopt some or all of al Qaeda's jihadist ideology and cooperate with the core group, but they will maintain their independence for a variety of reasons. In recent years, these groups have assumed the mantle of leadership for the jihadist movement on the physical battlefield.

The third (and broadest) component of the jihadist movement is composed of grassroots jihadists. These are individuals or small groups of people located across the globe who are inspired by the al Qaeda core and the franchise groups but who may have little or no actual connection to these groups. By their very nature, the grassroots jihadists are the hardest of these three components to identify and target and, as a result, are able to move with more freedom than members of the al Qaeda core or the regional franchises.

As long as the ideology of jihadism exists, and jihadists at any of these three layers embrace the philosophy of attacking the "far enemy," there will be a threat of attacks by jihadists against the United States. The types of attacks they are capable of conducting, however, depend on their intent and capability. Generally speaking, the capability of the operatives associated with the al Qaeda core is the highest and the capability of grassroots operatives is the lowest. Certainly, many grassroots operatives think big and would love to conduct a large, devastating attack, but their grandiose plans often come to naught for lack of experience and terrorist tradecraft.

Although the American public has long anticipated a follow-on attack to 9/11, most of the attacks directed against the United States since 9/11 have failed. In addition to incompetence and poor tradecraft, one of the contributing factors to these failures is the nature of the targets. Many strategic targets are large and well-constructed, and therefore hard to destroy. In other words, just because a strategic target is attacked does not mean the attack has succeeded. Indeed, many such attacks have failed. Even when a plot against a strategic target is successfully executed, it might not produce the desired results and would therefore be considered a failure. For example, the detonation of a massive truck bomb in a parking garage of the World Trade Center in 1993 failed to achieve the jihadists' aims of toppling the two towers and producing mass casualties, or of causing a major U.S. foreign policy shift.

Many strategic targets, such as embassies, are well protected against conventional attacks. Their large standoff distances and physical security measures (like substantial perimeter walls) protect them from vehicle-borne improvised explosive devices (VBIEDs), while these and other security measures make it difficult to cause significant damage to them using smaller IEDs or small arms.

To overcome these obstacles, jihadists have been forced to look at alternate means of attack. **Al Qaeda's use of large, fully fueled passenger aircraft as guided missiles** is a great example of this, though it must be noted that once that tactic became known, it ceased to be viable (as **United Airlines Flight 93** demonstrated). Today, there is little chance that a flight crew and passengers of an aircraft would allow it to be seized by a small group of hijackers.

CBRN

Al Qaeda has long plotted ways to overcome security measures and launch strategic strikes with CBRN weapons. In addition to the many public pronouncements the group has made about its desire to obtain and use such weapons, **we know al Qaeda has developed crude methods for producing chemical and biological weapons and included such tactics in its encyclopedia of jihad and terrorist training courses.**

However, as STRATFOR has repeatedly pointed out, chemical and biological weapons are expensive and difficult to use and have proved to be largely ineffective in real-world applications. A comparison of the Aum Shinrikyo chemical and biological attacks in Tokyo with the March 2004 jihadist attacks in Madrid clearly demonstrates that explosives are far cheaper, easier to use and more effective in killing people. The failure by jihadists in Iraq to use chlorine effectively in their attacks also underscores the problem of using improvised chemical weapons. These problems were also apparent to the al Qaeda leadership, which scrapped a plot to use improvised chemical weapons in the New York subway system due to concerns that the weapons would be ineffective. The pressure jihadist groups are under would also make it very difficult for them to develop a chemical or biological weapons facility, even if they possessed the financial and human resources required to launch such a program.

Of course, it is not unimaginable for al Qaeda or other jihadists to think outside the box and attack a chemical storage site or tanker car, or use such bulk chemicals to attack another target — much as the 9/11 hijackers used passenger- and fuel-laden aircraft to attack their targets. However, while an attack using deadly bulk chemicals could kill many people, most would be evacuated before they could receive a lethal dose, as past industrial accidents have demonstrated. Therefore, such an attack would be messy but would be more likely to cause mass panic and evacuations than mass casualties. Still, it would be a far more substantial attack than the previous subway plot using improvised chemical weapons.

A similar case can be made against the effectiveness of an attack involving a radiological dispersion device (RDD), sometimes called a "dirty bomb." While RDDs are easy to deploy — so simple that we are surprised one has not already been used within the United States — it is very difficult to immediately administer a lethal dose of radiation to victims. Therefore, the "bomb" part of a dirty bomb would likely kill more people than the device's "dirty," or radiological, component. However, use of an RDD would result in mass panic and evacuations and could require a lengthy and expensive decontamination process. Because of this, we refer to RDDs as "weapons of mass disruption" rather than weapons of mass destruction.

The bottom line is that a nuclear device is the only element of the CBRN threat that can be relied upon to create mass casualties and guarantee the success of a strategic strike. **However, a nuclear device is also by far the hardest of the CBRN weapons to obtain or manufacture and therefore the least likely to be used.** Given the pressure that al Qaeda and its regional franchise groups are under in the post-9/11 world, it is simply not possible for them to begin a weapons program intended to design and build a nuclear device. Unlike countries such as North Korea and Iran, jihadists simply do not have the resources or the secure territory on which to build such facilities. Even with money and secure facilities, it is still a long and difficult endeavor to create a nuclear weapons program — as is evident in the efforts of North Korea and Iran. This means that jihadists would be forced to obtain an entire nuclear device from a country that did have a nuclear weapons program, or fissile material such as highly enriched uranium (enriched to 80 percent or higher of the fissile isotope U-235) that they could use to build a crude, gun-type nuclear weapon.

Indeed, we know from al Qaeda defectors like Jamal al-Fadl that al Qaeda attempted to obtain fissile material as long ago as 1994. The organization was duped by some of the scammers who were roaming the globe attempting to sell bogus material following the collapse of the Soviet Union. Several U.S. government agencies were duped in similar scams.

Black-market sales of military-grade radioactive materials spiked following the collapse of the Soviet Union as criminal elements descended on abandoned Russian nuclear facilities in search of a quick buck. In subsequent years the Russian government, in conjunction with various international agencies and the U.S. government, clamped down on the sale of Soviet-era radioactive materials. U.S. aid to Russia in the form of so-called "nonproliferation assistance" — money paid to destroy or adequately secure such nuclear and radiological material — increased dramatically following 9/11. In 2009, the U.S. Congress authorized around $1.2 billion for U.S. programs that provide nonproliferation and threat reduction assistance to the former Soviet Union. Such programs have resulted in a considerable amount of fissile material being taken off the market and removed from vulnerable storage sites, and have made it far harder to obtain fissile material today than it was in 1990 or even 2000.

Another complication to consider is that jihadists are not the only parties who are in the market for nuclear weapons or fissile material. In addition to counterproliferation programs that offer to pay money for fissile materials, countries like Iran and North Korea would likely be quick to purchase such items, and they have the resources to do so, unlike jihadist groups, which are financially strapped.

Some commentators have said they believe al Qaeda has had nuclear weapons for years but has been waiting to activate them at the "right time." Others claim these weapons are pre-positioned inside U.S. cities. STRATFOR's position is that if al Qaeda had such weapons prior to 9/11, it would have used them instead of conducting the airline attack. Even if the group had succeeded in obtaining a nuclear weapon after 9/11, it would have used it by now rather than simply sitting on it and running the risk of it being seized.

There is also the question of state assistance to terrorist groups, but the actions of the jihadist movement since 9/11 have served to steadily turn once quietly supportive (or ambivalent) states against the movement. Saudi Arabia declared war on jihadists in 2003 and countries such as Yemen, Pakistan and Indonesia have recently gone on the offensive. Indeed, in his Feb. 2 presentation to the Senate committee, Blair said: "We do not know of any states deliberately providing CBRN assistance to terrorist groups. Although terrorist groups and individuals have sought out scientists with applicable expertise, we have no corroborated reporting that indicates such experts have advanced terrorist CBRN capability." Blair also noted that, "We and many in the international community are especially concerned about the potential for terrorists to gain access to WMD-related materials or technology."

Clearly, any state that considered providing WMD to jihadists would have to worry about blow-back from countries that would be targeted by that material (such as the United States and Russia). With jihadists having declared war on the governments of countries in which they operate, officials in a position to provide CBRN to those jihadists would also have ample reason to be concerned about the materials being used against their own governments.

Efforts to counter the proliferation of nuclear materials and technology will certainly continue for the foreseeable future, especially efforts to ensure that governments with nuclear weapons programs do not provide weapons or fissile material to jihadist groups. While the chance of such a terrorist attack is remote, the devastation one could cause means that it must be carefully guarded against.

Game of Drones: the unmanned revolution in CBRNe security

By Anna Paternnosto

Source: http://www.cbrneportal.com/game-of-drones-the-unmanned-revolution-in-cbrne-security/

Feb 29 – Recent technological developments in the field of Unmanned Aerial Vehicles (UAVs) have demonstrated the outstanding potential of remotely operated capabilities in mitigating risks to human security in CBRNe environments. On one side unmanned capabilities in contaminated sites can perform a wide range of information gathering tasks without compromising human security. On the other side of the spectrum, the spread of civilian UAVs on the market represents opportunities for potential illicit exploitation of these capabilities by criminal or terrorist groups. Public gatherings and critical infrastructure can be the target of CBRNe attacks conducted through the use of unmanned aircrafts. The wide availability and low cost of remote control devices make them easily obtainable by terrorist groups with illicit purposes. In this challenging security environment, the priority needs to be set on the development of mitigation strategies that include detection and interception systems, but also enhanced legislation and regulations to deter illegal UAVs activities.

In terms of CBRNe defense missions, unmanned systems can perform a wide variety of tasks that range from reconnaissance and surveillance to detection and decontamination. CBRNe sensors installed on a UAV platform can perform their functions independent of ground conditions, thus reducing risks of human loss and permanent health damages to first responders and soldiers. Instead of deploying personnel in non-secure and contaminated environments, UAVs can perform extensive information gathering tasks in areas that are too hazardous for normal workforce activities. Unmanned aerial vehicles can detect radiations, chemical and biological hazards, as well as explosives while saving human labor and increasing force protection. By deploying unmanned systems in non-secure environments, CBRNe first responders can perform more oriented and specialized tasks where the necessity of human labor is needed.

In the aftermath of the Fukushima Daichii accident occurred in 2011, the deployment of unmanned vehicles allowed wide-area measurements in high-contaminated areas without exposing human workers to nuclear radiation. In 2015 Japanese scientists developed a drone able to enter the Fukushima reactor buildings through a laser technology. Not only can this drone avoid obstacles, but it can also to operate in areas without GPS signal and replace its own batteries, without human intervention. UAVs have been sent into Fukushima's reactors previously, but the high level of radiations have put the drones out if action in few hours. In addition to monitoring functions in highly-contaminated areas, drones have also been deployed in remote areas to prevent the outbreak of diseases and detect new infectious agents. In Malaysia UAVs have been used to monitor macaque movements and prevent malaria cases. Currently a group of researchers is working on a project that involves a drone programmed to collect and analyze mosquitoes with the aim of detecting potential diseases before they become an epidemic.

Despite the CBRNe capabilities that unmanned vehicles can perform, the flip side is all but encouraging. The impact of drone technology rises concerns that UAVs could be illicitly exploited by terrorists posing emerging threats to public security. The expansion of civilian unmanned vehicles on the market and the attractiveness – in terms of price and manageability – of these systems have inspired a considerable amount of concern about the possible misuse of drones. Without the need of precision flying or advanced technologies, unmanned aerial systems can be transformed in delivery platforms for CBRNe materials. Most consumer drones will be employed for legitimate purposes, but the potential of their misapplication cannot be ignored.

Previous events confirm that UAVs has already been used by criminals and terrorists to threaten public security. **For example**, in 2013 al Qaeda's plot to deploy remote controlled aerial vehicles packed with chemicals was thwarted by Iraqi military Intelligence; during the battle of Kobane in 2014, ISIS released propaganda videos taken from drones and started using UAVs for battlefield reconnaissance; in 2015 a small drone with traces of radiation and marked with radioactive symbols was found on the roof of Japanese Prime Minister Shinzo Abe's office in Tokyo; in 2015 a drone carrying a pro-Albanian flag flew into Belgrade's football stadium during a Euro 2016 qualifying match, forcing the interruption of the game. These episodes rise fear that terrorist organizations could use remote control vehicles to release CBRNe materials during major events or in critical infrastructure causing mass casualties.

Because of the novelty of UAV technology, the threat of rogue drones is underestimated by decision makers and law enforcement personnel. Currently there is a lack of a common understanding towards the threat posed by UAVs. Law enforcement efforts demonstrate vulnerabilities to potential weaponized drone threats, and the development of a cohesive defense strategy seems far away.

In order to mitigate the risks posed by UAVs, in recent years new technologies have been exploited to develop anti-Unmanned Aerial Vehicles defense systems able to keep drones away from critical infrastructure. Innovative systems emerged and numerous companies are working on solutions that neutralize drones in the air before they can reach their target. Some of these technologies use shoulder mounted rifles that employ radio waves to disrupt drone's communication capabilities, others consist in high power lasers that shoot hostile or suspicious UAVs from long distances. To prevent damages caused by falling drones, some systems also include technologies able to wrest control of the unmanned vehicle from its operator and land the drone safely. Novel solutions in anti-drones systems are not only linked to industrial and technological innovations. The Netherlands National Police has started training eagles to identify suspicious drones and the Tokyo Metropolitan Police has established a drone squad with the aim of intercepting rogue UAVs by patrolling relevant buildings. Air surveillance and innovative defense system are not the only ways of addressing the potential threat of UAVs. An important role in the process should be the implementation of relevant policies able to ensure the safe integration of drones in the national airspace system of a country. Lawmakers should introduce regulatory measures in drone industry as restrictions on carrying capacities, increased air traffic control regulations and the establishment of no fly zones.

Recent developments in Unmanned Aerial System technologies make the exploitation of drones in CBRNe operations extremely successful. Drones have the potential to contribute CBRNe disaster prevention and response. However, if illicitly exploited, they can constitute a threat themselves. Incidents involving the use of UAVs for illicit purposes should act as a red flag to decision-makers to develop mitigation strategies, not only based on technological developments and active defense, but also on deterrence and legislation efforts. Raising concerns for a possible revolution in CBRNe security should urge governments to fight terrorists in the existing game of drones.

***Anna Paternnosto** is a consultant at IB Consultancy. She holds a Master's Degree in International and Diplomatic Studies from the University of Trieste (Italy). From 2013 to 2015 she served as the Deputy- Secretary of the Youth Atlantic Treaty Association of Gorizia and participated in numerous international seminars on transatlantic security and emerging security challenges. Before joining IB Consultancy, she conducted a traineeship at the Austrian Mission to NATO in Brussels.*

Nuclear power plants under drone attack

By Andy Oppenheimer

Source: http://www.cbrneportal.com/nuclear-power-plants-under-drone-attack/

"You don't need massive amounts of force to allow a nuclear plant to go into instability. The plant has enough energy to destroy itself. Drones can be used to tickle the plant into instability."

