LLNL-TR-740336

Lawrence Livermore National Laboratory

The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications

17 October 2017

BALL, RYAN JOKL

Disclaimer

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

Contents

Figures

Tables

Executive Summary

"Those worried about drone proliferation must face facts. We are no longer in a world where only the United States has the technology, and we are not moving toward a future in which the technology is used only in the same way we use it now."

—Peter Singer, 2013[1]

There has been unparalleled proliferation and technological advancement of consumer unmanned aerial vehicles (UAVs) across the globe in the past several years. As witnessed over the course of insurgency tactics, it is difficult to restrict terrorists from using widely available technology they perceive as advantageous to their overall strategy. Through a review of the characteristics, consumer market landscape, tactics, and countertactics, as well as operational use of consumer-grade UAVs, this open-source report seeks to provide an introductory understanding of the terrorist-UAV landscape, as well as insights into present and future capabilities. The caveat is evaluating a developing technology haphazardly used by terrorists in asymmetric conflicts.

Key Findings

- There is a substantial increase in sophistication and availability of UAV technologies in the private sector at a relatively decreasing cost.
- UAVs provide terrorists with novel aerial capabilities without requiring large-scale infrastructure, proving to be suitable for asymmetrical warfare.
- This advantageous technology will increasingly be acquired and integrated into their combat operations for a wide range of nonlethal and lethal applications—yet currently remains a "niche" threat due to lack of sophistication.
- Future technology developments will significantly enhance terrorist aerial capabilities with the potential for overmatch in certain operational facets.

Introduction

There has been unparalleled proliferation and technological advancement of consumer UAVs across the globe in the past several years; over two million units were sold globally in 2016 alone, with over three million units projected for 2017, according to an online news source.[2] Technology once considered proprietary to more advanced militaries such as the United States and Israel is now increasingly available and used by nonstate actors to serve their interests across a broad set of applications—from industry to entertainment. This multibillion-dollar market for remotely piloted vehicles has enabled nonstate actors, including terrorists, an increasing degree of accessibility and tactical flexibility for a range of previously unobtainable combat capabilities at a relatively low cost.

The rapid proliferation, popularity, and decreasing cost of this sophisticated yet easily used technology has not gone unnoticed by terrorists. These small, portable aircrafts have been acquired and modified by some terrorist organizations to conduct intelligence, surveillance, target acquisition, and reconnaissance (ISTAR), as well as to create propaganda tools. Terrorist tactics have included weaponization of cheap UAVs to deploy grenades and mortar rounds.

The public discourse on UAVs has largely revolved around the use of this technology by states and has included topics such as tactical advantages gained by using this technology and ethical concerns of civilian casualties. Only recently has media attention focused on terrorist use and potential use of these

UAVs. This delayed attention comes despite terrorist group using this type of technology as far back as 1994, when the Japanese doomsday organization Aum Shinkrikyo failed to disperse sarin gas in Tokyo from a remotely controlled helicopter due to technical difficulty.[3]

Understanding and evaluating how the continued global distribution of UAVs pose threats to national security and how they can potentially alter the landscape of asymmetric conflicts is important. UAVs have the potential to significantly augment nonstate actors' capabilities by requiring minimal technical expertise and infrastructure. Such technology's affordability, ease of purchase, and portability may also lead to a high degree of difficulty in predicting and detecting use by terrorists.

Terminology and Taxonomy

Organizations and institutions from the media to the military use varying terminology when referring to UAVs—unmanned aerial system (UAS), remotely piloted vehicle (RPV), and most commonly, drone. These terms have negligible difference in meaning, some offering more formality preferred by groups such as the military. The Federal Aviation Administration (FAA) defines a UAV by law as "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[4] UAVs are part of unmanned aerial systems, which encompass the "components that control the unmanned aircraft," such as communication stations and controllers. In this report, we use the term *UAV* as it is formally defied by the FAA, noting that UAS and RPV are often used interchangeably with UAV.

UAVs vary extensively in size, weight, range, payload capacity, accessibility, and affordability. For a clear and effective examination of insurgent UAV usage, we assign formalized categories of UAVs to focus on those that are the most relevant for terrorist use. We use a slightly modified version of the taxonomy of UAVs established by the Center for New American Security's Kelley Sayler: hobbyist, midsize military and commercial, large military-specific, and stealth combat.[5] **Figure 1** shows this taxonomy.

- **Hobbyist and commercial UAVs (consumer UAVs)**. This category includes products that are accessible to the public domain and can be purchased from nongovernment entities for any purpose: personal or industrial. Units cost between several hundred dollars to several thousand dollars, and operational use requires negligible technical skills and infrastructure, typically referred to as do-it-yourself (DIY) UAVs that are preassembled (or close to it). This technology provides operators with the ability to survey the ground or deploy payloads, such as improvised explosive devices (IEDs) and chemical weapons, from several miles away. These UAVs are classified as those available in the consumer retail marketplace, so we group them under the umbrella term *consumer UAVs*.
- **Midsize military and commercial UAVs**. This category comprises systems that are developed by nation states (e.g., Iran, Saudi Arabia) for military applications. These units are not generally accessible to nonactors due to the technical expertise and infrastructure required to build these systems, as well as numerous export controls on their purchase. However, there is some indication that these types of systems may have been distributed by states to nonstate actors, such as Hamas and Hezbollah.[6] Overall, this category of systems is designed for more advanced operations than hobbyist and commercial UAVs, such as deploying missiles.
- **Large military-specific UAVs**. These systems are designed, manufactured, and exclusively accessible to the most advanced militaries. They require a sophisticated operational and engineering infrastructure. This category of the technology enables these large military-specific UAVs to fly for dozens of hours, delivering payloads of up to several thousand pounds, including weapons such as precision-guided missiles.

- **Stealth combat UAVs**. This category is the apex of UAV technology, incorporating stealth tactics with highly advanced capabilities. The United States and China are the only verified users of such aerial systems, which cost upwards of tens of millions of dollars.

This report will focus on the first category—consumer UAVs—as this UAV category is the most widely available and most frequently used by terrorist groups. More sophisticated systems provided to terrorist by a nation state is outside the scope of this report.

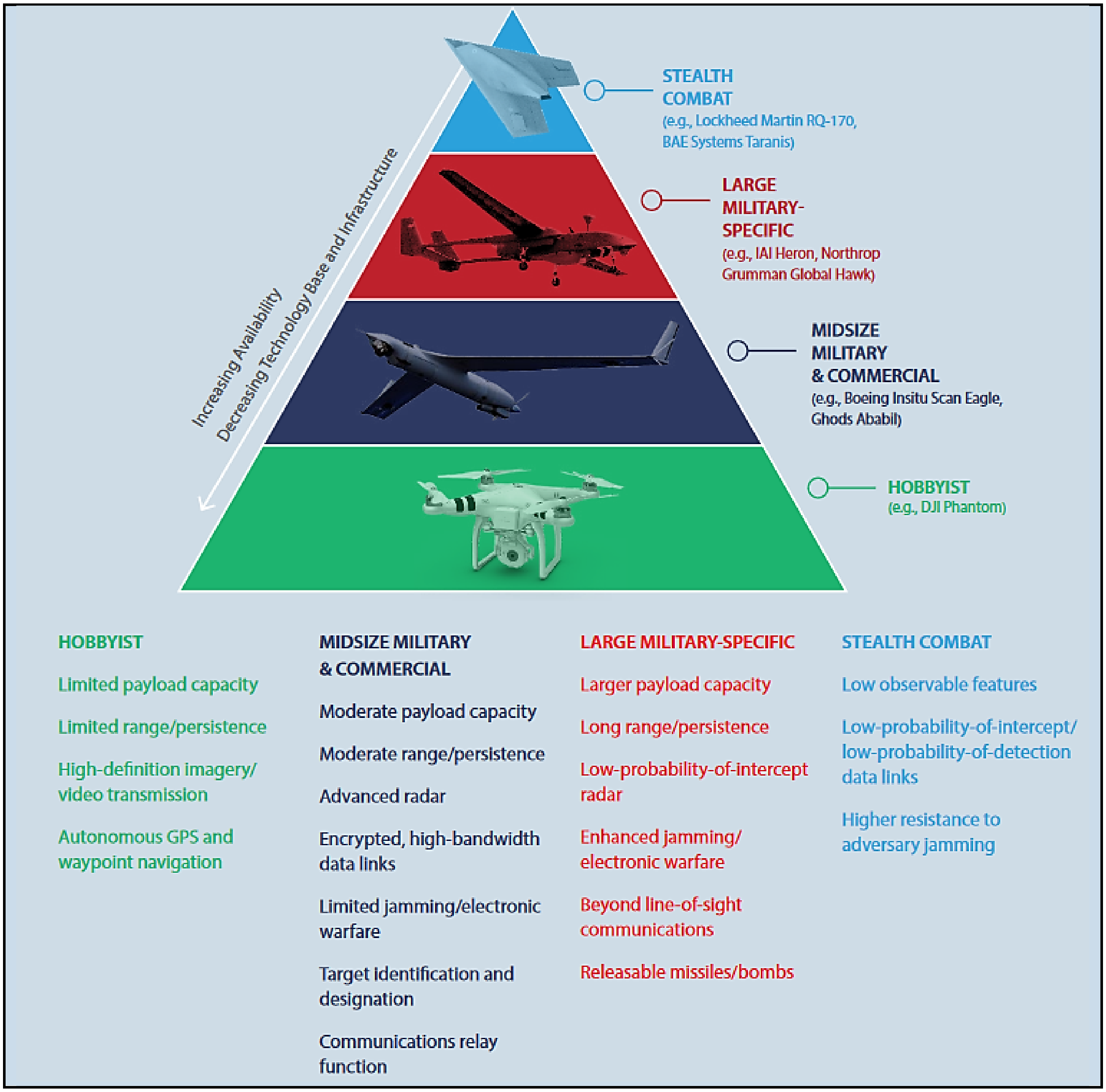


Figure 1. Taxonomy of UAVs.[7]

Technical Characteristics

UAVs are defined by several technical characteristics: aerial structure, range, flight time, speed, and payload capacity.