– John Large, Large & Associates

March 31 – Compiled by leading British nuclear expert John Large of consulting engineers Large & Associates, and commissioned by Greenpeace France, the report followed several unexplained, but apparently co-ordinated, flights of tiny versions of drones – unmanned aerial vehicles (UAVs) – over French nuclear installations. Unidentified UAVs breached restricted airspace over 13 of France's 19 nuclear power plants between early October and late November 2014. In January a UAV was spotted over the Elysée Palace, and in February drones were seen flying around five other Paris landmarks.

In public evidence to the French parliament, Mr Large stated various modes of drone attack against the defences of a standard NPP could include precisely targeted IEDs (improvised explosive devices) or dropping equipment to aid an insider saboteur.

Not toys but machines

The report modelling showed that the "flexible access and manoeuvrability of the drones" means that they were able to fly over and twist around physical barriers that "belonged to a different age." Even small, battery-powered drones can lift at least 10 kg, while vehicles available in high-street hobbyist shops "are certainly not toys but machines capable of following and discharging intelligent commands."

Chatham House cyber security expert Caroline Baylon backed this up: "Because drones are so small, conventional radar cannot detect them. There's a huge vulnerability there." She wrote in *Newsweek* in December 2014 that drones could also provide air support for an actual ground-based attack; drop explosives to damage power or communications networks; and be used to bomb spent-fuel pools, which are less well protected than reactor cores.

According to the French Directorate General for Civil Aviation, 1,300 commercial drone licences were granted since 2012, but they can easily be bought without a licence on the high street or online. Soldiers are authorised to shoot drones down, but not when they are over an NPP for fear of causing damage – which is exactly where they would be if used in an attack.

In 2014 Britain's 16 operational reactors suffered 37 security breaches, including by at least one small UAV – the highest number since 12 breaches in 2011. The Large report recommended a major exercise to test the resilience of the UK's power stations against acts of terrorism. With the recent terrorist attacks in Paris still painfully fresh in the national memory, France has now tasked its National Research Agency with investigating ways to improve detection and interception of small, low-flying drones and has announced that it plans to share its findings with other European countries.

No defence

NPP's defences are designed to prevent accidents, not against terrorist threats. According to Large "most plants in France are not acceptable. The plants in the rest of Europe are old and need reviewing in this respect." NPP defences are based on the design-based threat (DBT) – defined by the NRC and the UK Office for Nuclear Regulation (ONR), as the "range of threats faced by nuclear facilities," based on assumptions about the capabilities of an attacker.

By 2014, and after many recommendations, the NRC characterized the DBT as a "well-trained and dedicated paramilitary force armed with automatic weapons and explosives and intent on forcing its way into the plant to commit radiological sabotage. Such a force may have the assistance of an 'insider'… The threat also includes bomb-laden land and waterborne vehicles." But so far it does not include drones.

Cyber threats

In warning that the authorities are "burying their heads in the sand," Large added cyber sabotage to the threat of physical attacks: existing NPPs are not designed to counter the threat of "near-cyborg technology… In each of the four… attack scenarios that I examined, the plant fared very badly indeed – if these scenarios had been for real, there would have been the potential for a major radioactive release."

In March 2014 the South Korean government accused North Korea of carrying out cyber-attacks in December 2014 on its NPP operator, after investigators concluded the North was responsible. In 2003, a computer virus penetrated the network at the Davis Besse Nuclear Power Plant in Ohio. Although the plant was shut down at the time it was, nevertheless, still vulnerable as technicians had not installed a Microsoft security patch.

Plots and attempts

The NPP at Lucas Heights, near Sydney, Australia was the intended target of terrorists in 2005 with in the inset, one of the rocket launchers found in the search for weapons. ©Bob Pearce

What precedent is there for NPP attack? Previous attempts are rare, but a hallmark plot was uncovered in November 2005 to carry out an attack on the Lucas Heights NPP, on the outskirts of Sydney, Australia. A group of Melbourne- and Sydney-based jihadists had undergone terrorist training on two country stations in New South Wales. After tracking the group, police stopped three suspects near the plant a year before their arrest, as part of police Operation Pendennis. Investigators discovered that an access on the outer security fence had been cut. The group had stockpiled weapons, including Australian Army rocket launchers, explosives, and other bomb-making materials – and had scoped out other high-profile Australian targets as well as Lucas Heights. Five men were convicted of terrorism charges in October 2009.

More recently, in May 2014 20 activists of the Ukrainian Right Sector were detained by Russian police for allegedly trying to seize the Zaporozhye NPP – Europe's largest nuclear power plant, located between the beleaguered city of Donetsk and Russian-occupied Crimea – in the country where the world's worst NPP disaster occurred, at Chernobyl in April 1986.

Andy Oppenheimer *AIExpE MIABTI is Editor of CBNW (Chemical, Biological & Nuclear Warfare) journal and a consultant in CBRNE and counter-terrorism. He is author of IRA: The Bombs and the Bullets (Irish Academic Press, 2008) and of the CBRN and IEDs module courses for the St Andrews University Certificate in Terrorism Studies.*

US Follows Islamic Terrorists' Use of Explosive UAVs

Source: http://i-hls.com/2016/07/us-follows-islamic-terrorists-use-of-explosive-uavs/

July 28 – Warfare against IEDs (improvised explosive devices) has been on the US Defense Administration agenda for a long time. Lessons have been learned also from Israel's operational activities in this field. In mid-2016 the U.S. Department of Defense asked Congress for an additional $20 million to develop countermeasures to the growing Islamic terrorist use of cheap commercial UAVs. The Islamic terrorists, especially ISIL (Islamic State in Iraq and the Levant), have been using these UAVs more frequently in the last few years and the Department of Defense believes ISIL is planning to eventually use these commercial UAVs as flying bombs. The defense administration organization JIDO has long been working on better ways to detect and deal with non-flying IEDs and considers bomb equipped UAVs a flying IED.

The Department of Defense points out that since September 11, 2001 two-thirds of the Americans killed in combat were the victims of IEDs in the form of roadside bombs and (much less often) mines. JIDO, that has been spotting and defeating bomb equipped commercial UAVs, wants more money to get results faster.

There have been electronic chatter among Islamic terrorists about the possibility of armed commercial UAVs. According to Strategy Page, U.S. counter-IED tactics concentrate on discovering who is organizing the IED effort, and then going after the key members of that organization. This is done using a combination of powerful computer software, and traditional detective and military intelligence methods. Those same methods have been picking up more discussions about using commercial UAVs and eventually arming them.

JIDO found out that the most effective tactic was to take out the leaders and technical specialists (bomb builders). That worked in Iraq, it worked in Afghanistan and worked in Israel.

Going after commercial UAVs is not just to eliminate explosive UAVS but also unarmed UAVs used for reconnaissance by Islamic terrorists. For the moment the Islamic terrorists do not have enough UAVs for anything but reconnaissance. These are often shot down or lost due to equipment failure or operator error. Money is often scarce in Islamic terror groups and there are more urgent priorities (like more guns, bullets and food). But the Department of Defense believes it's only a matter of time and wants to be ready.

The UAV "Dirty" Work

By David Oliver

Source: http://www.cbrneportal.com/the-uav-dirty-work/

Jan 27, 2015 – Unmanned aircrafts are an ideal choice when operations are required in environments that would be hostile to a manned aircraft or its crew. Airborne sampling or observation missions related to chemical, biological, radiological and nuclear (CBRN) threats would be ideally suited to unmanned aircrafts. Sensors can be fitted to a range of types, from a small man-portable system for local tactical use, to large aircraft-sized systems for global monitoring. The smaller systems can be sacrificed in a safe area once data has been gathered rather than having to recover to an airfield where it would have to be decontaminated, or risk contaminating personnel and other equipment.

This 'dirty' role involves the detection and identification of CBRN, high-yield explosives and toxic industrial material agents and substances. Unmanned Aerial Vehicles (UAV) can be used to support these aspects of a survey team's mission. Specific tasks that can be performed by UAV include marking and timing the team's route, scanning for hazards, conducting air monitoring, checking for corrosives, and detecting radiation, chemical warfare agents, and biological hazards.

Clarification, containment, and combat of incidents that are caused by uncontrolled emissions of dangerous gases and liquids or CBRN weapons remain an emerging challenge. Instead of sending specially equipped forces with expensive transport and measurement devices into the contaminated area, an autonomous, wirelessly connected swarm of micro-UAVs, equipped with lightweight mobile sensor systems, could be used in the future. Utilizing a MUAV swarm enables the calculation of gas concentrations and also allows for propagation forecasts, which assist rescue forces in averting danger by evacuation at a very early stage. Widespread chemical plumes can have a spread of 20 km or more which could be tracked by using several UAVs in a swarm and assigning a relay functionality to each UAV or by using public wireless networks. Relevant incident areas are usually urban or metropolitan where infrastructures of cellular networks are available such as GSM, UMTS/HSPA or Mobile WiMAX.

The sophistication of UAV's instrumentation and sensor systems will increase, providing data levels similar to or better than manned aircraft. Increases in performance are likely to be incremental, rather than revolutionary, with the greatest effect on unmanned aircraft likely being the decrease in sensor size and associated packaging. Research effort for sensors is likely to be focused on sensor integration, fusion and on board analysis. The timely distribution of analyzed data will be a key issue and work is required to determine the best mix of on-board versus off-board analysis.

One company involved in this sector of the market is the Washington-based Research International Inc., which has developed a pioneering UAV-based product called the "Flying Laboratory" that has full CBRN monitoring capabilities. A second-generation ion mobility spectrometer (IMS) is mounted onboard a UAV to provide toxic gas detection and up to 20 chemical warfare agents and toxic industrial gases can be detected at part per billion to part per million concentrations. A UV particle fluorometer is used to detect any unusually high biological aerosol levels, and a gamma spectrometer is used in combination with two Geiger counters to detect and identify nuclear materials and monitor radiation levels. One of the Geiger tubes is used for monitoring general background radiation levels, while the second, capable of detecting either alpha, beta or gamma radiation, is mounted so that it monitors radiation emitted from particulates captured by an aerosol sampling filter included in the payload. An on-board air sampling circuit can grab a biological or radiological aerosol sample if the biological or radiological sensors detect unusual conditions. This sample is either collected onto a compact 44 mm diameter high-flow electret filter with a 50 percent collection point of 0.5 microns, or with a lower flow electret filter with 99+ percent efficiency at 0.3 microns. The latter is used for radiological sampling.

A single-board computer is used to combine, analyze and store digital data created by the various CBRN sensors. Sensor data, along with GPS coordinates and time, is stored on a 32GB SD memory card for post-flight analysis.

Its system detectors typically respond in 1 to 2 seconds while the gas detector has the largest latency period, of about four seconds, which corresponds to less than +-45 meters uncertainty in position at cruising speed, or about +-26 meters at the lowest possible speed. Research International Inc. is also partnering with the Russian company ENICS to offer the world community a range of UAVs with integrated CBRN capability.

The German armed forces already operates CBRN-capable UAVs including the EMT LUNA tactical UAV that can deploy a wide range of payloads such as EO/IR, SAR, SIGINT or CBRN sensors and relay payloads. It can stay aloft for 8 hours and is able to respond to fast changing mission requirements. Also designed to meet the urgent requirements of the German Bundeswehr is the EMT ALADIN Mini-UAV that can carry EO/IR and CBRN sensor payloads.

***David Oliver** is a defense photo-journalist for more than 30 years, and member of the Independent Defense Media Association (IDMA) and the European Security and Defense Press Association (ESDPA). David is the author of 18 defense-related books, and is currently an IHS Jane's consultant editor and a regular correspondent for defense publications in the UK, USA, France, Poland, Brazil and Thailand.*

Thunderstorm: Drones in CBRN Detection and Terrorism

Source: http://globalbiodefense.com/2014/11/03/thunderstorm-drones-cbrn-detection-terrorism/

Nov 03, 2014 – The Department of Defense has issued a Request for Information (RFI) in support of future capability demonstration events conducted by the Thunderstorm Technology Demonstration Program.

A Tactical Unmanned Aerial System maintainer assigned to the TUAS Platoon, Company B, 3rd Special Troops Battalion, 3rd Brigade Combat Team, 101st Airborne Division (Air Assault), conducts maintenance on a "Shadow" Unmanned Aerial System at Fort Campbell, Ky. Credit: Brian Smith-Dutton 3/101 Public Affairs, courtesy of DVIDS.

Thunderstorm is a series of technology demonstrations and other activities sponsored by the Deputy Assistant Secretary of Defense, Emerging Capability and Prototyping, Rapid Reaction Technology Office (RRTO).

In FY15, Thunderstorm will focus on two areas of interest: 1) Chemical and biological detection capabilities deployed on Unmanned Aerial Systems (UAS); 2) Countering threat of UAS with chemical and/or biological WMD payloads.

Airborne Detection of Chemical and Biological Threats

The first focus area will explore emerging technologies, technical applications and their potential to use a battery-powered Vertical Take-Off and Land (VTOL) UAS to support the detection and identification of chemical and biological agents.

Highlighted capabilities of interest include:

- A system that is carried in one backpack up to systems carried/deployed from a HUMVEE-sized vehicle
- UAS payloads that can remotely detect and/or collect and transmit chemical and/or biological data to a receiving unit at least 1 kilometer from the sensing location.
- UAS operable by organic Chemical Biological Radiological and Nuclear (CBRN) unit personnel with minimal training and should be able to hover and land at or near the desired survey locations.
- Ground station capability to provide visual displays of the sensing data received from the mobile detection systems.
- Modular payload(s) capable of detecting: Standard G, H and V series chemical agents in the vapor phase and/or liquid phase on surfaces or aerosolized particles; Chemical agent precursors or degradation products, priority toxic industrial compounds and materials; Biological Warfare Agents (vegetative cells, spores and toxins); Persistent and natural flora (providing biological surveillance on current and emerging flora).
- Ground station may utilize autonomous operation (takeoff, navigation, sample detection/collection and landing) of the UAS utilizing standard geo-referenced satellite imagery that is either pre-loaded or downloaded on-demand from cellular or Wi-Fi networks. The autonomy interface should be simple enough to be learned in one day or less.
- UAS able to operate between 0 and 1000 feet above ground level (AGL) and should have a flight time of at least 30 minutes.
- Positional accuracy of UAS should be +/- 10 meters and altitude accuracy within 1 meter.

Remote collection of samples for identification and confirmation at qualified DOD laboratories is required for biological payloads and highly desired for chemical payloads.

Countering Threat of WMD Delivery by Unmanned Drones

The second focus area will explore emerging technologies, technical applications and their potential to counter a low cost, small/man portable, UAS carrying a chemical and/or biological WMD payload.
Highlighted capabilities of interest include:

- Command, Control, Communications, Computers, Collaboration and Intelligence (C5I) and sensor systems that facilitate rapid detection, identification and classification of UAS targets;
- Electronic systems that can interdict, defeat or deny hostile use of UAS.
- Systems providing the capability to intercept and neutralize the UAS. Both kinetic and non-kinetic solutions are encouraged and should cover both CONUS and OCONUS applications.

Interested parties are welcome to submit their applications to participate in both or either of the above focus areas. Technologies at all classification levels will be considered.

This RFI is for Thunderstorm Spiral 15-3 technology demonstration event, planned for 2nd Quarter Fiscal Year 2015 in Camp Shelby, MS. This event facilitates the identification of potential technology solutions to meet technical objectives. Materiel solutions brought to the event must be at a Technology Readiness Level (TRL) of 4 or greater.

The Applied Research Laboratory at Pennsylvania State University (ARL/PSU) will act as the demonstration director for Spiral 15 demonstrations and host the receipt of the application packages.

5 Drone Technologies for Firefighting

Source: http://dronelife.com/2015/04/02/5-drone-technologies-for-firefighting/

Apr 02, 2015 – Drones armed with cameras and sensor payloads have been used by military and border control agencies for decades to improve situational awareness. Commercialization now has brought more UAVs, or unmanned aerial vehicles, to market — making the technology more accessible to fire, EMS and emergency departments.

These eyes-in-the-sky can be used across public-safety services, from transmitting birds-eye video of a forest fire to incident commanders to mapping out hard-hit areas after a natural disaster. Here are five drone technologies worth watching for fire and emergency response operations.

1. ELIMCO's E300 with FÉNIX

The ELIMOC E300 is a UAV with a large payload capacity and low-noise electrical propulsion being used by INFOCA, the Andalusian authority for the management of wildfires in Spain, to track wildfires at night. The E300 can be launched remotely and operated for 1.5 hours with a radio control from up to 27 miles away. However, during night flights, the E-300 can loiter over a fire for around 3 hours and get as far as 62 miles from the launching point.

It is important to improve night wildland firefighting using technology, as a lull in firefighting efforts during the night lets wildfires expand. The night UAV with specific payloads can fly directly above the wildfire area to record video of the fire line, including thermal images that are then geo-tagged and relayed in real time to mobile command centers using the company's planning and monitoring system for forest fire fighting (FÉNIX). FÉNIX lets operators locate and address spots in a forest fire in real time using a mapping application.

2. L3 Communication's Viking 400-S

The Viking 400-S Unmanned Aircraft System (UAS) is integrated with Autonomous Take-Off and Landing (ATOL) technology supplied by L-3 Unmanned Systems' flightTEK system. The UAS operates for up to 12 hours and can be equipped with up to 100 pounds of payload technologies, including chemical, biological, radiological and nuclear detectors for hazmat emergencies.

The CBRN payload would let a first responder stay up to 70 miles line-of-sight away from a hazmat incident and, instead, send a drone to collect CBRN information from the scene and transmit it wirelessly back to incident command. UAS units carrying high-resolution cameras can capture bird's-eye images of a manmade or natural disaster, which can help incident commanders identify hard-hit areas and prioritize resources.

Images captures are transmitted wirelessly back to into a GIS software suite for mapping an affected area and later reporting needs.

3. **Information Processing Systems' MCV**

Information Processing Systems (IPS) Mobile Command Vehicles and incident command mobile carts are deployable, customized, public-safety vehicles that integrate aerial, ground and subsurface remotely controlled robotic platforms. MCVs basically are custom mobile ground control station for UAVs and other public-safety robotics.

They are modified Ford trucks that can house security cameras, sensors, radar and communication infrastructure. The truck can be outfitted with trailers to carry drones, which then can be commanded from within the center.

Having a mobile command center for drone deployment allows wildland firefighters working in remote areas to take their entire communication system with them to launch a UAV or drones over a wildfire and map out affected areas.

In urban areas, an aerial video provides actionable information so commanders can make informed decisions at the response site — whether at a bombing or a hurricane. Chiefs running structural fires could send the truck to four-alarm fires where UAVs conduct a 360-degree investigation of the fire scene before firefighters enter buildings.

4. **Sensefly's eBee**

Switzerland-based Sensefly's eBee drones are tiny compared to other drones; they have a 37.8-inch wingspan and weigh 1.5 pounds. The foam airframe eBee drones are equipped with a rear-mounted propeller and feature a 16-megapixel camera to shoot aerial imagery at down to 3cm/pixel resolution.

The drone as a flight time of up to 45 minutes, which is long enough to cover as far as 10 miles in a single flight. In addition, users can pre-program 3D flight plans using Google maps prior to deployment, with up to 10 drones controlled from a single base station. Then, using its Postflight Terra 3D-EB mapping software, it can create maps and elevation models with a precision of 5 centimeters and process aerial imagery into 3D models.

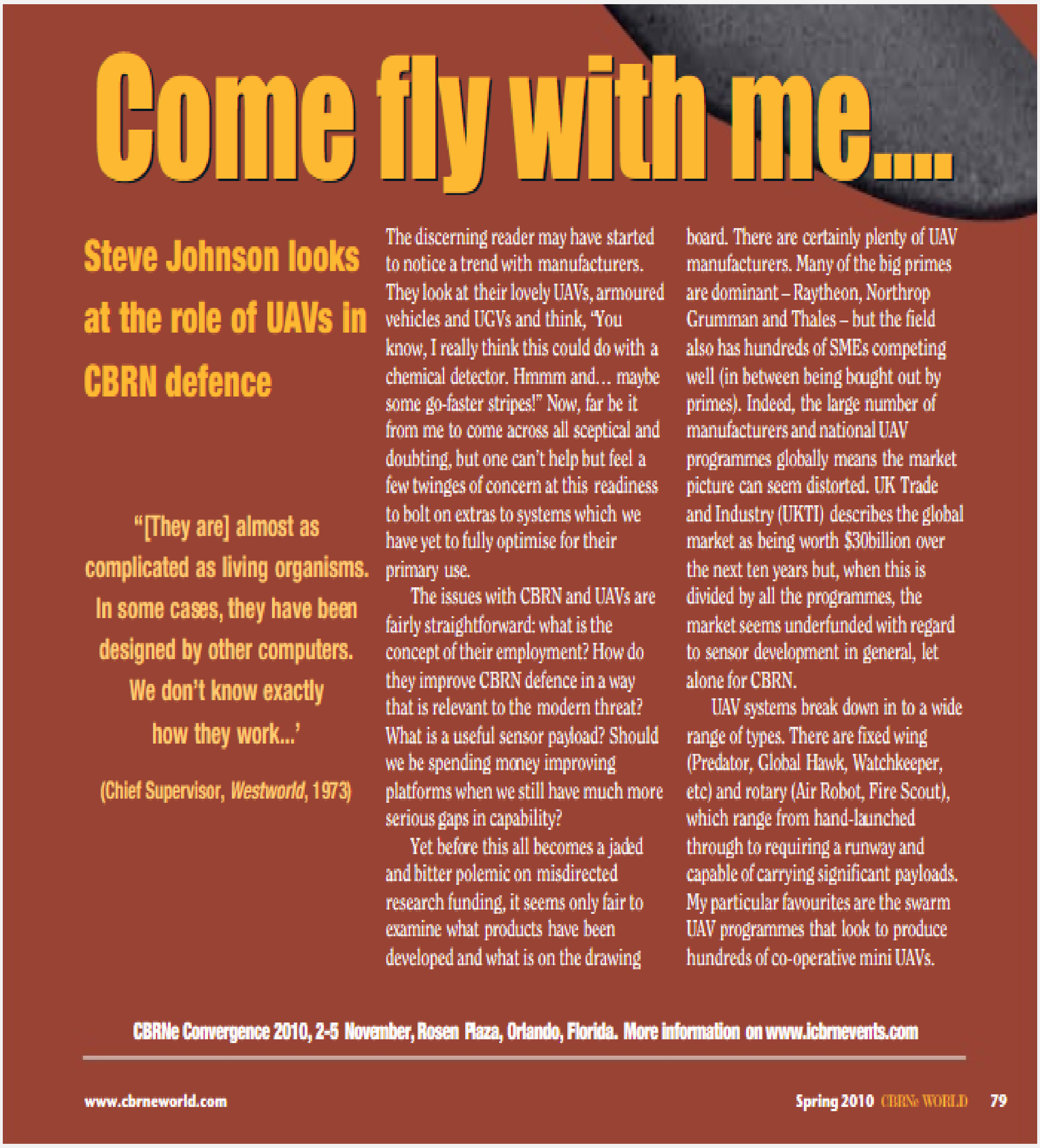
eBees could be used as a lightweight, deployable drone added to wildland firefighters backpacks for situational awareness. In the future, 3D models can be displayed on firefighters' ruggedized smartphones, which is expected in the next revision of NFPA 1802, the Standard on Two-Way, Portable (Hand-Held)

Land Mobile Radios for Use by Emergency Services Personnel. The information can be transmitted to incident command and stored for later use.

5. **Kaman's UAT**
The Unmanned K-MAX multi-mission helicopter is an Unmanned Aerial Truck based on the K-MAX heavy-lift aerial truck helicopter. The unit has 6,000 pounds of payload capacity and can move gear and personnel in and out of an area without endangering additional personnel.
Imagine providing supplies to firefighters, EMS and emergency responders in the field at a disaster with precision aerial delivery in high-wind, hot conditions without further risk to life or when personnel resources are stretched too thin. This ranges from delivering food, water, fuel, blood or even radio communications missions, such as sending the UAT to place data relay stations or communication equipment to a remote mountaintop.
With continued commercialization, drones carrying video payloads will arm first responders and incident commanders with myriad ways to capture data at a fireground, from CBRN dangers to wildfire spread, in order to better safeguard their community and emergency responders on the ground.

CBRNe World

Spring 2010 issue



Come fly with me....

Steve Johnson looks at the role of UAVs in CBRN defence

"[They are] almost as complicated as living organisms. In some cases, they have been designed by other computers. We don't know exactly how they work...'

(Chief Supervisor, *Westworld*, 1973)

The discerning reader may have started to notice a trend with manufacturers. They look at their lovely UAVs, armoured vehicles and UGVs and think, 'You know, I really think this could do with a chemical detector. Hmmm and… maybe some go-faster stripes!" Now, far be it from me to come across all sceptical and doubting, but one can't help but feel a few twinges of concern at this readiness to bolt on extras to systems which we have yet to fully optimise for their primary use.

The issues with CBRN and UAVs are fairly straightforward: what is the concept of their employment? How do they improve CBRN defence in a way that is relevant to the modern threat? What is a useful sensor payload? Should we be spending money improving platforms when we still have much more serious gaps in capability?

Yet before this all becomes a jaded and bitter polemic on misdirected research funding, it seems only fair to examine what products have been developed and what is on the drawing board. There are certainly plenty of UAV manufacturers. Many of the big primes are dominant – Raytheon, Northrop Grumman and Thales – but the field also has hundreds of SMEs competing well (in between being bought out by primes). Indeed, the large number of manufacturers and national UAV programmes globally means the market picture can seem distorted. UK Trade and Industry (UKTI) describes the global market as being worth $30billion over the next ten years but, when this is divided by all the programmes, the market seems underfunded with regard to sensor development in general, let alone for CBRN.

UAV systems break down in to a wide range of types. There are fixed wing (Predator, Global Hawk, Watchkeeper, etc) and rotary (Air Robot, Fire Scout), which range from hand-launched through to requiring a runway and capable of carrying significant payloads. My particular favourites are the swarm UAV programmes that look to produce hundreds of co-operative mini UAVs.

CBRNe Convergence 2010, 2-5 November, Rosen Plaza, Orlando, Florida. More information on www.icbrnevents.com

Could ISIS Really Attack the West With a Dirty Drone?

Source: http://www.popularmechanics.com/military/weapons/a20334/isis-dirty-drone/

Apr 08 – ISIS is planning to kill thousands of people by sending drones delivering radioactive material over Western cities—or so British Prime Minister David Cameron warned last week at a summit on nuclear terrorism in Washington. Rather than carrying a "dirty bomb" to disperse material with explosives, the drones would work like toxic crop sprayers—"dirty drones" perhaps—and cause thousands of casualties. The British PM urged other world leaders to consider urgently how they would counter this new threat.

Could the terrorist organization actually launch such an attack? To appreciate the issue, you have to know a few things about drones and dirty bombs.

Saddam's Drone That Wasn't

The threat of unmanned aircraft from Iraq spraying weapons of mass destruction may sound familiar. That's because it's exactly what Colin Powell warned us Saddam Hussein was up to in 2003: "This effort has included attempts to modify for unmanned flight the MiG-21, and with greater success an aircraft called the L-29.… Iraq could use these small UAVs which have a wingspan of only a few meters to deliver biological agents to its neighbors, or if transported, to other countries including the United States." British PM Tony Blair made the same claim in the infamous "sexed-up dossier" on Iraq he delivered to support the case for going to war.

Iraqi L-29 UAV Test-bed aircraft at Samarra East Airbase

The L-29 is a jet trainer, made in the 1960s in what was then Czechoslovakia. The Iraqis had 70 of them in their fleet of aging Eastern Bloc aircraft and apparently converted several to be flown unmanned. According to an intelligence report of the time, these could "be fitted with chemical and biological warfare (CBW) spray tanks." After the U.S.-led invasion, the Iraq Survey Group was never able to establish whether the L-29s really could have been equipped with spray tanks; instead, they may have beenused for reconnaissance or simply as surface-to-air missile training targets. (The Iraqis knew their air defences needed improving).

In any case, GlobalSecurity.org reports the Iraqis did not have much success with their improvised drone conversion. On its third flight in 1997, the L-29 flew 45 miles before the controllers lost the signal and it crashed. Subsequent attempts to correct the problem using a stabilizer cannibalized from a Chinese cruise missile were "largely unsuccessful."

A dirty bomb is not a 'Weapon of Mass Destruction' but a 'Weapon of Mass Disruption'

The Spray Drone Is the Easy Part

Fast-forward to the modern day, however, and it is vastly easier for anyone to get their hands on an unmanned crop sprayer. Agriculture has been tagged as the biggest growth area for drones, which offer low costs and high precision compared to typical spraying airplanes. Companies like HSE LLC already provide a full range of remote-control crop dusters, from the portable electric RHCD02 to the piston-engined Hercules-50 and its payload of more than 100 lbs. Spraying drones may seem exotic now, but with industry giant DJI (builders of all those obnoxious consumer drones) now making its own budget octocopter sprayer, the mantra that there will be more drones than tractors on American farms starts to looks plausible.

In addition, police forces have already adapted various drones to deliver tear gas. So in theory, spray drones with a range of several miles should be easy for terrorists to obtain.

But the spray drone is the easy part. Robert Bunker, a counterterrorism expert at TRENDS Research & Advisory, says that planning such attack is difficult because it involves several steps, all of which have to go right. "It's a more complex operation than is generally understood," Bunker tells Popular Mechanics.

To start with, ISIS would need to get its hands on highly radioactive material. In the scenario proposed by David Cameron, terrorists buy it over the Dark Web. In reality, any such WMD offer online is likely to be a sting by the authorities. ISIS has stolen some uranium from an Iraqi university, but it is the heavy kind and would not be effective if dispersed. "Putting it in a dirty bomb is a pretty silly idea," nuclear expert Bob Kelly told NBC News.

Let's says ISIS *could* get the right material. It would then need to contain the stuff safely to prevent prematurely martyring the team working on the dirty drone. Low-grade material would not be an effective weapon, but high-grade material is incredibly hazardous to work with, especially for amateurs.

Then the terrorists need to develop an effective dispersal system, one that would neither scatter the materail so widely it has no effect nor dump it all on one spot. This requires considerable expertise, plus someone who knows how to operate a crop-spraying drone.

Next ISIS would need to get in some spraying practice runs. Otherwise it would be going in blind without any idea how wind or other conditions might affect the attack. A test with inert material will only have limited value, but a live test would be far more difficult.