Aerial structure. Although most UAVs are fixed-wing or rotary-wing/multirotor, some UAVs fall outside of these categories, in most cases (although not limited to) UAVs assembled from different model components. We focus on the two most common types.

- *Fixed-wing*. An airplane that uses forward airspeed to produce lift (typically comprising a tail, a singular wing, and at least one propeller located in the front or back) is considered a fixed-wing UAV. Most UAVs at the consumer level use lithium-polymer (LiPo) batteries to power the aircraft. In some cases, the weight of a fixed-wing UAV may render it necessary to use a catapult takeoff system that employs a bungee cord or similar tension-line variation. Landing options typically involve a skid landing due to lack of landing gear.
- *Rotary-wing, multirotor*. This type of UAV achieves airlift via rapid rotation of the rotor, typically using brushless motors. Two significant advantages of this UAV type are its ability to take off and land vertically and its hovering capabilities, demonstrating significantly more tactical flexibility than fixed-wing UAVs. Most consumer versions are multirotor UAVs, consisting of a symmetrical number of rotors to maximize aerodynamics (e.g., quadcopters, octocopters). Additional motors enhance capabilities to the extent of greater range, speed, and gross takeoff weight (GTOW). Due to the superior flexibility and capability offered by multirotor UAVs, this aerial structure is most commonly purchased by consumers (the DJI Phantom shown in **Figure 2**, a quadcopter, is the highest-grossing-revenue UAV in the world).

Figure 2. DJI Phantom 3.[8]

Flight time. Flight time is the total sustained flight time of an aircraft. This is considered the primary performance benchmark for UAVs as it often determines the scope of applications possible. This varies significantly depending on the aircraft model and chosen flight conditions regarding speed, range, payload capacity, altitude, and battery capacity—the most significant factor. Compared to fixed-wing types that demonstrate 45–60 minutes of flight time, multirotor consumer UAVs have substantially less flight time—approximately 20–30 minutes—due to their powered lift designs. Flight time can be adjusted through basic modifications, such as decreasing the payload weight.

Speed. The selected speed for a UAV flight varies depending on the objectives. For instance, an optimal speed for maximizing range and flight time is not necessarily suitable for a flight with significant payload weight. Rotary-wing UAVs, comprising a majority of the consumer marketplace aircrafts, can fly between 10 and 30 miles per hour (mph) as they lack the speed capabilities of the more aerodynamic fixed-wing aircrafts, which can reach speeds up to 45 mph.

Payload capacity. UAV payloads can be located either in the front, back, or (most commonly) at the center bottom of the UAV. The central payload positioning allows for a camera to be carried for an expansive surveillance view or as an optimal position for weapon deployment. The capacity significantly varies depending on the design of the UAV. Hobbyist UAVs' payload capacity are between 0.5 to 1 kilogram (kg); commercial UAVs can carry between 6 and 10 kg. Ultimately, the user faces tradeoffs between weight capacity and performance—payload weight is inversely related, albeit not linearly, to flight time. An increase in payload weight, given that it does not exceed takeoff capacity, decreases a UAV's flight time. For example, the DJI Phantom 3 carrying 0 kg payload weight measured a flight time of 24.4 minutes, compared to only 14.4 minutes flight time when carrying 1 kg payload weight.[9] **Figure 3** shows two examples.

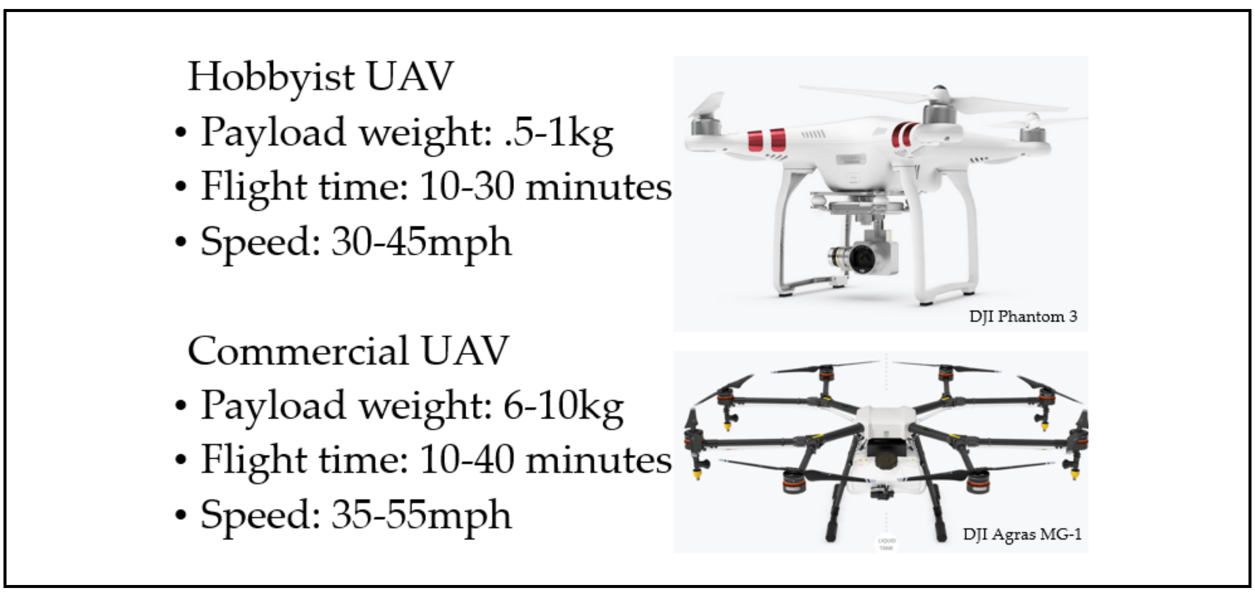


Figure 3. Consumer UAV characteristic metrics.*

* This figure was compiled based on information from DJI and other UAV manufacturing websites, so there is some subjectivity. The author considers the listed flight parameters as most consequential in the context of evaluating terrorist use of this technology.

Communication and Ground Control Systems

A datalink serves as the communication and control channel between the ground and the UAV. The type of datalink (described in **Table 1**) varies depending on the UAV's application and capabilities and generally falls into three categories—command, telemetry, and video—that use transmitter and receivers.[10] These UAVs have a datalink range typically between 1 and 4 kilometers (km). The ground control station uses radiofrequencies to establish this communication network, typically at 2.4 gigahertz (GHz). Numerous UAVs integrate all three datalinks, which allows for increased flexibility of operation, such as navigating the aircraft via GPS and accessing real-time video feed simultaneously. Increasingly, consumer UAVs offer wireless (wi-fi) and Bluetooth built-in to the firmware, providing a new method for communication and control.

Table 1. UAV datalinks.[11]

Type	Purpose	Ground Equipment	Aircraft Equipment	Example
Command Uplink	Control the aircraft and payload	Transmitter	Receiver	72 MHz Remote Control
Telemetry Downlink	Send instrumentation data to the ground	Receiver	Transmitter	900 MHz Digital Radio
Video Datalink	Send video to the ground	Receiver	Transmitter	5800 MHz Analog Video
Bi-directional Datalink	Moves command and telemetry data and may also send digital video	Transceiver	Transceiver	2400 or 5800 MHz WiFi

The ground control station (GCS) consists of the software and hardware that enables the operator to operate the UAV via a command uplink. Rudimentary versions take the form of a remote-controlled joystick, and more advanced operations comprise a computer with customized global positioning system (GPS) software. Increasingly adopted and offered by consumer UAV companies are smartphone and tablet applications—such as on an iPad—that serve as the GCS. This has become a popular choice due to the familiarity of this technology, as opposed to the user learning an entirely new operating system. This highlights the behavioral tendency of users to modify the aircraft system to optimally serve their interests—such as using an iPad instead of the given controller or replacing the propellers with a more efficient type.

When purchasing a UAV in most cases, no additional equipment or infrastructure is required. The manufacturer provides the technology, such as controllers and GPS integrated into the UAV, that will enable the operator to fly the aircraft in its maximum capacity. However, some fixed-wing aircraft packages do not include launching gear—for example, a basic catapult system—that is necessary for heavier UAVs.

Autonomous Capabilities

The level of autonomy by a UAV—the ability to complete a certain phase of flight without human interaction—is often misunderstood and misrepresented in the consumer marketplace, with more companies increasingly advertising their UAVs as autonomous. Through a modified autonomous construction typology (shown in **Table 2**), we group autonomous UAV capabilities into four categories: human operated, function-specific automation, semi-autonomous, and autonomous.[12]

Table 2. UAV Autonomous Typology.[13]

***Human Operated*:**	The operator exerts total control throughout the duration of flight.
***Function-Specific Autonomous*:**	Operator is responsible for a majority of the flight parameters with the ability to give the UAV specific tasks.
Semi-Autonomous:	UAV completes a subset of required tasks without human intervention.
***Autonomous*:**	UAV executes each task without human intervention.