Finally, Bunker says, the terrorists need to carry out a surveillance of the target area and identify a suitable launch point before assembling the attack team, plus the drone and the radioactive material, and carrying out the attack. And they have to do all this without attracting the attention of the world's combined intelligence agencies, even after having acquired rare and easily-detected radioactive material. Even then, the attack would probably be disappointing for terrorists hoping to kill a lot of people.

"Terrorism dirty bomb scenarios are typically disruption as opposed to destruction attacks," Bunker tells PM. "It's about fear or panic generation, and area denial of a facility or part of a city—not about straight out killing."

Missing the Point

"A dirty bomb is not a 'Weapon of Mass Destruction' but a 'Weapon of Mass Disruption,'"—so says U.S. Nuclear Regulatory Committee's fact sheet on dirty bombs. Such an attack would force people to leave the area or stay inside, but "any additional risk [of cancer] will likely be extremely small."

"It's about fear or panic generation… not about straight out killing"

Detlof von Winterfeldt, director of the Center of Risk and Economic Analysis of Terrorism Events, has suggested that a worst-case dirty bomb attack would cause perhaps 100 cancer deaths in the long run, but generally the number of victims would be "tens" rather than "hundreds." The Homeland Security Introduction to WMD states that "a dirty bomb containing one kilogram of plutonium in the center of Munich, Germany, could ultimately lead to 120 cancer cases attributable to the blast." A dirty drone, like a dirty bomb, would not be a terrorist spectacular. Even over the course of years, it might cause fewer cancers than the massive quantities of potentially harmful dust kicked up by the 9/11 attack.

To be sure, there are killer drones out there in terrorist hands. ISIS has drones packed with explosives in Syria, and some claim drones are the new IEDs. But radioactive material would be difficult and expensive to acquire, challenging to deliver effectively, and might have more of an effect on property prices than on people.

Hackers have already fitted consumer drones with flamethrowers, firearms and even chainsaws. Terrorism is increasingly a matter of multiple attacks by several individuals, and a terror attack involving a large number of simple drones to bypass security seems more of a threat than an elaborate radioactive plot. Security agencies might do well to focus on tackling the more immediate danger presented by drones.

Jihadists and Weapons of Mass Destruction

Gary Ackerman and Jeremy Tamsett

February 3, 2009 by CRC Press

Reference - 494 Pages - 28 B/W Illustrations

Source: https://www.crcpress.com/Jihadists-and-Weapons-of-Mass-Destruction/Ackerman-Tamsett/p/book/9781420069648

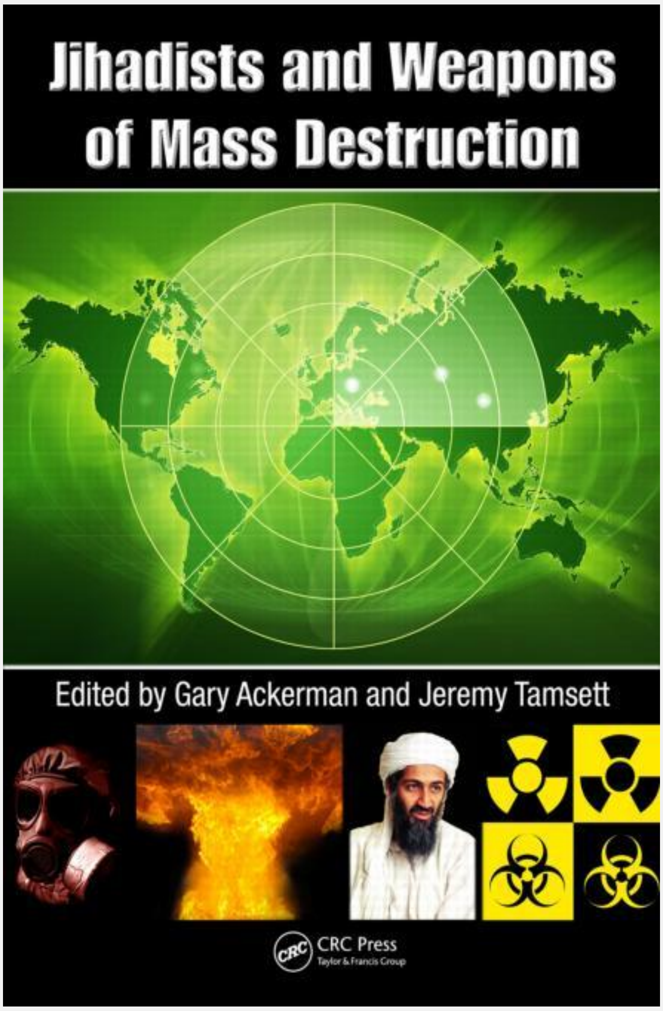
Features

- Documents current trends in the ideology, strategy, and tactics of jihadists as these relate to WMD
- Includes a section devoted to jihadist involvement with chemical, biological, radiological, and nuclear weapons
- Explores the role of intelligence, law enforcement, and policymakers in anticipating, deterring, and mitigating WMD attacks
- Provides an overview of nonproliferation policies designed to keep WMD out of the hands of jihadists
- Conducts a groundbreaking quantitative empirical analysis of jihadist behavior
- Elicits leading experts' estimates of the future WMD threat from jihadists

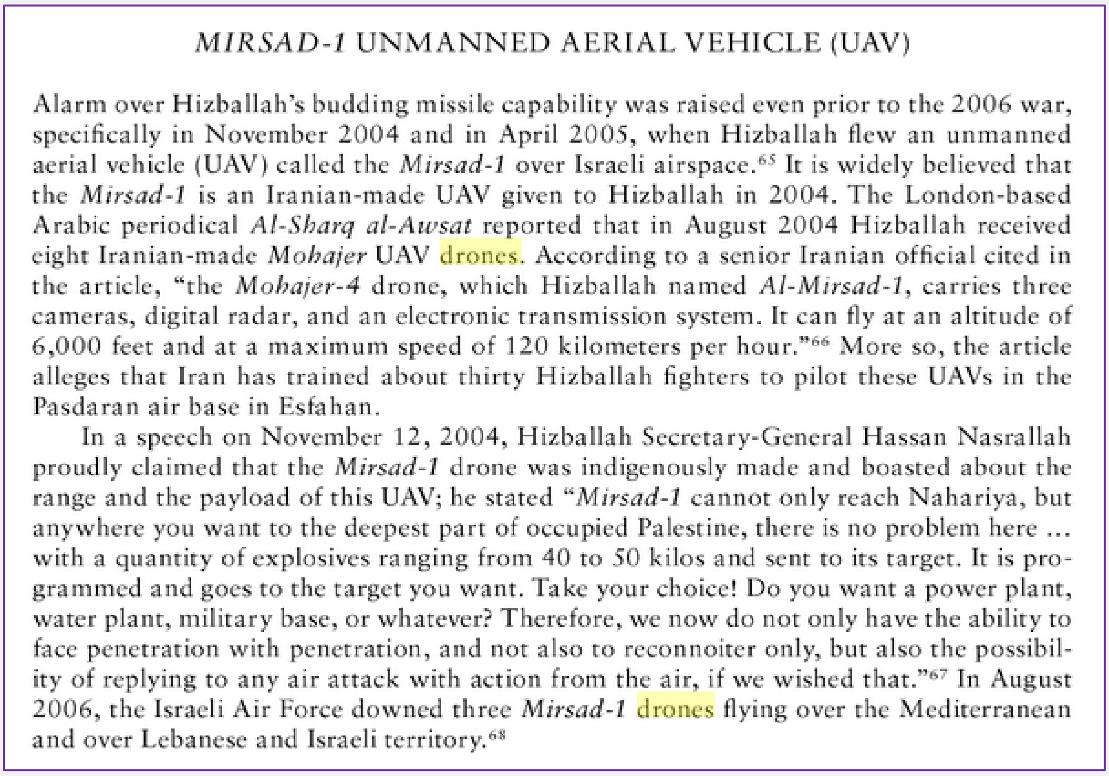
Summary

Explores the Nexus Formed When Malevolent Actors Access Malignant Means

Written for professionals, academics, and policymakers working at the forefront of counterterrorism efforts, **Jihadists and Weapons of Mass Destruction** is an authoritative and comprehensive work addressing the threat of weapons of mass destruction (WMD) in the hands of jihadists, both historically and looking toward the future threat environment. Providing insight on one of the foremost security issues of the 21st century, this seminal resource effectively:


Jihadists and Weapons of Mass Destruction
Edited by Gary Ackerman and Jeremy Tamsett
CRC Press
Taylor & Francis Group

- Documents current trends in the ideology, strategy, and tactics of jihadists as these relate to WMD
- Includes a section devoted to jihadist involvement with chemical, biological, radiological, and nuclear weapons
- Explores the role of intelligence, law enforcement, and policymakers in anticipating, deterring, and mitigating WMD attacks
- Provides an overview of nonproliferation policies designed to keep WMD out of the hands of jihadists
- Conducts a groundbreaking quantitative empirical analysis of jihadist behavior
- Elicits leading experts' estimates of the future WMD threat from jihadists



MIRSAD-1 UNMANNED AERIAL VEHICLE (UAV)

Alarm over Hizballah's budding missile capability was raised even prior to the 2006 war, specifically in November 2004 and in April 2005, when Hizballah flew an unmanned aerial vehicle (UAV) called the *Mirsad-1* over Israeli airspace.[65] It is widely believed that the *Mirsad-1* is an Iranian-made UAV given to Hizballah in 2004. The London-based Arabic periodical *Al-Sharq al-Awsat* reported that in August 2004 Hizballah received eight Iranian-made *Mohajer* UAV drones. According to a senior Iranian official cited in the article, "the *Mohajer-4* drone, which Hizballah named *Al-Mirsad-1*, carries three cameras, digital radar, and an electronic transmission system. It can fly at an altitude of 6,000 feet and at a maximum speed of 120 kilometers per hour."[66] More so, the article alleges that Iran has trained about thirty Hizballah fighters to pilot these UAVs in the Pasdaran air base in Esfahan.

In a speech on November 12, 2004, Hizballah Secretary-General Hassan Nasrallah proudly claimed that the *Mirsad-1* drone was indigenously made and boasted about the range and the payload of this UAV; he stated "*Mirsad-1* cannot only reach Nahariya, but anywhere you want to the deepest part of occupied Palestine, there is no problem here ... with a quantity of explosives ranging from 40 to 50 kilos and sent to its target. It is programmed and goes to the target you want. Take your choice! Do you want a power plant, water plant, military base, or whatever? Therefore, we now do not only have the ability to face penetration with penetration, and not also to reconnoiter only, but also the possibility of replying to any air attack with action from the air, if we wished that."[67] In August 2006, the Israeli Air Force downed three *Mirsad-1* drones flying over the Mediterranean and over Lebanese and Israeli territory.[68]

Leading international experts clearly differentiate between peaceful Muslims and jihadists, exploring how jihadists translate their extreme and violent ideology into strategy. They also focus on WMD target selection and the spread of WMD knowledge in jihadist communities. Devoid of sensationalism, this multidimensional evaluation adds a heightened level of sophistication to our understanding of the prospects for and nature of jihadist WMD terrorism.

***Gary Ackerman** is Research Director of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a Department of Homeland Security National Center of Excellence based at the University of Maryland. His research work focuses on threat assessment and terrorism involving unconventional weapons.*

***Jeremy Tamsett** is a consultant for Henley-Putnam University and an analyst at the Center for Terrorism and Intelligence Studies (CETIS), a research center dedicated to identifying, better comprehending, and accurately assessing the present and future security threats stemming from a variety of violence-prone extremists and their enablers. He has served as Project Manager for the U.S. Government funded Critical Infrastructure Terrorist Attack database and Global Terrorism Database (GTD).*

How to Respond to the Threat from Hostile Drones in the UK

By Chris Abbott and Matthew Clarke

Source: https://sustainablesecurity.org/2016/03/04/how-to-respond-to-the-threat-from-hostile-drones-in-the-uk/

March 04 – Islamic State (IS) has used aerial drones for reconnaissance and battlefield intelligence in Iraq and Syria and has attempted to use aerial and ground drones with explosive payloads to attack Kurdish troops. IS-directed or -inspired attacks in Australia, Canada, Denmark, the United States and France and failed or foiled attacks elsewhere, including the United Kingdom, have demonstrated the group's desire to attack targets outside the Middle East. Given that threat is a function of *capability* and *intent*, should we therefore be concerned about the possibility of Islamic State or another terrorist group using drones to attack Western cities? A recent report from the Remote Control project and Open Briefing examined this scenario, among others.

The Drone Threat

For *Hostile drones*, the Open Briefing team assessed the capabilities of over 200 commercial and consumer/hobbyist drones capable of operating in the air, on the ground or on or under the sea. Although limited at present, they found that there are consumer drones available today that are capable of delivering an explosive payload equivalent to a pipe bomb (1-4 kilograms) or a suicide vest (4-10 kilograms). Many more could be modified with readily-available components to increase their stated payload capacity. If used in a swarm against the crowd at a major sporting event, for example, they would cause serious injury and multiple fatalities. If one or more of the drones carried on-board cameras to record the event, it would also provide a group such as Islamic State with prime propaganda material.

Using drones for terrorist attacks has several advantages over conventional methods, including removing the need to convince a suicide bomber to carry out an attack and opening up targets a bomber would not usually be able to access due to security. An attacker would not even necessarily need to weaponise a drone, as the vehicle itself could be used as a projectile to target a light aircraft's engines on take-off or landing, for example. In addition to attack, Open Briefing identified intelligence gathering as another major capability that drones offer terrorists or insurgents, as demonstrated by Hezbollah, Hamas and Donetsk separatists. For example, Donetsk People's Republic militias reportedly possess and deploy sophisticated Russian-made Eleron-3SV drones for intelligence, surveillance and reconnaissance (ISR) in eastern Ukraine. Drones provide insurgent groups with an excellent level of battlefield awareness and provide terrorist groups the ability to reconnoitre a target before an attack These same capabilities are also of interest to criminal, corporate and activist threat groups. For example, aerial drones have been used to transport illicit drugs over the Mexico-US border and in April 2015 a man protesting over the Japanese government's nuclear energy policy landed a drone containing radioactive sand on the roof of the prime minister's office in Tokyo.

The same technology Western militaries have been controversially employing to target terrorists in Afghanistan, Pakistan, Yemen, Iraq and elsewhere for years is now being used by various threat groups to target Western interests. This is a prime example of how the tactics and technologies of remote-control warfare have created unintended consequences for those countries that have embraced them.

Towards Drone Countermeasures

No single countermeasure is completely effective at limiting the hostile use of drones by non-state actors. Open Briefing therefore proposes the United Kingdom adopt a hierarchy of countermeasures encompassing regulatory, passive and active countermeasures, which provides a layered defence. Regulatory countermeasures include point of sale regulations, civil aviation rules and manufacturing standards and restrictions. Passive countermeasures include early warning systems and signal jamming. Active countermeasures include kinetic defence systems, such as missiles, rockets and bullets, and less-lethal systems, such as projectile weapons and net guns. Each stage of the hierarchy of countermeasures requires government action, but it is the regulatory countermeasures upon which it can affect the greatest change.

Any changes to the laws surrounding the use of drones need to be proportionate to the risks and balance interests relating to privacy, individual freedoms, safety and commercial interest. In addition to the existing regulations around drones needing to be flown within visual line of sight, below 400 feet and not within 50 metres or a person, vehicle or building, there have been calls from airline pilots and politicians for a registration scheme for consumer drones and for the adoption of firmware limitations that restrict the ability of drones to travel near geofenced no fly zones around sensitive sites, such as airports or nuclear power stations. These are reasonable demands that should be implemented as soon as possible.

However, these regulations may have limited impact beyond reducing accidental incidents. Unless coupled with some kind of identification/tracking technology built in to drones, a registration scheme would not remove consumer drones from the terrorist arsenal altogether (in any case, such technology would be a step too far in terms of state surveillance and could be easily disabled). What registration would do is impose some control on a presently uncontrolled market and impress upon drone operators the responsibility they must take for their actions. It may also reduce the supply of readily-available drones that could be used for nefarious purposes. In the case of geofenced no fly zones, those wishing to carry out an intentional attack could still purchase open-source controllers that can bypass geofencing, and inertial navigation systems (using dead reckoning) would allow a drone to continue to a static target with reasonable accuracy even if it were possible to jam controller frequencies and GPS signals within the target perimeter. What geofencing would allow is for security to assume that any drone operating within the no fly zone is unauthorised and potentially hostile, allowing them to react appropriately (evacuation and/or deploying active defences).

There are two further regulations that have received little attention but which should also be considered. Firstly, the payload capacity of the *consumer* drones available for purchase or import in the United Kingdom without licence should be legally limited to that reasonably required to carry a camera and nothing else. This would mean these types of drones could not be used to carry explosive payloads without further modification. Secondly, owners of *commercial* drones capable of carrying heavier payloads for legitimate reasons (such as in agriculture or search and rescue) should be legally required to store them securely (in the same way fertiliser must be appropriately secured to prevent its use in homemade bombs, for example). This would prevent the theft and use of drones capable of carrying considerable explosive payloads by terrorists and other threat groups.

A Layered Defence

The current regulatory regime around drones in the United Kingdom is very limited. The adoption of the four regulations outlined above would balance the various interests and address specific risks without being unduly restrictive. However, regulations are not a panacea – they would merely limit the ability of terrorists and others to acquire drones with the capabilities needed for attack or intelligence gathering. That is why the government must also work with the police, security services and industry to explore the passive and active countermeasures that are needed to protect VIPs or sensitive sites and ensure that procurement and R&D funding is made available to purchase or develop the required systems. This should include the development of less-lethal systems for destroying or disabling hostile drones in urban environments, where little warning of an attack and the risk of collateral damage limits the usefulness of conventional kinetic countermeasures, such as missiles or bullets. Again, though, this will not be a panacea: the less-lethal systems currently available are of limited effectiveness against one or more fast-moving, small drones. As with all the possible countermeasures, such systems – if coupled with early-warning – would form part of an effective layered defence.

Ultimately, the regulations and technology needed to reduce the threat from the hostile use of drones are either available now or are under development. The British government has to act now to bring drone regulations up to date and invest in the technologies needed to keep us safe. In the meantime, the threat from the malicious use of civilian drones is only going to increase.

***Chris Abbott** is the founder and executive director of Open Briefing (www.openbriefing.org).*
***Matthew Clarke** is an associate researcher at Open Briefing.*

Defense Bill Has Nuclear Facilities Fighting Drones

Source: http://www.defensenews.com/story/defense/policy-budget/congress/2016/05/07/defense-bill-has-nuclear-facilities-fighting-drones/83931328/

May 07 – As US regulators grapple with the safety, privacy and national security concerns posed by a boom in the use of recreational drones, lawmakers worried about their use for malicious ends have advanced legislation aimed at letting Defense Department and Energy Department facilities defend themselves against them.

Two provisions contained in the 2017 National Defense Authorization Act would extend broad new authorities to the agencies to stop unmanned aerial vehicles deemed a threat to their facilities dedicated to nuclear power and weaponry. The authorities would dovetail with DoE and DoD's early efforts to develop technology that would discern small drones from birds and take them out.

"That is a very aggressive approach, and one we have yet to see in federal regulations," energy and infrastructure attorney Roland Backhaus, with the firm Pillsbury Winthrop Shaw Pittman, said of the bill.

While the US Federal Aviation Administration has yet to report any serious incident involving a drone at a nuclear facility, fears and speculation have been fueled by a commercial quadcopter's crash landing on the White House lawn last year, and a Massachusetts man's guilty plea in 2012 to plotting attacks on the Pentagon and US Capitol building with an explosive-laden model plane.

Drones reportedly buzzed nuclear facilities around France 32 times over two months in 2014, according to a report commissioned by Greenpeace, sparking concern the country's nuclear reactors are unsafe from aerial assaults and jangling nerves in other nations about the potential threat.

Unmanned aerial systems (UAS) small enough to elude radar could be used "by criminals and terrorists" to attack or spy on "critical government and industrial facilities," according to a Jan. 27 Congressional Research Service report. "Somewhat larger UAS could be used to carry out terrorist attacks by serving as platforms to deliver explosives or chemical, biological, radiological, or nuclear weapons," said the report, by aviation policy specialist Bart Elias.

Taking no chances given the devastation that could be wrought at such a facility, House Armed Services Committee (HASC) strategic forces subcommittee chairman Mike Rogers, R-Ala., included the two counterdrone provisions in the 2017 NDAA, which the HASC approved April 28.

"The bottom line is the members are tracking the increased prevalence and sophistication of unmanned aerial systems around the country, and they understand the threat these can pose to certain defense facilities," said a congressional staffer.

DoE has 10 active sites across the country that handle the US arsenal of nuclear weapons and material, while DoD controls nuclear missile fields, silos, underground storage and maintenance, as well as nuclear reactors for training and research.

"The chairman is interested in protecting these facilities. It would be a bad day if something happened," the staffer said.

The massive defense policy bill has several hurdles before it becomes law. The language would have to survive a vote on the House floor and reconciliation with the Senate bill due later this month. The reconciled bill will face a vote in both houses of Congress and must be signed by the president.

Under the bill's mandate for DoD, the defense secretary would develop a means to disrupt, seize, confiscate, control, disable or destroy drones deemed a threat to facilities related to nuclear deterrence, missile defense or the national security space mission.

For DoE, personnel and contractors who think a drone presents "a threat to people, property, or classified information" at a facility that stores or uses special nuclear material would be allowed to "mitigate the threat from, disable, interdict, interfere with" its operation. It varies by DoE facility, but most are operated by private contractors, and physical security is generally provided by third-party companies.

Lawmakers don't mean to encourage the shooting down of drones, and while the bill permits DoE to do it, its language discourages the use of force in favor of "appropriate escalation," saying "non-kinetic responses should be utilized when feasible to mitigate a threat."

An FAA spokesman declined to comment on the pending legislation, but had this to say:

"Generally, shooting at any aircraft — including unmanned aircraft — poses a significant safety hazard. An unmanned aircraft hit by gunfire could crash, causing damage to persons or property on the ground, or it could collide with other objects in the air."

The legislation comes as federal agencies have been waiting for the FAA to carve out security-based rules for drones, a step mandated by law in 2013. In the meantime, an FAA notice strongly advises pilots of airplanes and drones to avoid — and not "circle or loiter" in — the airspace of critical infrastructure, such as power plants, military bases and prisons.

Many interested parties are watching this space, including federal agencies, security contractors, nuclear facility operators and drone manufacturers — which are looking into geo-fencing software for a UAS to steer itself away from an off-limits area.

"With this opportunity for DoE to take a more aggressive approach, one wonders if this same approach would not get picked up by operators of sensitive facilities, nuclear or otherwise," Backhaus said.

According to a market survey performed by Sandia National Laboratories, the DoE research and development wing, a variety of means exist to detect, identify and neutralize a slow- and low-flying UAS — sophisticated sensors, high-energy lasers and signal jammers, water cannons, firearms and trained birds of prey.

There is still key research and development to be done in this sector, according to the counter-UAS (CUAS) survey. It concluded that differentiating targets from background clutter is a problem for existing technology, and that "no complete system appears to exist with evidence of acceptable performance."

Sandia in March announced it wants CUAS vendors to loan their equipment for testing and evaluation, to determine their suitability for "various security installations." **The CUAS would target systems that fly slow and slow, and weigh less than 55 pounds.**

DoD is also interested in the capability. The US military has since 2010 been conducting its annual Black Dart exercises at Naval Base Ventura County, California, to test a variety of UAS countermeasures.
During an April visit to Naval Submarine Base Kings Bay, Georgia, Deputy Defense Secretary Bob Work expressed concern about small drones being able to penetrate the security at nuclear missile and submarine bases nationally.
Although Work spoke broadly, he did call out a program in the Netherlands — run by a company called Guard From Above — that uses birds to take out small drones around nuclear power sites as a particularly interesting idea. Kings Bay already uses dolphins to spot any potential underwater threats to the nuclear sub fleet housed there.
Air Force Global Strike Command, which manages the US' nuclear arsenal, awarded a $75,000 contract for portable systems to counter personal drones to XCOM Wireless, of Long Beach, California, in January. The Air Force solicited a system to disrupt the navigational signals of a "wide range" of UAS targets and minimize collateral effects on friendly assets.

ISIL Plotting To Use Drones For Nuclear Attack On West

Source: http://freerock.uk/isil-plotting-to-use-drones-for-nuclear-attack-on-west

Apr 22 – **ISIL terrorists are planning to use drones to spray nuclear material over Western cities in a horrific "dirty bomb" attack,** David Cameron has warned.
World leaders are concerned that jihadists want to buy basic drones that are widely available online to transport radioactive material into the heart of major cities in a strike that could kill thousands.
The Prime Minister warned that the dangers of Islamic State of Iraq and the Levant (Isil) getting hold of nuclear material was "only too real".
Mr Cameron on Friday met world leaders, including the presidents of America, France and China, to plan how they would react to such an attack .
Footage has reportedly emerged showing Isil using drones and the threat was deemed so serious that – in a highly unusual move – world leaders were asked to take part in war games to plan how they would respond.
One scenario, mapped out by US officials and presented at the special Nuclear Security Summit session in Washington DC, spelt out the danger in remarkable detail.
It imagined radioactive material had been taken from a medical facility by "insiders" and sold to extremists through the internet's secretive "dark web".
Mr Cameron outlined how ministers would urgently hold a Cobra meeting and deploy counter-terrorism police and the UK Border Force. A British official said: "We have already seen Daesh [another name for Isil] trying to look at whether they can they get their hands on low-level crop-using-type drones."
Isil is believed to have seized around 90 pounds of low grade uranium from Mosul University in Iraq after taking over the city in 2014, though its limited toxicity means its use would likely cause panic than serious harm.
In Europe, fears have also been raised by apparent attempts to infiltrate nuclear facilities. Mr Cameron told journalists in Washington DC that concerns over a radioactive attack were real.
"So many summits are about dealing with things that have already gone wrong," he said. "This is a summit about something we are trying to prevent.
"The issue of nuclear security and the security of nuclear materials, particularly when it comes to the problems of international terrorism, the concept of terrorists and nuclear materials coming together – which is obviously a very chilling prospect. And something in the light of the Belgian attacks, we know is a threat that is only too real.
"That's the point of being here and that action Britain has taken with America, very much giving a lead on nuclear security, and the security of nuclear sites, transport and materials."
During the nuclear summit it emerged that US commandos have been trained to seize and disable radioactive bombs.
Mr. Cameron announced during his visit that Britain would hire 1,000 more armed police and deploy counter-terrorism units in cities outside London to help counter any future attack.

Small Drone Carries Any Payload You Want

Source:http://www.nationaldefensemagazine.org/archive/2012/October/Pages/SmallDroneCarriesAnyPayloadYouWant.aspx

Oct 2012 – Front-line troops have a growing appetite for small drones that they can launch by hand. Now, a new aircraft has been thrown into the field to compete with the Ravens and Pumas already being used by the military.

The Four Delta small unmanned aircraft system (SUAS) has a wingspan of 5.8 feet and weighs less than 3 pounds. It can carry a variety of payloads, from daylight cameras and thermal infrared sensors to chemical, biological, radiation and nuclear detectors.

“Most all SUAS are built around a specific payload and are mono-mission,” said Jeff Imel, founder of Air Robotics, which is based in Charleston, W.Va. That single mission generally is intelligence, surveillance and reconnaissance, but Air Robotics has developed a special pod that allows customers to switch out existing payloads for whatever the situation requires.

“The Four Delta can be daylight ISR one mission, then land, swap payload pods to a CBRN payload and conduct a remote-sensing operation,” Imel said. “This saves customers money and time by not needing to purchase a different SUAS for each specific payload they wish to carry.”

The Four Delta can fly for up to two hours at a time over a range of six miles. It operates at an average altitude of 1,000 feet and can reach speeds of up to 60 knots. It is built to withstand the hard landings and crashes common to smaller drones. The payload pod and wings are designed to detach when jarred by a wreck.

A video shows Imel purposely sending the Four Delta nose-diving into the ground to test the airframe’s durability. After more than a dozen crash tests, Imel is seen re-attaching a wing without any tools and launching the Four Delta up into the air for another flight.

What if Isis launches a chemical attack in Europe?

Source: https://www.theguardian.com/global/commentisfree/2015/nov/27/isis-chemical-attack-europe-public

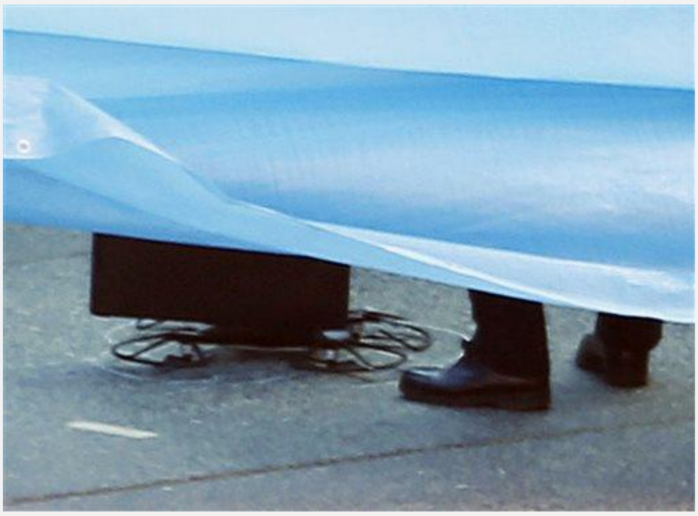
Nov 27, 2015 – The UK government must consider the possibility of an Islamic State attack on its territory with unconventional weapons. As Europe debates how to deal with Isis in the aftermath of the Paris attacks, Isis is revelling in what it considers success, and is undoubtedly planning the next assault. Only that the next strike may be just as Isis vows: more lethal, even more shocking, it may just be one where the internationally banned abhorrent weapons of mass destruction are used. The UK, and other states fighting Isis, need to be on alert.

French prime minister Manuel Valls has already warned the French parliament that Isis may use chemical and biological weapons in future, in a speech aimed at seeking parliamentary approval to extend a state of emergency. Valls’ office stressed that his mention of the possibility of a chemical weapons attack was “not new information on the status of the threat, just a realistic observation”. “Middle East experts know that Daesh [Isis] seeks and uses chemical weapons,” a spokesman told Le Monde. “To not consider this possibility would be a mistake.”