The capabilities currently demonstrated by UAVs in the marketplace can be categorized as semi-autonomous, transcending the early stages of this technology in which such aircrafts were entirely human operated. Semi-autonomous aircrafts incorporate a certain degree of autopilot technology—such as self-stabilizing altitude, hovering, takeoff, and landing—while the operator controls other phases of the flight. Increasingly, consumer UAVs assume autonomous navigation responsibilities for most of the flight. For example, the DJI Phantom can employ GPS waypoints selected by the user to create a programmed route.[14] Before takeoff, the operator provides the necessary flight parameters (altitude, speed, landing destination, etc.), and the UAV follows the selected route, giving real-time data and video feedback. This enables these aerial vehicles to autonomously launch and fly a predetermined path, even hovering at one location for a prolonged period. If battery power drops below a level of sufficient functionality to complete the trip, the software notifies the user, at which point the UAV can land at a new destination or return to the point of launch.[15]

This autonomous technology provides the user—specifically a terrorist—with two advantages not possible at the human-operated level. First, GPS waypoint navigation dissolves the necessity for line-of-sight communication with the UAV, allowing the UAV to be operated from several miles away. Second, it substantially increases the degree of anonymity by enabling the attack to be orchestrated from a remote location. Subsequently, the UAV can launch and land at different locations.

Truly autonomous UAVs entail no human responsibility. Under this definition, no available consumer UAV is autonomous as currently an operator is required to assume at least some degree of control, such as preprogramming the flight path. With constant improvements of UAV technology leading to a decreasing need for human intervention, it is inevitable that UAVs will eventually become fully autonomous. We discuss this in further detail in the Future Trends and Development section below.

The Consumer Market Landscape: Economics, Accessibility, the Dual-Use Dilemma

Following a similar path as the Internet and GPS, UAV technology has made the leap from strictly military application into the consumer marketplace. Decreases in production costs and increases in sophistication have advanced these products' abilities far beyond the rudimentary capabilities of earlier models. Consumer UAV kits equip nonstate actors with more advanced capabilities that were once proprietary to highly developed militaries at a low startup cost; prices range from several hundred to several thousand dollars.

Economics

This sophisticated technology is easily accessible and purchased, demonstrating a low barrier to entry; global sales of hobbyist and commercial UAVs increased 60 percent year-to-date, with over 3 million sold in 2016, bringing global revenue to over $4 billion.[16] Looking at major players in the market, the Chinese corporation DJI is the most valuable UAV company, grossing over $1.5 billion revenue in 2016 with an estimated 45 percent market share.[17] DJI's UAV model, the Phantom, sells for approximately $500. This company is widely recognized as the industry standard for consumer-grade UAVs.

The cost has substantially decreased as these manufacturing companies benefit from economies of scale, other production-line efficiencies, and vertical and horizontal integration. Consumer demand for this technology has increased as the multitude of cost-saving commercial applications (e.g., using UAVs for crop dispersal as a cost-alternative to an airplane) becomes clear. This synergy between the consumer and the UAV companies will continue to grow and thus lead to a further increase in the capabilities of these consumer-grade aircrafts—at a cheaper price point. Advancements in technology sophistication will also continue and speed up due to the ability and propensity for companies to invest significant capital in technology beneficial to their operations. **Figure 4** shows the projected economic impact of the commercial drone sector.

Accessibility

DJI and other UAV companies appear to comply with export and import laws—Iraq and Syria are not shipping options on their website.[18] However, as with other technologies, terrorists have found ways to circumvent barriers and acquire UAVs. First, they benefit from the DIY nature of UAV users. Hobbyist consumers have demonstrated a passion for this technology, so there are dozens of third-party retail sites and blogs in which such hobbyists discuss different ways to use this technology and sell UAV components to optimize flight parameters. A multitude of blogs and forums indicate a large community of consumers that collaborate on ways to enhance UAV capabilities, which is valuable information terrorists can use to their advantage. This enables terrorists to purchase UAVs from third-, fourth-, and fifth-party retailers, either in whole or as different parts that can easily be assembled, and it is likely that such products are sold through gray markets.[19] With millions sold each year in the U.S. alone and a substantial increase in supply year-to-year (as shown in **Figure 5**), it will continue to be difficult to prevent terrorists from acquiring this technology.

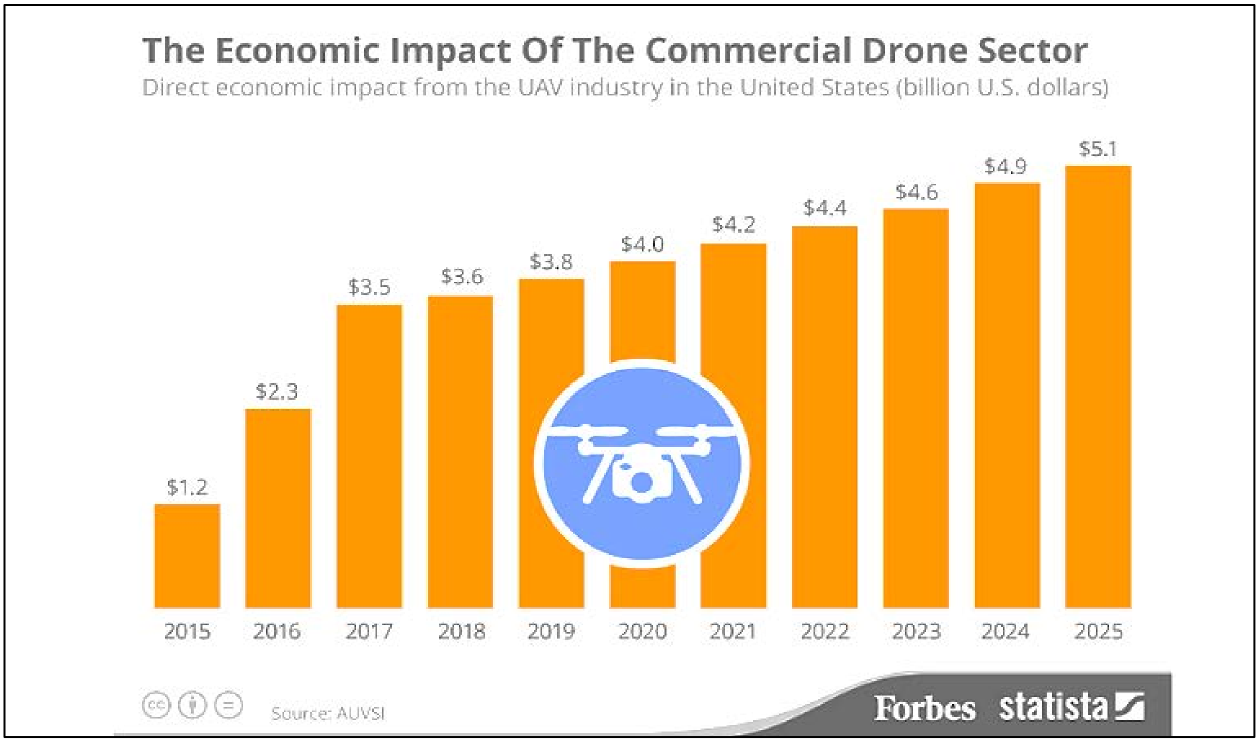


Figure 4. Commercial sector growth.[20]

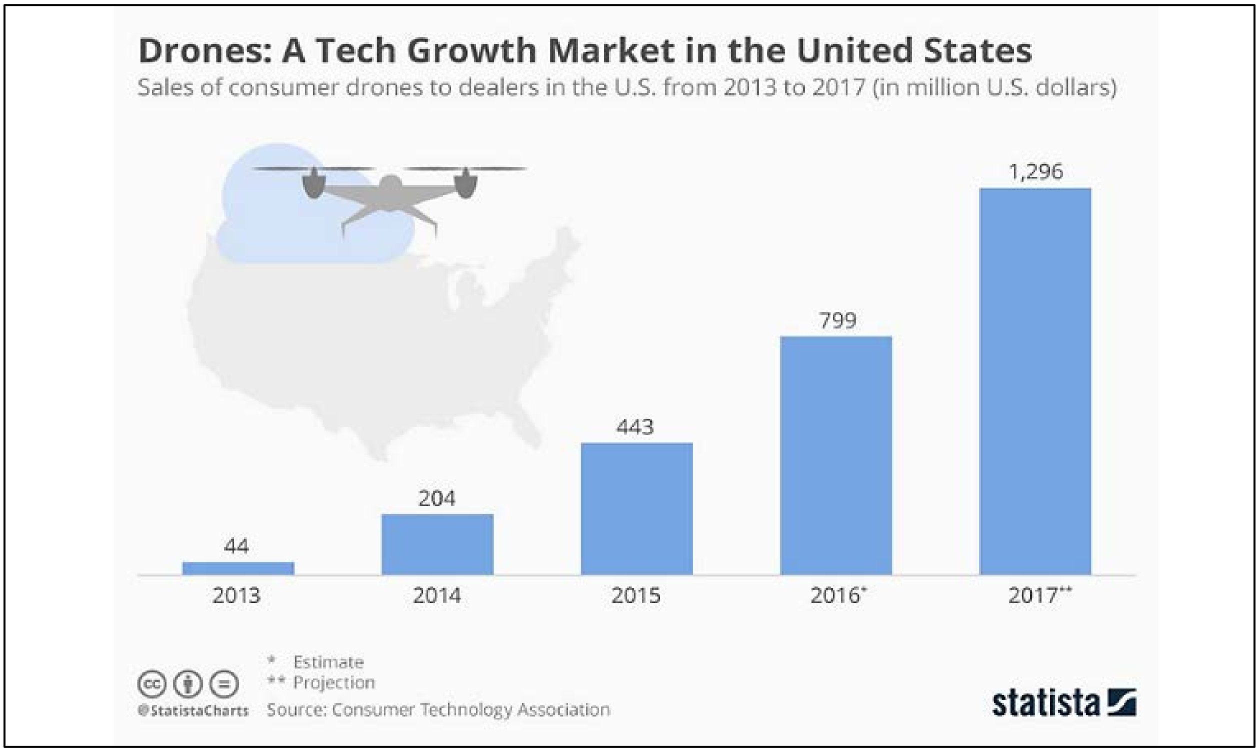


Figure 5. UAV industry revenue.[21]