On 14 November the French government authorised the use of atropine sulfate, which can be used as an antidote in the event of chemical attacks. The British government is yet to announce any such measures. Security around Paris's water supply recently increased following concerns that they might be vulnerable to a unconventional attack.

Japan radioactive drone: Tokyo police arrest man

Source: http://www.bbc.com/news/world-asia-32465624



Apr 25, 2015 – A man who flew a drone carrying radioactive sand on to the roof of the Japanese prime minister's office has been arrested, Tokyo police say.

Yasuo Yamamoto, 40, was protesting over the Japanese government's nuclear energy policy. He turned himself in late on Friday, police said.

No-one was hurt. Prime Minister Shinzo Abe was out of the country.

The drone landing triggered a security alert and raised fears of extremists using drones to carry out attacks.

The small amount of sand in the drone - which was equipped with a small camera - carried traces of radiation.

Police said the radioactive material was likely to be caesium but the levels were too low to be harmful to human health.

Japan does not yet regulate low-altitude drone flights except around airports. However, officials are looking into changing the law as the remote-controlled devices become more popular.

Japan shut down all 48 of its nuclear power plants after the tsunami and earthquake in March 2011 which wrecked the Fukushima power plant.

Previously, about 30% of Japan's power was nuclear-generated.

Prime Minister Shinzo Abe has lobbied for a restart, arguing that the shutdown has hurt the economy by forcing Japan to import expensive fossil fuels to make up the power shortfall.

But public anxiety about the safety of nuclear power remains high.

None of the plants has yet re-started. However, last week a Japanese court rejected an attempt by local residents to halt the restart of two nuclear reactors at the Sendai plant in Kagoshima prefecture.

Using Unmanned Aerial Vehicles (UAVs) for CBRN Reconnaissance

Source: http://www.cbrneportal.com/using-unmanned-aerial-vehicles-uavs-for-chemical-biological-radiological-nuclear-cbrn-reconnaissance/

Oct 10, 2013 – Due to the rapid advancement in UAVs and experience that has been gained by many nations involved in contemporary operations worldwide; CBRN detection in its current form is very likely to experience a fast transition towards a decade of new capabilities. Generally in the past the main focus has been concentrated around mounted and dismounted CBRN reconnaissance. With the emergence of new technologies and the focus on force protection in all operations; capability requirements are now addressing a new topic of unmanned platforms (UP) as part of CBRN Defence operations.

The operation of UP by armed forces is nothing new; the topic of drones has been prominent in world news and despite some bad press, UP has clearly contributed to the success of many an operation. The CBRN domain however, has seen limited UP utilisation. Although several unmanned ground vehicles (UGV) and robots have been equipped with a variety of sensors, the utilisation of flying platforms (UAV, rotary and fixed-wing) still seems to be a challenging topic.

Within the given CBRN context it must be pointed out that UGV will for sure not be High Altitude Long Endurance/Medium Altitude Long Endurance (HALE/MALE: operation above 15.000m/ operation between 5.000m – 15.000m) but could be categorised as a Tactical UAV (TUAV; operation up to 5.000m) or VTOL (Vertical Taking Off and Landing: operation up to 4.500m). This comprises rotary wing as well as fixed-wing solutions. Whatever the propulsion concept will be, the restrictions (buzzword: legal aspects) and limitations (in particular payload) will probably be the same for both concepts. Despite these challenges, Bruker has forged ahead together with an integration company experienced on working with UAVs to set-up a R&D project. Bruker teamed-up with the German company ESG with the aim to combine the μRAID (Rapid Alarm and Identification Device) chemical sensor with the UMAT (Unmanned Mission Avionics Test Helicopter) VTOL UGV. The focus of this ongoing project is to confirm the feasibility of mounting a C-sensor in a VTOL and develop a solid base for future tests.

Using the VTOL as the platform for this R&D activity provides a variety of advantages. Among others the vertical landing capability, the hovering mode as well as the availability of a multi-role payload bay serve as good examples.

From the technical perspective the biggest challenge was to combine the avionic flight system of the UAV, the chemical sensor system and the wireless communication link while guaranteeing the absence of any mutual interference. Crucially it was not known to what effect rotor movement would influence detection performance. As such, intensive ground and preparatory flight tests were conducted. These tests resulted in the design and production of a nose mast (see picture) that acts as an air inlet and negates the negative impact that the rotors have on detector air/gas intake.

So far the project is on time and despite some bespoke developments, there have been no significant setbacks. The next milestone will be to conduct a scheduled series of test flights, including the final confirmation of in-flight chemical detection capability. This series is scheduled to take place later this year.

Looking to the future, the intention of both companies, ESG as well as BRUKER, is to continue with this project. Our aim is to further exploit the CBRN detection capability of the "UMAT" VTOL in order to gain further understanding of the potential that UP can offer. The integration of additional C and R sensors will be accompanied by the development, description and assessment

Drones – terror from the skies

Lt. Gen. Prakash Katoch

Source: http://icast.org.in/news/2015/jul15/jul17NDT.pdf

July 16, 2015 – There was commotion in Tokyo this April when a drone with traces of radioactive material, a bottle with unspecified contents and mounted with a camera was discovered on the roof of Prime Minister Shinzo Abe's office. The 50cm diameter drone had a symbol that warned of radioactive material. Japan's Chief Cabinet Secretary, Yoshihide Suga, said the incident was a wakeup call to the potential dangers of drones including possible terror attacks. Earlier in January 2015, a drone had crashed on the White House grounds, raising questions about safe use commercial and consumer drones in the US. Significantly, Japanese aviation laws have had no restrictions for unmanned drones flying at or below 250 metres above ground except along flight routes. But now with a drone landing on the roof of the Prime Minister's office, a comprehensive review is underway. The magnitude of terror that drones can unleash may can be gauged from the fact that the Aum Shirikyo cult that executed multiple Sarin Gas bombings on Tokyo subway in 1995 was later found to have possessed two remote controlled helicopters and enough Sarin Gas to kill one million people. It was just providence that during practice, both helicopter drones crashed and the cult went had to execute the bombings nn foot. But why to talk of a cult or group of people, a recent study in the US brings home the chilling conclusion that one single disciple of 'Lone Wolf Terrorism' is capable of killing millions.

We have been hearing of drone strikes in Af-Pak region for decades now. They are also common fare in the Middle-East, particularly Syria and Iraq. Armed drones are an efficient method of striking terrorists, avoiding large scale collateral damage compared to aerial and artillery bombardment. Israel has been using armed drones to take out Hamas terrorists.

As modern conflict involves more and more employment of irregular forces, we witness nore and more use of drones. In 2014, 25 x US drone strikes in Pakistan reportedly killed between 114 to 183 individuals (including two civilians and two children) while 44 to 67 were reported injured. Interestingly in the decade 2004-2014, Wikipedia describes 357 x Obama strikes and 408 x total US strikes since 2004 killing between 2,410 to 3,902 individuals (including 416 to 959 civilians and between 168 to 204 children) while injuring between 1,133 to 1,706 individuals. This shows the intensity and effectiveness of use of drones in irregular conflict situations.

But a drone strike requires accurate intelligence which may not be available always. For example, a US development expert, Warren Weinstein, and an Italian aid worker, Giovanni Lo Porto, got accidentally killed in January this year when a US drone attacked an Al Qaeda compound in Pakistan where they were being held captive past several years. This sparked a lot of questions about drones being used in this type of conflict situations, especially when the intelligence that underpinned the said drone strike was incomplete.

But where drones are being used for counter-terrorism, they are also available to terrorists. Israel has been reporting Iranian origin drones with Hamas. Interestingly, an attempt was made in 2009 to deliver drugs to prisoners using a drone in a UK prison guarded by a 50 feet high electric fence. Two years later, Rezwan Ferdaus, an al-Qaeda affiliate, planned an attack on the Pentagon and Capitol buildings using a remote-controlled drone laden with explosives but the plot was intercepted before it could be executed. In 2012, criminals piloted a $600 remote-controlled quad-copter was piloted over a Brazilian prison to deliver cell phones to the prisoners. In recent months, the New York Police Department (NYPD) has been increasingly concerned about a potential terror attack from the air through a drone armed with a deadly weapon. The spurt in NYPD's concern about drones came amidst increased drone incidents in New York City. In 2014, a drone flew towards the podium and landed in front in Germany when German Chancellor Angela Merkel was delivering a speech. Then this summer, an NYPD night patrol helicopter flying at an altitude of 800 feet above ground level was suddenly confronted by a drone. The difficulties in combating such threats are obvious. It is not only a question of detecting drones especially during dark but also the payload and most significantly, the intention. Presently, NYPD is looking for technology which will allow them to take control of drones as well as scan the skies for them before major events, and stop potential attacks.

A democracy like India with less than requisite controls needs to acknowledge this threat seriously. In October 2014, the DGCA had announced that till proper rules and regulations are formulated, use of drones in the country is "illegal" but the problem as always is in implementation. In the US, while Amazon had successfully conducted test bed for delivery of items at the customer's doorsteps, it is prohibited to use drones till regulations for use of drones are revamped and promulgated in US. In contrast, there is little monitoring and prosecution in India, notwithstanding odd report about arrest in such cases. Last year, four individuals were caught filming the Ganga Arti in Varanasi using drone cameras without permission (photo). They admitted they had already done similar filming using cam-copter for a travel channel at Allahabad, Varanasi, Shimla, Manali and Agra, and that the filming team included foreigners. The cam-copter at Varanasi was observed and so the persons could be apprehended, but at other places such filming was unhindered.

Drones are being used in the country for shooting concerts and movies, filming private parties, by police organizations for surveillance and monitoring traffic, and for surveillance and intelligence gathering by armed forces. During Republic Day Parade of 2015 with President Barak Obama as Chief Guest, there were warnings that terrorists may attempt drone strikes, even using a glider. Similar warnings have been given by intelligence agencies in the recent past, particularly with respect to the New Delhi; groups like LeT and JeM have planning drone attacks.

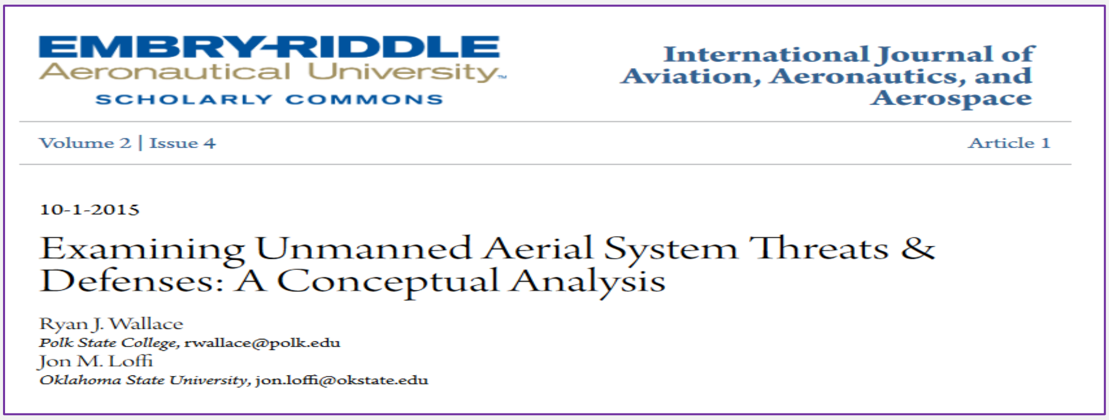
India is world's top drone importer after UK and France. Between 1985 and 2014, 22.5 percent of world's UAVs were imported by India. Within the country we have multiple manufactures marketing drones, remote controlled toys for children, cam-copters for surveillance and private clubs indulging in drone flying adventure. Monitoring drones in a populous country like ours is a herculean task. A terrorist organization could use drones with IR cameras by night and deliver chemical or radioactive payloads. Small drones are much more difficult to detect as they need little space to take off. All this requires tracking the manufactured equipment, its sale and distribution, intercepting and bringing down a terror drone including the method of bringing it down without activating its lethal payload. The government needs to seriously look into these issues aside from evolving comprehensive regulations for use of drones. The urgency is much more with more and more terrorism gravitating towards the Sub Continent. The NYPD is developing technologies to counter weaponized drones in concert with the US Military, bomb squad, emergency services and aviation units. Unfortunately, unlike the US and China, the military in India has not been integrated even in development of cyber warfare capability.

Concurrent to developing counter drone technologies, we should also build adequate responses for CBRN terrorism, which is a reality and has already been happening elsewhere in the world. We are not adequately prepared on both these counts.

The author is veteran Lieutenant General of the Indian Army.

Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis

Source: http://commons.erau.edu/cgi/viewcontent.cgi?article=1084&context=ijaaa



EMBRY-RIDDLE Aeronautical University SCHOLARLY COMMONS

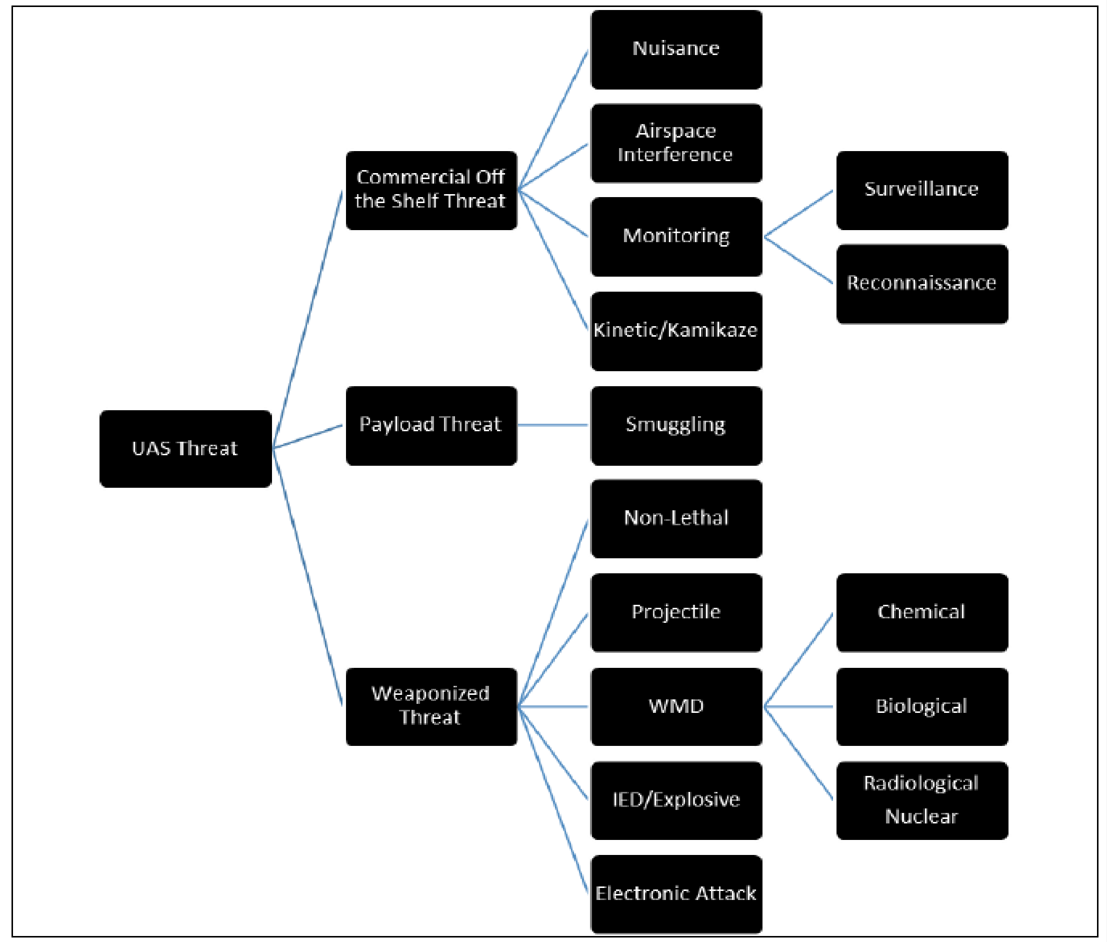
International Journal of Aviation, Aeronautics, and Aerospace

Volume 2 | Issue 4 Article 1

10-1-2015

Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis

Ryan J. Wallace
Polk State College, rwallace@polk.edu
Jon M. Loffi
Oklahoma State University, jon.loffi@okstate.edu



Concepts of Illicit UAS Use.