Dual-Use Dilemma

As with other technologies, restricting the terrorist use of UAVs suffers from a dual-use dilemma which limits the options for slowing the advancement of the technology and its spread to terrorist groups. For example, a UAV designed to disperse pesticides and upgraded with a heavier payload capacity could benefit terrorists in parallel. This applies to other flight characteristics, as well (e.g., speed and flight time). With the private sector serving as the primary catalyst of innovation and technology advancement, this increasingly available dual-use technology is well-suited for asymmetrical warfare. Paul Scharre states that "the U.S. military is used to competing in a world where some of the most game-changing innovations—such as stealth, GPS, and precision-guided weapons—come from the U.S. defense sector. It is ill-prepared for a world where such technologies are widely available to all."[22]

Tactics

"This is how adaptive the enemy (ISIS) was. About five or six months ago, it was a day that the Iraqi effort almost came to a screeching halt. Literally in the span of 24 hours, there were up to 70 UAVs in the air. At one time, 12 'killer bees,' if you will, right overhead."[23]

—SOCOM Commander General Raymond Thomas, May 2017

The degree to which adversaries prefer a UAV on the battlefield over other methods depends on its effectiveness. These consumer UAVs give terrorists the potential to carry out aerial operations with a high level of flexibility and agility that can be categorized as nonlethal and lethal, described in **Table 3**.

Table 3. Terrorist UAV combat applications.*

Type of Operation	Tool	Objective
Non-Lethal	Sensor Payload	ISTAR External Communication
Lethal	Offensive Payload	Weaponize Disruption|Deception

Nonlethal Operations: Sensor Payloads

Sensor payloads take the form of various instruments attached to UAVs used for (1) intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) and (2) external communication (propaganda). Cameras constitute most sensor payloads employed by consumer UAVs for such objectives, compared to, for instance, apparatuses that record weather or air quality. In many cases, these high-definition cameras are integrated into the UAV and use varying amateur and industrial, scientific and medical (ISM) radio bands to transmit the video to a ground monitor, such as a computer or smartphone application. Less expensive models, such as DIY versions, may attach lightweight consumer cameras such as GoPro or Garmin.

* This typology accounts for the scope of this report, deliberately leaving out other types of operation, such as smuggling.

ISTAR missions. UAVs enable terrorists to substantially enhance combat operations by providing them with formerly unobtainable aerial ISTAR that enables them to more efficiently gather information on adversaries from the sky, as well as to cover more surveillance ground. In March 2016, ISIS posted a surveillance video taken by a UAV online showing bases in northern Iraq with American and Iraqi forces. Several days later, a Katyusha rocket landed at one of the outposts hosting over 100 marines, killing one of them. "The strike was so accurate that military officials described it as a 'golden shot' to pierce the defenses put in place, and there was speculation that a UAV was used in the targeting."[24]

UAVs provide terrorists with the ability to conduct operations from a three-dimensional grid—attaining valuable information inaccessible from the ground. This enables terrorist organizations to enhance and optimize their kinetic ground attacks, such as placing suicide vehicles in ideal locations after reviewing adversary patterns or attaining information on weak points in secure facilities. Numerous videos have documented ISIS using UAVs to accurately guide and direct the driver of vehicle-borne improvised explosive devices (VBIEDs), benefiting from real-time video feeds. These UAV-enabled ISTAR operations work in conjunction with terrorists' ground attacks, enhancing their effectiveness.

Propaganda. Another facet enhanced is media operations and propaganda—a tactic that has served as a foundational pillar for modern insurgency strategy: public frenzy of palpable threats, recruitment tools, paranoia, and so on. In general, no terrorist group has extracted propogandist value from its operations as effectively as ISIS. The original leader of ISIS, Abu Musab al-Zarqawi, detailed this importance in July 2005—"How many battles has this nation lost because the lack of media/information? This is because of neglecting this aspect [of jihadi media]. Some look at the military fight as the most important thing, and others are not important. This is a shortsighted [view]."[25]

Thus, it is no surprise they are increasingly integrating UAV videos into their propaganda messages. In January 2017, ISIS released a 30-minute video titled "Knights of Bureaucracy," recording numerous suicide bombings inducing mass casualties from a UAV above.[26] This aerial video technology enables militants to record ground attacks from a distant location previously too dangerous and unfeasible to document from the ground.

Lethal Operations: Offensive Payloads

Consumer UAVs can be readily modified to carry lethal offensive payloads by exchanging the mounted camera for a small charge. UAVs can potentially be armed with a range of offensive payload, including conventional ammunition, IEDs, mortars or grenades, and biological or chemical weapons. As Armament Research Services states, "the method of weapon payload integration, and the effectiveness of such payloads, will also vary significantly, determined by a range of factors including desired application; UAV type, size, and GTOW; payload type, size, and method of function; and more."[27] The following section details technical characteristics of direct, indirect, and aerial-dispersal attacks (see **Figure 6**).

Direct attacks. Direct attacks involve a UAV striking a target with an offensive payload or acting as a self-guided weapon itself. Under this method, intended targets involve immobile sites (e.g., buildings and infrastructure) and mobile sites (e.g., public crowds, individuals, and vehicles.) Unconventional weapons of destruction, such as chemical, biological, or nuclear agents, can serve as a payload on these aerial vehicles but are limited in applications due to weight capacity and other limitations. Primary factors that determine effectiveness of direct attacks include the type of weaponry and blast, the accuracy and probability of hitting the intended target, and the UAV's capability to transport the selected payload.

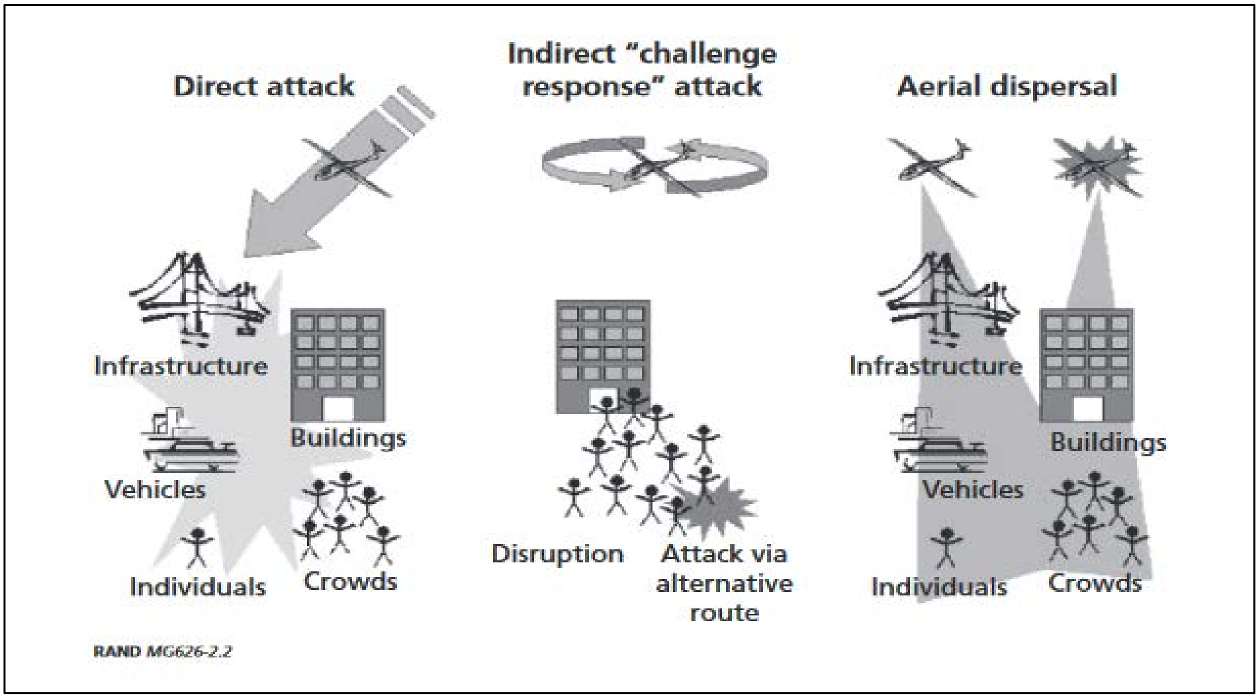


Figure 6. Type of lethal UAV attack.[28]

UAVs can deploy a multitude of explosive weapons; the varying degree of blast and fragmentation damage ultimately determines the effectiveness against targets. A UAV-released mortar projectile has the potential to inflict severe casualties in populated areas, especially suitable for circumstances that present ground-based security obstacles. However, buildings and other infrastructure are typically less affected by such fragmentation attacks.

Direct attacks require a mechanism that remotely releases the payload. After a terrorist successfully weaponizes the aircraft for flight, the UAV must possess the ability to release the payload. Accessories are increasingly available and sold in the marketplace that, when assembled and integrated, can achieve this feat.[29] However, even with this adopted technology, the precision of direct attacks remains low. This is due primarily to the limitations of the release mechanism, as well as the as-yet unavailable self-guided capability of weapons accessible to terrorists.

For IEDs embedded into the UAV itself, the payload release feature is not necessary as the UAV serves as the delivery mechanism. This mode of attack offers a significant increase in accuracy due to the users' autonomy of controlling the weaponized UAV.

In some instances, nonstate groups can engage UAVs in an offensive capacity without a weaponized payload. This security threat is highlighted by several close calls in recent years—the UK Air Proximity Board reported over 30 near misses between UAVs and commercial aircrafts in the first half of 2016 alone, with four of the incidents deemed serious Category A close calls.[30] Notably, a British Airways Airbus A320 was struck by a UAV in midair as it prepared for landing at Heathrow airport.

Possible "bird strike" attacks in which a UAV intentionally flies into the engine of an aircraft is becoming a more pressing security concern. Sion Owen Roberts, a pilot for the Royal Air Force, stated his worry for future attacks: "Whilst I was serving in the RAF, it was always dangerous when we accidentally hit a bird. A bird can cause significant damage to an aircraft and the same sort of damage could occur from a UAV strike, LiPo batteries [in UAVs] are extremely volatile and you wouldn't want one disappearing down an aircraft engine."[31] Furthermore, it is extremely difficult to identify the people responsible for these UAV collisions, as they occur at thousands of feet in the air. This anonymity adds another tactical dimension to potential terrorist attacks.

Recent developments in consumer UAVs' "direct attack" capabilities present challenges to current security paradigms, leading to a justified heightened sense of fear for adversaries and the public. Security strategies for facilities, national borders, and military battle zones primarily revolve around deterring nonstate threats on the ground due to the assumption that such entities have a limited attack portfolio. However, these small-scale UAVs challenge these conventional security views, increasing the possibility of aerial attacks and penetration that even modern air defenses do not account for, and ultimately shrinking previously assumed safe areas.

For instance, there have been dozens of UAVs documented flying over nuclear facilities in France and the United Kingdom.[32] More concerning, in January 2015 a commercialized DJI quadcopter breached secret service security, crash landing on the White House lawn after a recreational user lost control, ending up in national headlines.[33] Although the latter event was unintentional, it publicly highlights the flaws in security defenses around the U.S. and across the globe—hypothetically the UAV could have been armed with explosives.

Indirect attacks. While there is no documented evidence of terrorist indirect UAV attacks, the number of direct attacks makes an indirect scenario a plausible future threat. Indirect attacks would be employed to produce a ground reaction to a seemingly tangible threat (e.g., groups of people evacuate a crowded area such as a concert due to fear of a UAV strike). The production of a reaction on the ground could be the extent of the operational objective, or the intended outcome could be to subsequently enable the real attack (e.g., bombs located at numerous locations when the crowd evacuates).[34] UAVs could be used in a similar capacity as suicide bombs and IEDs for indirect attack methods, channeling people to vulnerable positions with the intent to instigate a follow-up direct attack, or merely producing mass chaos.

The effectiveness ultimately hinges on the reaction from potential targets. The consistent use of cell phones and luggage for bomb attacks has enabled these items to be used for indirect attacks, prompting evacuations and relocating people to unknowingly dangerous locations, perhaps beyond security parameters. The extent that UAVs will serve in a similar threat-only capacity ultimately depends on terrorists consistently deploying successful direct attacks using UAVs. This could result in an increased psychological effect of UAVs flying, increasing public concern as is the case with a luggage bomb.

Propaganda videos of UAV attacks disseminated by insurgent groups like ISIS can significantly aid the legitimization of such threats, making this tactic more attractive to other terrorist groups of individuals. The "Knights of Bureaucracy" video in January 2016 surprised many when it showed ISIS using dual-use UAVs to release explosives against targets; this video resulted in countless television segments and media articles dedicated to describing this new threat.

Aerial dispersal. Aerial dispersal is an attack method in which the UAV releases a payload typically over a prolonged distance. The utility of this attack mode depends on the ability and accuracy of disseminating the weapon at the designated target while accounting for external conditions, as well as timing this gradual dispersal over a certain period for maximum effectiveness. This method has become a concern for national security officials, as the two primary obstacles for terrorists after acquiring chemical or biological weapons is their ability to effectively transport and release it.

Currently, consumer UAVs are limited in payload capacity. While the lack of technical knowledge and infrastructure limited terrorists just several years ago, the rapid UAV innovation in the agricultural industry—applications ranging from drop dusting and crop scouting to drought assessment—have advanced the technologies that could enable an effective aerial dispersal attack. The UK government set up numerous surface-to-air missiles on the top of buildings for the 2012 Olympic venue after intelligence revealed ISIS was training members to produce toxic chemicals with linkages to England.[35]

Some of this technology is already available in the consumer marketplace as UAVs have been designed and manufactured to disperse pesticides and similar chemicals for farmers, ranging from ten-thousand to thirty-thousand dollars.[36] For instance, the DJI Agras MG-1 is advertised as an agricultural pesticide fertilizer costing approximately ten-thousand dollars that can carry a maximum payload of 12.5 kg, with 10 minutes of flight time.[37] Currently available consumer UAVs provide terrorists with the capability to employ aerial dispersal attacks by methods formerly unobtainable, although with likely limited effectiveness due to the relative immaturity of this technology.

Countertactics

The rapid proliferation of UAVs used by terrorists and adversarial nation states has motivated some manufacturing companies and nation states to develop technologies to counter this emerging threat. UAV companies such as DJI have increasingly come under criticism for drones ending up in the hands of terrorists. The main avenue in which companies have proven to be effective in developing countermeasures is via software.

UAV manufacturers such as DJI have successfully integrated virtually designated no-fly zones—dubbed "geofencing"—over the past several years. DJI states that this technology ensures "the UAV will by default not fly into or take off in, locations that raise safety or security concerns."[38] The software explicitly bans the aircraft to fly in forbidden areas, such as historic landmarks, military bases, and airports—the UAV is physically unable to enter designated areas selected by the manufacturing company. In 2017, DJI expanded this list to numerous locations in Syria and Iraq, such as the city of Mosul, due to documented use by ISIS.[39]

However, as *MIT Technology Review* describes, it is unclear whether no fly zones will be effective in stopping terrorist UAV usage.[40] ISIS UAVs that are assembled from various components—purchased on popular websites like HobbyKing.com that have benefited from the growing DIY movement—are essentially impossible to restrict. Older software does not include this countermeasure, and some companies have not yet integrated geofencing capabilities into their product lines. Furthermore, when implemented, such software's operator can simply choose to turn off navigation and control the UAV by remote controller or to cache the map offline. In some cases, skilled programmers can hack and disable geofencing limitations, enabling the operator to use navigation features.[41] The increasing demand for circumventing this technology has created an opportunity for businesses. A UAV company based in Russia called Coptersafe openly sells hardware and software modifications for around $350 that enables DJI users to deceive the UAV's GPS software and operate in no-fly zones.[42] Finally, such restrictions inadvertently weaken other actors, as well. Iraqi militias and nongovernment organizations (NGOs) in nearby areas operating UAVs are subject to the same geofencing no-fly zones.

From a national security standpoint, the United States military is devoting substantial resources to countermeasures, but there is debate surrounding what is a proportional response. Earlier this year, General David Perkins announced that a U.S. ally deployed a Patriot missile, costing around $3 million, to shoot down a $200 drone from Amazon.[43] Gen. Perkins states that "it certainly exposes in very stark terms the challenge which militaries face in attempting to deal with the adaptation of cheap and readily available civilian technology with extremely expensive, high-end hardware designed for state-on-state warfare."[44]

An effective strategy will revolve around (1) detection and (2) defense technology specifically designed for small, consumer-grade UAVs. Radars cannot easily distinguish between a large aircraft and a small drone. The challenge therefore lies in developing better sensors that identify the type of aircraft threat to deploy a proportional counterattack. Along with the private sector, this technology is currently being developed and employed by the U.S on a larger and more advanced scale, although information on the specifics is limited.

As alternatives to weapons such as the Patriot missile, nonkinetic tactics are being developed to terminate this threat; nonkinetic weapons use radiofrequency signals (electromagnetic pulse, or EMP) to destroy UAVs, which is termed "electronic warfare." Airbus DS electronics and border security and Dedrone partnered to release a counter-UAV system that reliably detects and employs electronic countermeasures. Similar to Chess Dynamics and Blighter Surveillance Systems, Airbus' platform uses jamming technology to disrupt the datalink between the operator and UAV, causing the UAV to fly back to its takeoff point or land at a certain location, within the operational range of 3 to 6 miles.[45] "Due to the Smart Responsive Jamming Technology developed…the jamming signals are blocking only the relevant frequencies used to operate the drone while other frequencies in the vicinity remain operational," Airbus stated. "Since the jamming technology contains versatile receiving and transmitting capabilities, more sophisticated measures like remote control classification and GPS spoofing can be used as well. This allows effective and specific jamming and, therefore, a takeover of the UAV."[46]

More lethal methods employed include the Laser Weapons System (LWS) developed by the United States Navy. Lieutenant Cale Hughes stated that "it is throwing massive amounts of photons at an incoming object."[47] This has proven to be highly effective in destroying UAVs.