Merkel Buzzed by Mini-Drone at Campaign Event

Source: http://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html

Chancellor Merkel looked on with amusement on Sunday as a miniature drone approaches the stage. Defense Minister De Maizière, right, seemed less pleased.

Sept 2013 – Just when the scandal surrounding the Merkel administration's bungled purchase of a multi-million euro surveillance drone was beginning to fade, the Internet activist Pirate Party has managed to draw attention to it once again.

A Christian Democrat (CDU) campaign event taking place on Sunday in the eastern city of Dresden was interrupted when a miniature drone started circling above the audience. Chancellor Angela Merkel and Defense Minister Thomas de Maizière, who were on the stage alongside several other CDU politicians, looked on with amusement as the 40-centimeter (16-inch) aircraft came crashing down at their feet.

Soon after the event, the Pirate Party released a statement confirming it was responsible for the stunt. "The goal of the effort was to make Chancellor Merkel and Defense Minister de Maizière realize what it's like to be subjected to drone observation," said Markus Barenhoff, deputy head of the party.

The unnamed 23-year-old Pirate Party member who was operating the drone from a nearby hide-out was quickly located by the police and briefly taken into custody for disturbing the event. "The deployment of the drone served the purpose of capturing Chancellor Merkel and the other CDU politicians on camera," he said upon release.

De Maizière came under fire earlier this year amid reports that his Defense Ministry had tried to cover up a scandal over the bungled purchase of a multi-million euro surveillance drone. The aircraft proved uncertifiable for use in European air space. Among other deficiencies, the drone, known as the Euro Hawk, was found not to have a proper collision-avoidance system.

The Defense Minister is considered one of Merkel's closest allies and has been tipped as one of her possible successors.

"Though the crash landing wasn't part of the plan, we did achieve what we wanted," Pirate Party deputy head Markus Barenhoff told SPIEGEL ONLINE. "The intention was two-fold: firstly, to draw attention to the government surveillance scandal, and secondly to put de Maizière's Euro Hawk failings back on the agenda."

The party was also likely hoping that the drone might manage to help its current abysmal poll numbers take flight. Support for the pirates is hovering around 3 percent.

Whether it will be enough to win over more voters to the party remains to be seen. But it did inject a bit of lightness into an afternoon on the stump. "This kind of event is supposed to be fun, after all," concluded Stanislaw Tillich, the Christian Democrat governor of Saxony who hosted the rally.

Why Defense Minister was NOT smiling

To exemplify the potential kinetic lethality of unmanned vehicles, one can simply turn to a gruesome **2003 event in which 13-year old Tara Lipscombe was struck in the head by an out of control RC aircraft** (Allen, 2003). Flying at 50 mph, the 5-foot wide aircraft delivered a lethal blow to the young girl, who died merely three hours after the incident (Allen, 2003). While the aforementioned incidents appear unintentional, they exemplify the lethal potential of UAS systems. Should criminal or terrorist elements wish to carry out an attack, an out-of-the-box UAS platform has the potential to deliver a lethal kinetic blow to soft targets, while having the potential added benefit of appearing as accidental or negligent.

Allen, P. (2003). Teenager is killed after she is hit by model plane. Daily Mail. Retrieved from: http://www.dailymail.co.uk/news/article-177139/Teenager-killed-hit-model-plane.html

In June **2015 an 18-year old mechanical engineering student equipped his UAS with a semiautomatic pistol and successfully fired the weapon while his UAS was airborne** (Kerley, 2015). Local and federal authorities were investigating the incident to determine if any criminal statutes had been violated.

Kersey, B. (2012). New police drones could be equipped with nonlethal weapons. Slash Gear. Retrieved from: http://www.slashgear.com/new-police-drones-could-be-equipped-with-non-lethal-weapons-12217918/

Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists

Source: https://archives.fbi.gov/archives/boston/press-releases/2012/man-sentenced-in-boston-for-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-detonation-devices-to-terrorists

U.S. Attorney's Office November 01, 2012 • District of Massachusetts (617) 748-3100

Rezwan Ferdaus was sentenced today for plotting an attack on American soil and attempting to provide detonation devices to terrorists.

Ferdaus, 27, was sentenced by U.S. District Judge Richard G. Stearns to 17 years in prison, to be followed by 10 years of supervised release. On July 20, 2012, Ferdaus pleaded guilty to attempting to damage and destroy a federal building by means of an explosive and attempting to provide material support to terrorists. In the plea agreement, the parties agreed to a joint sentencing recommendation of 17 years in prison, to be followed by 10 years of supervised release. In exchange for the defendant's guilty plea, the government dismissed the remaining charges against Ferdaus after the imposition of his sentence.

At the change of plea hearing, the prosecutor detailed the evidence against the defendant, which Judge Stearns concluded was "overwhelming." Had this case gone to trial, the government would have shown through consensually recorded conversations that, beginning in 2010 and continuing until his arrest, Ferdaus planned to commit acts of violence against the United States, both here and abroad.

Beginning in January 2011, Ferdaus began designing and constructing detonation components for improvised explosive devices (IED) using mobile phones. Ferdaus supplied 12 mobile phones, which he modified to act as an electrical switch for an IED, to FBI undercover employees (UCEs), whom he believed were members of al Qaeda, with the intention that they be used to kill U.S. soldiers overseas. In June 2011, Ferdaus delivered his first mobile phone detonation device to the UCEs. At a subsequent meeting, the UCEs falsely told Ferdaus that his first phone detonation device had succeeded in killing three U.S. soldiers and injuring others in Iraq. Ferdaus responded, "That was exactly what I wanted" and that he felt "incredible....We're changing the world." He also suggested that he could make "20 to 30 [detonation components] per week" to send to his "brothers overseas."

He told the UCEs that he was "100 percent" at "peace" with the fact that his devices "are killing American soldiers" and was "so happy to hear that and so thankful." After each subsequent delivery to the UCEs, Ferdaus asked how each detonation device had worked and how many Americans had reportedly been killed. Ferdaus also made a 20-minute training video, which was recorded by the UCEs, giving instructions on how to make cell phone detonators. Ferdaus believed that the video would be used for training members of al Qaeda.

Ferdaus also planned to obtain a remote-controlled aircraft similar to a small drone aircraft, fill it with grenades, and fly the plane into the Pentagon using a built-in GPS system. Ferdaus told the UCEs that he conducted Internet research on remote-controlled aircraft and found a website that sells such airplanes, which can fly 100 mph.

According to the prosecutor, in May and June 2011, Ferdaus provided two very detailed attack plans to the UCEs. The defendant's first attack plan, among other things, contained photographs of the Pentagon and U.S. Capitol with superimposed arrows, showing where he intended to strike. The defendant stated that his plan "ought to terrorize...it ought to result in the downfall of this entire disgusting place. That is my goal."

In May 2011, Ferdaus traveled to Washington, D.C., where he conducted surveillance, and photographed the Pentagon and Capitol Building. He also identified and photographed sites at the East Potomac Park, in Washington, D.C., from which he planned to launch his airplanes filled with explosives.

In June 2011, Ferdaus informed the UCEs that he had decided to expand his attack plan to include a ground assault on the Pentagon and requested that the UCEs supply him with explosives, grenades, fully automatic weapons, and a silencer. Ferdaus then rented space at a storage facility under a false name, where he planned to store and prepare the components for his attack plan. In July 2011, Ferdaus placed an order with a Florida distributor for a remote controlled aircraft under a false identity. He told the UCEs that he wanted them to get him 24 pounds of plastic explosives to maximize the attack. He explained that 15 of the 24 pounds of explosives were for the planes—five pounds per plane. Ferdaus later increased his request to 25 pounds of explosives.

In September 2011, Ferdaus instructed the UCEs to deliver C-4 explosives, three grenades, and six fully automatic AK-47 assault rifles to him, which he later received at the storage facility he rented. Ferdaus inspected the explosives and firearms and placed some of the C-4 explosives inside the remote-controlled aircraft he had previously ordered.

Shortly after receiving the explosives and weapons in the storage facility, Ferdaus was arrested. The public was never in danger from the explosive devices, which were closely monitored by the UCEs. Ferdaus was under surveillance as his alleged plot developed and the UCEs were in frequent contact with him.

During their communications with him, the UCEs told Ferdaus more than 25 times that he did not have to go through with his plan to attack the Pentagon and Capitol, that there was no shame in backing out, and that he could turn back at any time. In response to these inquiries, Ferdaus repeatedly reaffirmed his commitment to his attack plans and his hope to cause mass destruction and psychological harm to the United States.

"As is evident from the facts of this case, Mr. Ferdaus posed a significant threat to the people of the United States," said First Assistant U.S. Attorney Jack Pirozzolo. "His actions were self-initiated, deliberate, and dangerous. He intended to unleash horrific acts of violence against the people of the United States both here and abroad. His plea and 17-year sentence should send a strong message to others that our priority is to move aggressively to investigate and prosecute anyone who intends to commit acts of terrorism whether at home or abroad."

"Mr. Ferdaus' sentence reflects that he alone conceived the plot, was responsible for his illegal acts, and acted purposefully," said Richard DesLauriers, the Special Agent in Charge of the Boston FBI. "The FBI's top priority and clarion mission is to detect, deter, and disrupt all potential terrorist threats to the United States. Our community should be proud of the efforts of the Worcester Police Department, U.S. Attorney's Office, and all members of the Boston Joint Terrorism Task Force. Working in partnership, we seek to disrupt homegrown violent extremists like Mr. Ferdaus who attempt to use violence, rather than democratic means, to achieve their political or social goals."

First Assistant U.S. Attorney Jack Pirozzolo and Richard DesLauriers, Special Agent in Charge of the FBI Boston Field Division, made the announcement today. Assistance was provided by the Worcester, Massachusetts Police Department; the Ashland, Massachusetts Police Department; and the Bureau of Alcohol, Tobacco, Firearms, and Explosives. The case is being prosecuted by Assistant U.S. Attorney B. Stephanie Siegmann of the U.S. Attorney's Office's Anti-Terrorism and National Security Unit.

FBI: Man plotted to fly drone-like toy planes with bombs into school

Source: http://www.cbsnews.com/news/fbi-man-in-connecticut-plotted-to-fly-drone-like-toy-planes-with-bombs-into-school/

Apr 08, 2014 – A Moroccan national was detained without bail in Connecticut after FBI agents discovered his plot to fly bombs on drone-like devices made out of radio-controlled airplanes into a school and a federal building, according to federal authorities.

The FBI arrested 27-year-old El Mehdi Semlali Fahti on Monday on immigration-related charges, and he may later face terrorism charges in a federal grand jury investigation, federal prosecutors said. Fahti's arrest was first reported by the Connecticut Post.

Authorities didn't disclose the exact locations of the alleged targets, only that Fahti purportedly planned to fly the bombs into an out-of-state school and a federal building in Connecticut, the Post reported.

The FBI said Fahti was secretly recorded by an undercover agent saying he studied the bomb attack operation for months. Authorities say they found wires and tools in his Bridgeport apartment but didn't say if any explosives were found.

Fahti told the undercover agent that he could obtain items needed for the bomb plot in Southern California near the Mexico border and that funding would come from secret accounts filled with laundered money and drug-dealing profits, the FBI said.

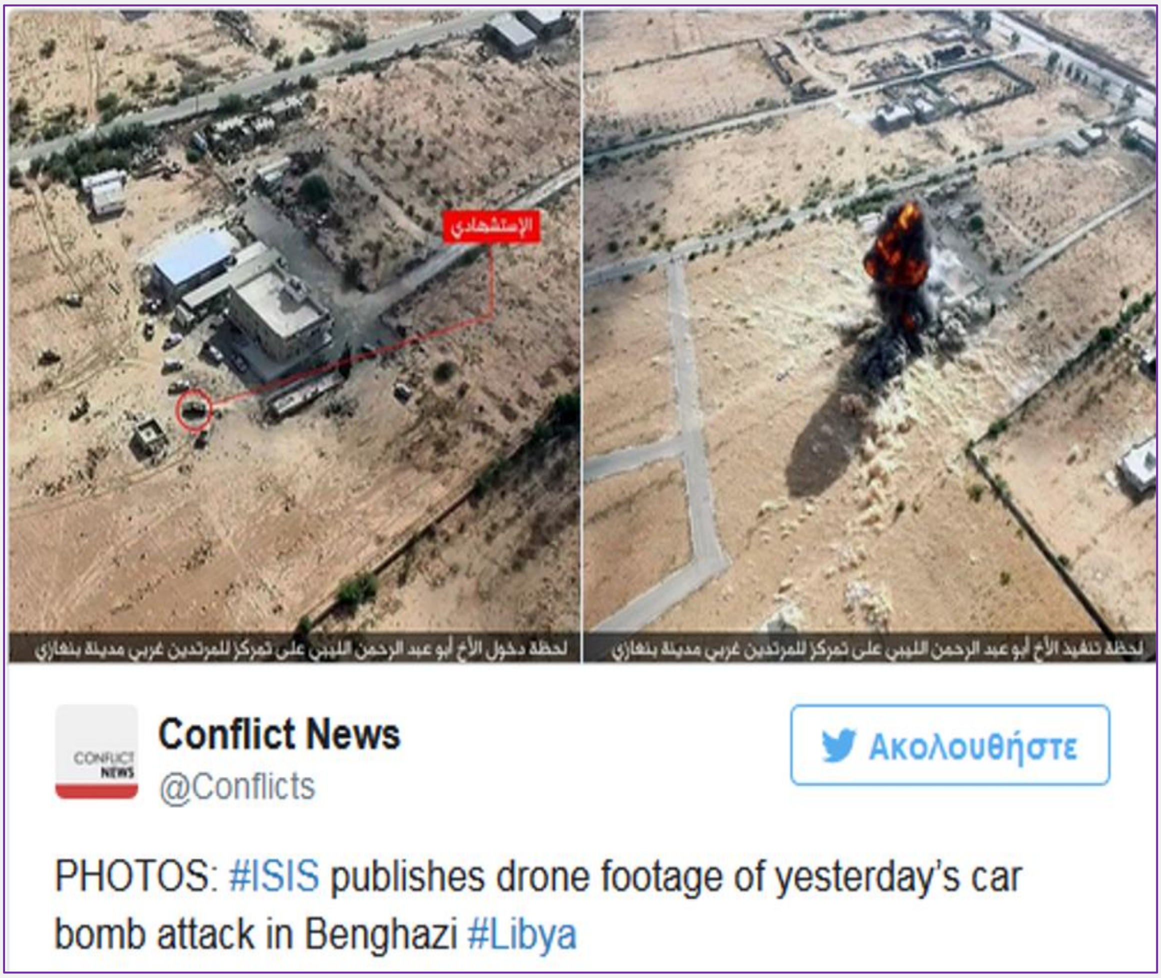
Fahti appeared Monday in federal court in Bridgeport, where Magistrate Judge William Garfinkel granted prosecutors' request to detain Fahti without bail.