In addition, cyber warfare will serve a crucial role. Consumer-grade UAVs lack encrypted communication datalinks, so they are vulnerable to hacks. As these aircrafts are increasingly adopted into terrorists' strategy on the battlefield, counter-drone technology will be ever more crucial in neutralizing this threat, ensuring that terrorists are unable to extract the novel benefits.

Terrorists' Operational Use

There are currently four terrorist groups identified by the *Combatting Terrorism Center* at West Point (CTC) with a proven pattern of consistent UAV employment and, in some cases, rudimentary production facilities: Islamic State (ISIS), Hamas, Hezbollah, and Jabhat Fateh al-Sham.[48] Low barriers of access to such technology suggest a high probability that other terrorist groups are attempting to establish similar programs, with evidence of their adversaries following suit. Militant groups such as the Iraqi Armed Forces and Free Syrian Army are increasingly integrating UAVs into their warfare strategy to combat terrorists. However, there is not sufficient evidence of consistent use by other terrorist organizations.

Because ISIS is widely recognized as the prominent terrorist organization across the globe posing the most significant near-term threat—and for the sake of brevity—we focus our selected case study on this group. The selected operational cases represent the benefits that terrorist groups can gain from currently available UAV technology: propaganda, ISTAR, and direct attacks. Also, while Hamas and Hezbollah contain more advanced UAV technology that cross the threshold into midsize military UAVs, it is primarily provided by Iran. Such technology provided by benefactor countries remain outside the scope of this report.

Available evidence of UAV usage is substantially limited by the inherent difficulties of meticulously tracking each terrorist UAV operation across the globe. It is conceivable that sporadic terrorist use of hobbyist and commercial UAVs is on a larger scale than documented, with a wider scope of applications.

Selected Case Study: Islamic State (ISIS)

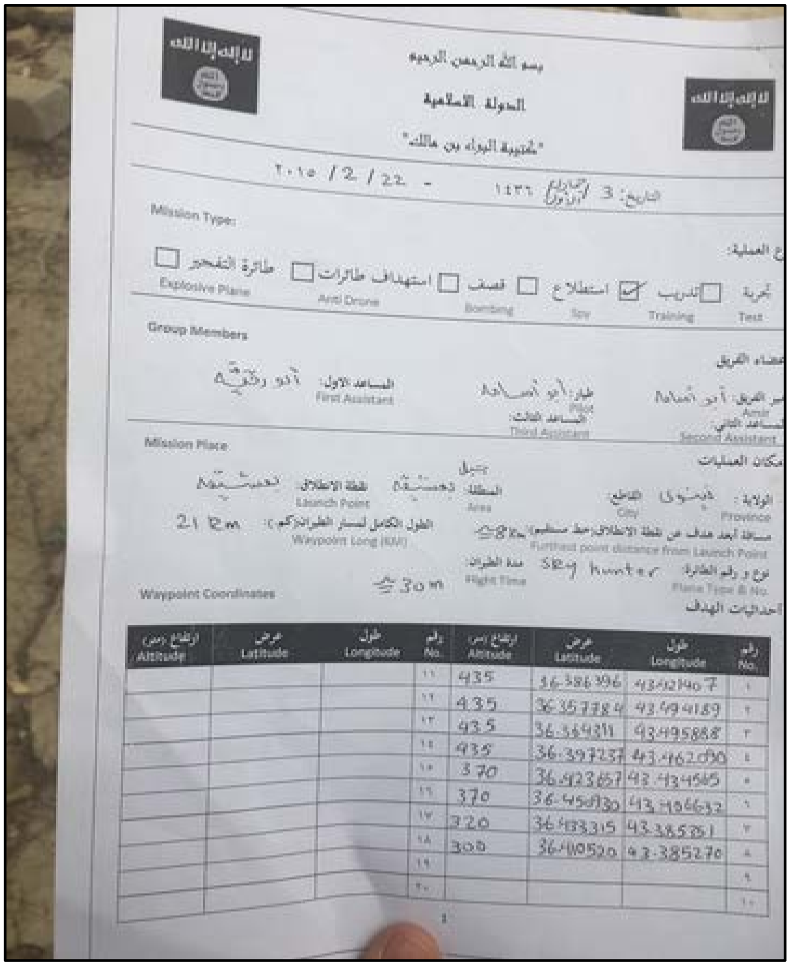
The first evidence of ISIS interest in UAVs dates back to 2013 in Iraq, prior to officially announcing its caliphate and denouncing ties with al-Qaeda. Iraqi authorities thwarted the organizations' plot attempting to use toy aircrafts to disperse chemical weapons in the Middle East, Europe, and North America.[49] Defense ministry spokesman Mohammed al-Askari stated that the arrests were possible due to collaboration between foreign and Iraqi intelligence services.[50] This included the discovery of several chemical manufacturing workshops containing sarin and mustard gas.

Since the formal inception of the Islamic State, records reveal that the organization successfully employed UAVs across Syria and Iraq beginning in 2014 for propaganda videos. This is supported by a May 2014 video "The Clanging of the Swords Part IV," partially recorded with a UAV by ISIS's media department al-Furqan that was disseminated to the public after seizing control of Falluja, Iraq.[51] A few months later, in December 2014, an ISIS video captured the first ever aerial footage of ground suicide bombings.[52] The terrorist group filmed ground attacks in the Battle of Kobane in Syria, evidently adding a unique element to its propaganda. Since then, most ISIS videos released included suicide attacks by their militants, in many cases using VBIEDs. (The DJI Phantom series quadcopters and fixed-wing Skywalker X8 models are the most popular choices among ISIS combatants due to accessibility, capabilities, and ease of use.)

ISIS ISTAR operations have also significantly benefited from UAV technology. In August 2014, a video on YouTube showed Islamic militants in Syria using the DJI Phantom UAV for surveillance footage to scout the Tabqa military airfield that was subsequently captured by ISIS.[53] Colin Clarke, a political scientist at Rand Corporation, stated that the UAVs were used "as a recon method to scout out what the base looked like before going in with a more kinetic attack," and "they used multiple suicide bombers to gain entry."[54] The location of this takeover is significant due to its location in Raqqa, the city considered the capital of ISIS operations. In April 2015, ISIS released a video of a UAV used for reconnaissance to enhance combat operations at the Baiji oil refinery facility located in Iraq. They used the UAVs "to gather intelligence…for command and control purposes, as well as act as [*sic*] spotters for artillery pieces."[55] The footage highlights ISIS fighters operating the UAVs from a relatively advanced ground control station[56]

As UAVs increased in accessibility and capability in subsequent years, ISIS rapidly integrated consumer UAVs into its battlefield operations on a larger and wider scale. In October 2016, Kurdish forces in Iraq shot down and retrieved an ISIS-operated UAV, assuming this was merely another surveillance UAV. During disassembly, however, it exploded, killing two Kurdish soldiers in what is the first record of an ISIS UAV causing fatalities.[57] In January 2017, the terrorist organization formally announced the formation of the "Unmanned Aircraft of the Mujahideen" drone fleet.[58] In the same month, ISIS released a video titled "The Knights of the Dawawin" showing ISIS deploying explosives from UAVs.[59] This tactic was also used in operations involving UAVs releasing explosives on crowds and stationary vehicles like tanks. These videos are edited propaganda material to deceive viewers of a false sense of capability and accuracy—not showing failed attacks or inaccurate aerial bombings.

These videos highlight the rapid increase of ISIS UAV direct attacks. In the past two years, rudimentary UAV workshops were discovered in Mosul and Ramadi comprising makeshift materials and documents. These documents and UAV components purchased by ISIS were given to the CTC at West Point by Harvard research fellow Vera Mironova, providing insight into the organization's effort to establish a systematic UAV program.[60] The documents, all from 2015, indicate that ISIS created a documentation system for UAV operators to record their missions (see **Figure 7**). The form enables the user to detail specifics of the mission such as attack method and navigation route, creating a systematic catalog for all UAV employments. Such methodical data collection enables the organization to optimize future UAV operations.



بسم الله الرحمن الرحيم

الدولة الإسلامية

٢٠١٥ /2 /22 - ١٤٣٦

Mission Type:

Explosive Plane | Anti Drone | Bombing | Spy | Training | Test

Group Members

First Assistant | Pilot | Amir | Third Assistant | Second Assistant

Mission Place

Launch Point | Area | City | Province

21 km | Waypoint Long (KM)

Furthest point distance from Launch Point | ≈8 km

Flight Time | ≈30 m

Plane Type & No. | sky hunter

Waypoint Coordinates

Altitude	Latitude	Longitude	No.	Altitude	Latitude	Longitude	No.
			١١	435	36.386396	43.4121407	١
			١٢	435	36.357784	43.494189	٢
			١٣	435	36.364311	43.495888	٣
			١٤	435	36.397237	43.462090	٤
			١٥	370	36.423657	43.434565	٥
			١٦	370	36.450930	43.406632	٦
			١٧	320	36.433315	43.385261	٧
			١٨	300	36.410520	43.385270	٨
			١٩				٩
			٢٠				١٠

Figure 7. ISIS UAV documentation system.[61]

Furthermore, other documents reveal the methods by which ISIS acquires hardware and software to modify UAVs as well as build its own aircraft from varying components. As CTC notes, "none of these points are tremendously surprising as the level of focus—and obsession with details and standardization—mirrors the approach the Islamic State has taken with other programs, like the development of rockets and mortars."[62] The purchase and receipt forms suggest that although the terrorist groups' UAVs are limited in capability, ISIS is increasing efforts to bolster its program. The documents list purchased items such as GPS devices, GoPro cameras, propeller blades, and telecommunication units.

The tactical utility that ISIS combatants derive from UAVs is highlighted by the increasing number of deployments. However, despite several deceiving propaganda videos, these UAVs are significantly limited in capability. As RAND states, the advantage UAVs "…provide is not, therefore, in the destructive power that they can carry; rather, it is in the way they carry it and the distance from which they allow an adversary to control its delivery."[63]

How UAVs Alter the Insurgency Landscape

We summarize below unique advantages and limitations of UAVs in the insurgency landscape. **Figure 8** describes the operational advantages provided by UAVs' aerial capabilities.

Unique Advantages

- Increasing use and accessibility of hobbyist and commercial UAVs provides a low barrier to entry due to widespread global production and subsequent decreasing costs. These cheap and portable aircrafts require minimal technological infrastructure, making them ideal for asymmetric conflicts.
- Novel capabilities that otherwise are not available add an effective aerial facet to their operations. Thus, they offer higher marginal utility extracted for weaker actors like terrorists due to formerly nonexistent airpower. Although low-barrier to entry, in many cases can replicate the capabilities and effectiveness of conventional human-inhabited aircrafts, especially for ISTAR operations.
- The dual-use dilemma for technology with both military and civilian applications applies to UAVs—those manufactured for civilian use can be applied in parallel for battlefield operations (crop-spray dispersal, chemical attack dispersal).
- Such technology's affordability, ease of purchase, and portability indicates a high degree of difficulty in predicting and detecting use by terrorists.
- Anonymity to operate UAVs from a remote location is suitable for terrorists, and especially for state benefactors who wish to conceal support for a certain terrorist group.

Current Limitations

- Payload weight capacity.
- Flight time, range, and speed.
- Unable to deploy advanced missiles and large bombs.
- Susceptible to broad range of countermeasures.
- Datalinks are unencrypted.

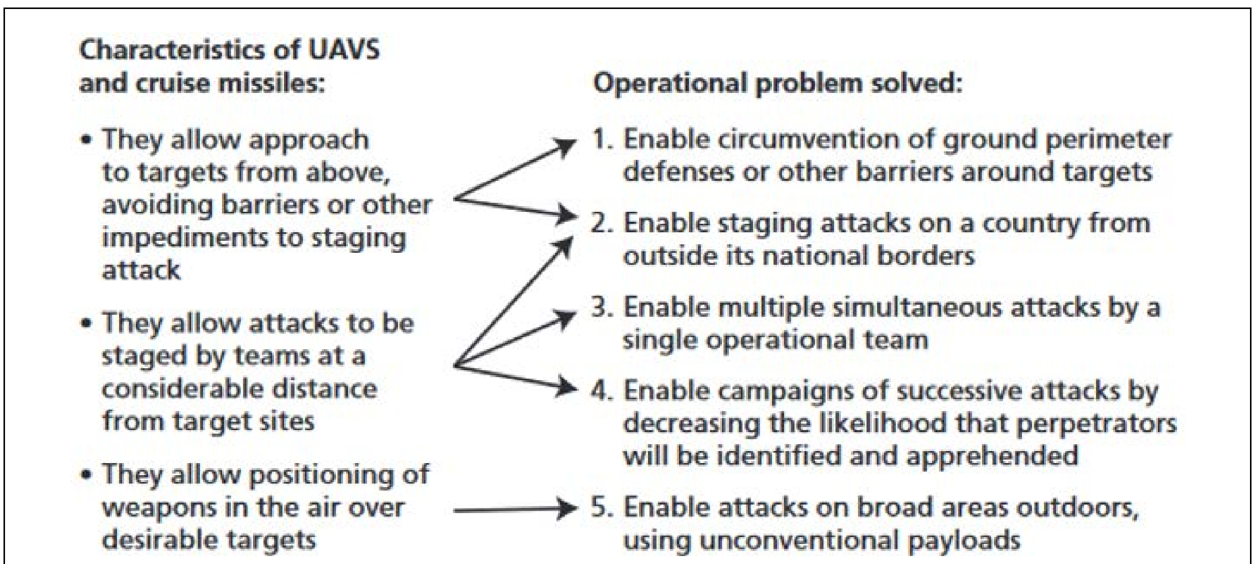


Figure 8. Operational advantages of aerial capabilities.[64]

Future Trends and Developments

The rapid research and development of consumer-grade UAVs will continue in several dimensions: autonomy, swarming, and general flight characteristics (e.g., speed, size, payload capacity). The latter is assumed to follow a similar linear growth trajectory that is usually inherent in a product line: faster with longer range, greater payload weight capacity, and more. However, autonomous and swarming capabilities may exponentially increase and become achievable in the near future, with the possibility of substantially enhancing terrorists' aerial capabilities.

Autonomous Enhancements

"Sense and avoid," also known as "obstacle avoidance," is a technology that will propel UAV autonomy into the future, serving as a primary catalyst in enabling UAVs to cross the "fully autonomous" threshold. The industry recognizes the significant demand in the market for such capability. It will enhance the range of applications possible, especially in the commercial industry as businesses need UAVs capable of maneuvering in challenging conditions—such as construction and mining. While GPS enables a UAV to fly to a set location without human interaction, GPS alone is incapable of detecting all obstacles.

Increasingly integrated into newer versions are sensors that employ a basic degree of obstacle avoidance, preventing the UAVs from crashing. While sense-and-avoid capabilities have improved over the past several years—the new DJI Mavic Pro uses numerous interconnected sensors to detect its surroundings, such as large objects—they are unreliable in avoiding smaller obstacles and maintaining a comprehensive 360-degree view.

An additional autonomous feature being developed—using a majority of the same hardware and software for sense and avoid—is the ability for UAV tracking. DJI names it "ActiveTrack," which enables the operator to select a subject—such as a person or vehicle—and follow it. This provides a new tactic in three forms, as detailed by DJI: "Trace—follow behind, in front or circle a subject as it moves. Profile—fly alongside a person or object. Spotlight—Keep the Mavic Pro camera trained on an object while you fly almost anywhere."[65] The industry is investing significant resources into perfecting this facet of autonomous flight, fiercely competing with each other. As with sense and avoid, its operational capability remains a work in progress, with future autonomous developments ultimately determining the fruition of this technology.

Ongoing progress and integration of technology, such as Light Detection and Radar (LIDAR) improved GPS accuracy and more efficient batteries, will enable mass-produced UAVs to simultaneously sense and avoid obstacles and achieve full autonomy in the next couple of years.[66] Furthermore, research and development of fully autonomous automobiles undertaken by companies such as Google and Tesla—roadways being an environment that inherently contains significantly more obstacles than the sky—will certainly speed this process, with the potential for integration across multiple industries.

Swarming

As UAVs become smaller and cheaper to produce with full autonomy achievable in the near future, swarming—defined as multiple autonomous aircrafts networked together—will serve as the backbone for a new era of UAV capabilities. This technology provides one person with the ability to operate a potentially limitless number of UAVs. In multiple instances, Intel has showcased its synchronized Shooting Star UAV fleet used for light shows that can "easily be programmed for any animation."[67] Earlier this year during the Super Bowl halftime show, several hundred UAVs formed to create the American flag.[68] More recently, Intel has used them as alternatives to fireworks—they are evidently safer and environment-friendly. As a longer-term objective, researchers at Harvard's Wyss Institute are working on their RoboBee project, developing paper-clip-sized UAVs for a variety of applications—weather and agricultural monitoring and even crop pollination—due to the decline of honey bees.[69]

As this technology inevitably disseminates into the consumer marketplace, the asymmetrical battlefield ramifications are clear. For instance, hundreds of tiny quadcopters can fly together to gather ISTAR. Advanced military operations could be overmatched by terrorists' synchronized attack UAVs approaching from multiple directions at once. As an example, thousands of small aircraft could initiate an attack on a warship. While most might be destroyed, many would penetrate the defenses and inflict severe damage. The ability to fly in unison indicates that such an operation will require one operator—or perhaps none—leading to higher utility extracted per militant. While currently available UAVs are limited in payloads compared to military aircrafts, hundreds of UAVs releasing explosives simultaneously would significantly mitigate this disparity. With no designated leader in a UAV swarm, as all components are equal, such a threat is exponentially difficult to destroy.

UAV swarm technology remains in its infancy stage, but as with sense-and-avoid and UAV tracking, it is rapidly evolving. Once all three are achieved and adopted into mass market UAVs, swarming will substantially alter the asymmetrical warfare landscape.

Conclusion

As UAV trends—primarily technological sophistication and availability—continue to rapidly proliferate in the civilian sector, terrorists will find themselves increasingly able to purchase and operate such technology for a wide scope of applications. With a low cost of several hundred dollars, consumer drones enable novel and formerly unattainable aerial capabilities to be integrated into terrorists' tactical arsenal. As the ease of use continues to be demonstrated, additional terrorist groups will likely seek to develop a UAV capability.