His federal public defender, Paul Thomas, declined to comment Tuesday in an email to The Associated Press.

Authorities charged Fahti with immigration-related crimes including making a false statement, falsely swearing under oath and falsifying declarations to a federal immigration judge. Officials said Fahti stayed in the U.S. for seven years after his student visa expired after flunking out of Virginia International University.

Fahti was facing deportation to Morocco and made the false statements while seeking political asylum in the U.S., authorities said.

IS drone in Libya (July 30, 2016)


الإستشهادي
لحظة دخول الأخ أبو عبد الرحمن الليبي على تمركز للمرتدين غربي مدينة بنغازي
لحظة تنفيذ الأخ أبو عبد الرحمن الليبي على تمركز للمرتدين غربي مدينة بنغازي
CONFLICT NEWS
Ακολουθήστε

Conflict News
@Conflicts

PHOTOS: #ISIS publishes drone footage of yesterday's car bomb attack in Benghazi #Libya

Top 10 Best Most Expensive Drones on Amazon – 2016

Source: http://www.top10drone.com/top-10-most-expensive-drones/

Looking for the best most expensive drones with accessories on Amazon? Drones are a great way to capture majestic landscapes, sporting events or anything else you want to capture from high up in the air. The drone market is saturated with low end drones that can be used for fun. Most even allow you to capture video and images, but the camera quality is not always the greatest. If you want to splash out and treat yourself to the best drones available on the market today – then look no further. We've rounded up the best expensive drones on Amazon in 2016.

Available at amazon

10) Autel Robotics XSTAR-PREM-WH X-Star Premium Drone

What we like most: HD 720p live streaming

Key Features:

- 4K (Ultra HD) video camera (4K30, 2.7K60, 1080p120, 720p240) with 12-MP still images, conveniently integrated into a quick-release 3-axis gimbal stabilizer
- HD Live View (720p streaming up to 1.2 miles away) and autonomous flight modes including follow, orbit, and waypoints via the free Starlink app for iOS or Android (mobile device sold separately)
- Dual GPS/GLONASS outdoor navigation, SecureFly magnetic interference protection, and the Starpoint Positioning System for precise flying where GPS signals are unavailable
- Intuitive remote controller with LCD display for flight information and one-touch action buttons for starting the motors, takeoff, hover, going home and landing
- Included accessories: Premium hard case, 64-GB MicroSD card that can record over 2 hours of 4K video, intelligent battery for up to 25 minutes of flying time per charge, a 1-hour fast charger, spare propellers and small parts

Price: $899.00

9) Thunder Tiger Robotix Ghost Drone

What we like most: The lightweight 12" APC Propellers

Key Features:

- Max Payload: 0.81kg; Max Take-off Weight: 2.25kg; Max Flight Time: 25minutes
- Enlarged frame plates provides abundant space for electronic system sand easier to install various auxiliary equipment required for aerial photography.
- Intelligent power system provides battery capacity check and anti-spark design.
- Matte black finish body shell with sleek scheme.
- Retractable landing skid provides better view of camera lens.

Price: $981.06

8) Yuneec Q500 4K Typhoon Drone

What we like most: Comes with a ground station

Key Features:

- Designed for Aerial Photo and Video; Capture Up to 4K / 1080p120 Video
- Take Up to 16 MP Still Photos; 3-Axis Gimbal Stabilizes Camera
- ST10+ Ground Station / Transmitter; 5.5" Touchscreen to View/Operate Camera
- OSD Overlay of Flight Telemetry Data; No-Fly Database
- Battery Lasts up to 25 Minutes

Price: $1,099.99

7) DJI Phantom 2 Vision+ V3.0 Drone

What we like most: The 1080p camera still captures better footage than the new models of drones

Key Features: Live streaming HD video

- 32GB Extended Video BUNDLE comes with additional 32GB MicroSD Card for 8x the standard recording length together with USB Card Reader for easy video transfer and viewing. Super smooth video thanks to the 3-axis gimbal
- More flight power and security from the high-efficiency self-tightening propellers, redesigned for V2.0
- Crystal clear stills and live streaming video from the redesigned HD video camera with built-in FPV link
- Advanced GPS-based navigation and programmable features you can set up via the built-in USB port
- Extra-long flight times of up to 25 minutes from the intelligent 5,200-mAh battery

List Price: $1,499.99

6) Walkera TALI H500 RTF5 Hexacopter/Hexrotor Drone

What we like most: The 3 axis YAW stabilized GoPro compattible gimbal
Key Features:

- iLook 1080p / 12MP Action Camera + G3-D 3-Axis Gimbal (Compatible with iLOOK & GoPro Models)
- 12-Channel Transmitter DEVO F12E FPV Transmitter/Receiver with 5" FPV Screen
- Flight Time of Up to 25 Minutes
- Up to 3,280' Line-of-Sight Radio Range
- Groundstation for use with smartphones & tablets

List Price: $1,699.99 ■ Price: $1,836.21

5) 3D Robotics Solo Drone

What we like most: The expansion bay which can be used for various mods / add-ons in the future such a parachute
Key Features:

- Capture Aerial Photos/Video with a GoPro; Linear Tracking with Cablecam Mode
- Follow Me: Tracks Your Mobile Device; HDMI Output on Transmitter
- Android and iOS Mobile Apps; Video Game-Style Controls
- Return Home and "Safety Net" Modes; One-Button Flying / "Pause" Button
- Operate GoPro Through App; Works with Optional Solo Gimbal

Price: N/A

4) Walkera QR X800 Drone

What we like most: Retractable Landing Gear
Key Features:

- FCS800 Multi Axis Control Platform
- Core-Integrated Circuit System
- Carbon Fiber Structure Design
- Retractable Landing Skids
- High Performance Brushless Motors

List Price: $2,999.99

3) Phantom 3 Professional Carbon Fiber Drone

What we like most: Can be controlled from up to 2km away
Key Features:

- 4k UHD video recording with fully stabilized 3-axis gimbal; Vision Positioning system allows stable flight indoors
- Lightbridge digital streaming allows live viewing of 720p video (full resolution video is simultaneously recorded on the internal microSD card)
- Included flight battery and rechargeable remote controller means this system is ready to fly out of the box
- DJI Pilot app for iOS and Android allows live viewing and complete camera control (phone/tablet sold separately; see DJI's website for compatible models)

Price: $1,545.00

2) DJI Matrice 100 Drone

What we like most: Four directional-antennas & shock absorbing landing gear
Key Features:

- DJI Matrice 100
- Extra Charger + Extra DJI Self-Tightening Propeller Set + 2 64GB Micro SD Memory Cards + High Speed Memory Card Reader
- 2 Apple iPad Mini 2 with WiFi 32GB Silver
- Extra Remote Controller
- Microfiber Cleaning Cloth Manufacturer Included Accessories: 3 DJI Self-Tightening Propeller Sets + Battery + Remote Controller + Charger

Price: N/A

1)DJI Inspire 1 Pro Carbon Fiber Zenmuse X5 Drone

What we like most: 4K video with a Sony EMOR 1/2.3-inch sensor

Key Features:

- Bundle Includes: Custom Painted Carbon Fiber Inspire 1 PRO Zenmuse X5 4K Camera Quad + 1 Tb47 Battery and 1 Tb48 Battery in Carbon Fiber Design + Hard Case + All Included Accessories + Free Drones Etc. Lanyard!
- Ready-to-fly aerial system
- Live, wireless HD video transmission via DJI Lightbridge
- Dedicated remote with flight and camera controls
- Powerful app to adjust camera settings, edit videos, and more

Price: N/A

17 Cheap Drones for Beginners (Under $150)

By Alan Perlman on July 3, 2016
Source: http://uavcoach.com/cheap-drones-for-beginners/

Note: This list is updated for summer 2016. Fly safely and responsibly, folks. Never flown before? Check our flying guide here!

Today, I'm going to walk you through 17 inexpensive drones for beginner pilots.

At UAV Coach, we always suggest starting off with a less expensive system. This is so you can hone your skills before moving on to the bigger guns (like the DJI Phantom 4) or the like the Yuneec Typhoon H).

These models don't have all the bells and whistles of high-end drones for sale, but you'll be surprised at how advanced their features can get.

Drone technology has come a long way, which means we've been able to pack more capabilities into smaller, less expensive packages.

These are some of the most affordable UAVs on the market today, and they're great for anyone looking to get into the hobby.

Don't want to scroll down and read all the specs and just want to see the full list? Here they are:

- UDI U818A
- MJX X400W FPV (enter code JKJZSO3O for $20 off)
- X4 H107C
- Parrot Rolling Spider
- Syma X5C
- Blade Nano
- USA TOYZ F180+
- JJRC H8C
- Syma X5C
- NightHawk DM007
- Eachine X6 hexacopter
- Hubsan H111
- Yi Zhan X4
- Hubsan X4
- DBPOWER UDI U845 (enter code VDQKAIAB for $25 off)
- FQ777-124 Pocket Drone
- Cheerson CX-10 Mini

▶ **Full specifications are available at source's URL.**

Hezbollah Drone Is a Warning to the U.S.

Source: http://www.thedailybeast.com/articles/2016/08/17/hezbollah-drone-is-a-warning-to-the-u-s.html

Aug 17 – The cheap commercial drone the militant group deployed to bomb Syrian rebels in Aleppo could soon be seen above battlefields all over the world—and it's way ahead of U.S. defenses.

As if Syrian regime forces, Russian airstrikes, and internal squabbling weren't enough to worry about, Syrian rebels have apparently now come under attack from Hezbollah drones dropping bombs.

On Aug. 9, the Iran-backed Lebanese militant group posted a video online purportedly depicting a commercial, quad copter-style drone dropping small explosive devices at alleged rebel positions in Aleppo, a major opposition-held city in northern Syria.

The 42-second video, apparently a compilation of footage shot by the attacking drones themselves, seems to show the robots hovering a few hundred feet over vehicles and structures as small blasts scatter fragments and send smoke and dust billowing into the sky.

In the third and final attack, the grenade-size munitions themselves—possibly Chinese-made MZD-2 artillery submunitions—are visible falling away from the drone. A person on the ground spots the bombs falling toward them and flees the targeted structure moments before the explosives detonate.

Hezbollah has deployed thousands of fighters to Syria to help bolster troops loyal to Syrian president Bashar al-Assad. Hezbollah fighters lack heavy vehicles and weaponry but have moved quickly to adopt small, inexpensive drones for surveillance and attack missions.

As early as November 2004, Hezbollah sent Iranian-supplied Mirsad drones into Israeli airspace on spy missions, catching Israeli air defenses off guard. Shortly thereafter, Hezbollah leader Hassan Nasrallah proclaimed that the Mirsad could penetrate "anywhere, deep, deep" into Israel while carrying more than 200 pounds of explosives.

It was a bold claim for the time. The United States was the first country to deploy a modern, armed drone—the Predator—in 2001. For several years, America possessed a virtual monopoly on weaponized flying robots.

Nasrallah was perhaps exaggerating, but he wasn't bluffing. In August 2006 during Israel's brief, bloody war with Hezbollah in Lebanon, the militant group launched three explosives-laden Ababil drones toward Israeli territory. Israeli jet fighters shot down all three robots.

Hezbollah's current armed drones represent a departure from the group's previous concept for drone operations. The Mirsads and Ababils were, in a sense, strategic terror weapons, meant to cross borders and strike fear in enemy populations.

The submunition-armed drones that Hezbollah has deployed over Aleppo are, by contrast, strictly tactical. Hovering, commercial-style drones can fly only a short distance away from their operators and, under the best of circumstances, can haul only a few pounds of payload. But what the drone-copters lack in sheer power, they make up for in stability—hence their ability to accurately drop an unguided submunition.

They're also cheap, easy to procure, and simple to operate. For all but the most impoverished military force, a $200 quadcopter is disposable. And that means the type could crop up again not only in Syria, but also on battlefields all over the world—as a bomber... or as a bomb itself, rigged to explode on command.

The Pentagon, for one, is assuming that small, cheap, weaponized drones will soon pose a significant danger to American troops. "I personally believe that the unmanned platform is going to be one of the most important weapons of our age," U.S. Navy Capt. Vincent Martinez, who oversees technology development for the fleet's bomb squads, told *Defense News* last year.

Martinez said he was doubly worried about drones crashing or landing while hauling improvised explosive devices or other munitions that the robot or its operator might trigger as bomb-disposal troops approach. "I'm going to have to start thinking not only about how I defuse the payload but how I defuse the platform," Martinez said. "When I walk up on that platform, is it watching me, is it sensing me, is it waiting for me?"

The U.S. military is preparing its drone defenses. On Aug. 11, the fringe-science Defense Advanced Research Projects Agency asked for researchers and companies to propose technologies that might "detect, identify, track and neutralize these [drone] systems on the move, on a compressed timeline and while mitigating collateral damage."

One private firm has already begun marketing one such tech. In March, OpenWorks Engineering began offering its SkyWall 100—in essence, a bazooka that fires a drone-entangling net—as a non-destructive robot-countermeasure.

The U.S. Marine Corps, for one, is signaling that it won't hesitate to simply blow up drones in midair. Skipping ahead of DARPA's own solicitation, the Marines recently announced plans to fit a drone-blasting laser cannon to its new armored vehicle starting in 2022.

But with Hezbollah already lobbing grenades from quadcopters in Syria, the non-state perpetrators of small-scale drone warfare have the jump on the world's established armies and their lumbering bureaucracies.

At present, weaponized drones are way ahead of defenses against weaponized drones. If you shoot one down, another might quickly take its place. And once it drops its bomb, you can only do what that unfortunate figure can be seen doing at the end of Hezbollah's new video—run.

IN CONCLUSION

The articles presented herein support the opinion that the CBRNE-UAV threat is real! Terrorist threatening our societies have already put their hands on chemical warfare agents and radiological materials and now are beginning to use unmanned air vehicles during their operations in the countries they are activated. It seems that there is a matter of time to combine CR agents with UAVs for their next terrorist attack. Since there is a competition between Islamic State and al Qaeda on who is the bloodiest terrorist organization, they might attempt to set the pole even higher than 9/11 tragedy and bloodshed. And the only way to do that is to use either chemicals or dirty bombs. New aerial technologies are cheap and affordable worldwide and since money is no object (especially for Islamic State) it is quite possible to attempt at least a CR-UAV attack against urban targets causing enormous disruption while injecting more fear and panic to our societies. The main conclusion is that although this is not as easy as it looks, it can be done. The biggest issue here is what we are going to do about it NOW!