Effective terrorist applications primarily revolve around nonlethal tactics—surveillance and propaganda. On a smaller and less successful scale, lethal operations have increasingly been undertaken—with effectiveness ultimately determined by developments of future technology. Based upon operational terrorist use and lethality, individual deployment of single-consumer UAVs can currently be classified as a niche threat. However, autonomous and swarm technologies—along with substantial increases in payload capacity and other characteristics—will soon be proliferated among the consumer drone market, drastically altering the asymmetric warfare landscape and enhancing the scope of the threat to potentially include the delivery of chemicals or biological agents. Thus, we conclude that lethal UAV tactics are a dangerous frontier of future terrorist attacks, and will likely experience an increase in utility fueled by future technology developments, primarily in the commercial industry.

Subsequently, counterproliferation efforts face difficult challenges, mostly due to the dual-use nature of this technology that distorts the line between civilian and military use—an aspect that is particularly advantageous to terrorists due to the inherent challenges of monitoring such activity. UAV developments in the private sector—which is increasing in market value by billions of dollars each year—will continue to cause a corresponding increase in capabilities for terrorist organizations. With at least 10 countries possessing robust armed drones and an additional 20 developing such capabilities, it nearly impossible to contain the dissemination of this technology in which terrorists can benefit from a state benefactor.

As a result, developments outside of the terrorist sphere should be evaluated, delving into the private sector—the main catalysts of consumer UAV technology—to gain an all-encompassing understanding of this threat.

References

1. Singer, P.W. “The Global Swarm.” *Foreign Policy*. 11 Mar. 2013. Web. 07 July 2017. <http://foreignpolicy.com/2013/03/11/the-global-swarm/>.
2. “Gartner Says Almost 3 Million Personal and Commercial Drones Will Be Shipped in 2017.” *Gartner*. Web. 20 June 2017. <http://www.gartner.com/newsroom/id/3602317>.
3. “Chronology of Aum Shinrikyo's CBW Activities.” *James Martin Center for Nonproliferation Studies*. 23 June 2016. Web. 09 Aug. 2017. <http://www.nonproliferation.org/chronology-of-aum-shinrikyos-cbw-activities/>.
4. “Unmanned Aircraft Systems (UAS) Regulations & Policies.” *FAA seal*. 6 July 2017. Web. 24 July 2017. <https://www.faa.gov/uas/resources/uas_regulations_policy/>.
5. Sayler, Kelley. “A World of Proliferated Drones: A Technology Primer.” June 2015. Web. 22 June 2017. <http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf>.
6. Hoenig, Milton. “Hezbolla and the Use of Drones as a Weapon of Terrorism.” N.p., Spring 2014. Web. 29 June 2017. <https://fas.org/wp-content/uploads/2014/06/Hezbollah-Drones-Spring-2014.pdf>.
7. Sayler, Kelley. “A World of Proliferated Drones: A Technology Primer.” June 2015. Web. 22 June 2017. <http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf>.
8. DJI Phantom 3 Picture
9. Friese, Larry. “Special Report No. 2: Emerging Unmanned Threats.” *Armament Research Services*. Feb. 2016. Web. 14 June 2017. <http://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/>.
10. Friese, Larry. “Special Report No. 2: Emerging Unmanned Threats.” *Armament Research Services*. Feb. 2016. Web. 14 June 2017. <http://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/>.
11. Friese, Larry. “Special Report No. 2: Emerging Unmanned Threats.” *Armament Research Services*. Feb. 2016. Web. 14 June 2017. <http://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/>.
12. News, Measure. “Drones: Autonomous or automated?” *Measure*. N.p., n.d. Web. 11 Aug. 2017. <http://www.measure.com/blog-2017/drones-autonomous-or-automated>.
13. Ibid.
14. Coxworth, Ben. “DJI Phantom can now perform autonomous flight.” *New Atlas - New Technology & Science News*. New Atlas, 02 July 2014. Web. 28 July 2017.
15. Coxworth, Ben. “DJI Phantom can now perform autonomous flight.” *New Atlas - New Technology & Science News*. New Atlas, 02 July 2014. Web. 28 July 2017.
16. “Gartner Says Almost 3 Million Personal and Commercial Drones Will Be Shipped in 2017.” *Gartner*. N.p., n.d. Web. 11 July 2017. <http://www.gartner.com/newsroom/id/3602317>.

    Glaser, April. “DJI is running away with the drone market.” *Recode*. Recode, 14 Apr. 2017. Web. 9 Aug. 2017. <https://www.recode.net/2017/4/14/14690576/UAV-market-share-growth-charts-dji-forecast>.
17. Glaser, April. “DJI is running away with the drone market.” *Recode*. Recode, 14 Apr. 2017. Web. 9 Aug. 2017. <https://www.recode.net/2017/4/14/14690576/UAV-market-share-growth-charts-dji-forecast>.
18. Conger, Kate. “How consumer drones wind up in the hands of ISIS fighters.” *TechCrunch*. TechCrunch, 13 Oct. 2016. Web. 29 June 2017. <https://techcrunch.com/2016/10/13/how-consumer-drones-wind-up-in-the-hands-of-isis-fighters/>.

19. Ibid.
20. McCarthy, Niall, Felix Richter, Chris Siegwald, and Robin Huedepohl. "Infographic: The Economic Impact Of The Commercial Drone Sector." *Statista Infographics*. 20 Oct. 2015. Web. July 2017. <https://www.statista.com/chart/3898/the-economic-impact-of-the-commercial-drone-sector/>.
21. Loesche, Dyfed, Felix Richter, Chris Siegwald, and Robin Huedepohl. "Infographic: Drones: A Tech Growth Market in the United States." *Statista Infographics*. N.p., 23 May 2017. Web. July 2017. <https://www.statista.com/chart/9525/sales-of-consumer-drones-to-dealers-in-the-us/>.
22. Scharre, Paul. "Robotics on the Battlefield Part II: The Coming Swarm." Center for a New American Security, Oct. 2014. Web. July 2017. <http://acikistihbarat.com/Dosyalar/robots-us-military-swarm-technology-report-acikistihbarat.pdf>.
23. Tucker, Patrick. "In Urgent Request, US Special Ops Adds 350 Kamikaze Drones to Fight ISIS." *Defense One*. N.p., 18 May 2017. Web. July 2017. <http://www.defenseone.com/technology/2017/05/Special-Ops-Gets-350-More-Kamikaze-Suicide-UAVs-to-Fight-ISIS/137987/?oref=DefenseOneTCO&utm_content=buffer2428d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>.
24. Michael S. Schmidt and Eric Schmitt. "Pentagon Confronts a New Threat From ISIS: Exploding Drones." *The New York Times*. The New York Times, 11 Oct. 2016. Web. June 2017. <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.
25. Katz, Rita. "How ISIS Maximizes the Terror From Its Killer Drones." *The Daily Beast*. The Daily Beast Company, 03 May 2017. Web. June 2017. <http://www.thedailybeast.com/how-isis-maximizes-the-terror-from-its-killer-drones>.
26. Watch, Heavy Terror. "WATCH: New ISIS Video Shows Them Using Drones to Conduct 'Airstrikes' in Mosul." *Heavy.com*. N.p., 24 Jan. 2017. Web. July 2017. <http://heavy.com/news/2017/01/new-isis-islamic-state-video-knights-of-bureaucracy-mosul-iraq-wilayat-ninawa-modified-weaponized-drones-bombings-airstrikes-uncensored-video/>.
27. Friese, Larry. "Special Report No. 2: Emerging Unmanned Threats." *Armament Research Services*. Feb. 2016. Web. 14 June 2017. <http://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/>.
28. Jackson, Brian A., David R. Frelinger, Michale J. Lostumbo, and Robert W. Button. "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles." 2008. Web. June 2017. <https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf>.
29. "Inspire Payload Drop System (Stork)." *Fire Cam*. Web. July 2017. <http://firecam.com/inspire-payload-drop-system-stork/?gclid=COKmmPmM0NQCFdaEswodHI4O3g>.
30. "Drones involved in near misses at UK airports." *BBC News*. BBC, 29 Jan. 2016. Web. June 2017. <http://www.bbc.com/news/uk-35442130>.

    "'Drone' hits British Airways plane approaching Heathrow Airport." *BBC News*. BBC, 17 Apr. 2016. Web. June 2017. <http://www.bbc.com/news/uk-36067591>.
31. Drones and planes in mid-air near misses increase." *BBC News*. BBC, 07 July 2016. Web. June 2017. <http://www.bbc.com/news/uk-england-36734096>.
32. Baylon, Caroline. "Drones: The Threat to Nuclear Plants." *Newsweek*. N.p., 11 Mar. 2016. Web. July 2017. <http://www.newsweek.com/drones-threat-nuclear-plants-294458>.
33. Calamur, Krishnadev. "'Quad Copter' Flew Into, Crashed On White House Grounds, Secret Service Says." *NPR*. NPR, 26 Jan. 2015. Web. July 2017.
34. Jackson, Brian A., David R. Frelinger, Michale J. Lostumbo, and Robert W. Button. "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles." 2008. Web. June 2017. <https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf>.

35. Stephanie Condron and Christopher Leake,"Poison Drones Carrying Biological Weapons Are New Olympic Threat, Warns Colonel in Charge of Keeping London Calm," Daily Mail Online, May 5, 2012

36. Atherton, Kelsey D. "This Drone Sprays Pesticides Around Crops." *Popular Science*. 23 June 2016. Web. July 2017. <http://www.popsci.com/agri-drone-is-precision-pesticide-machine>.

37. "AGRAS MG-1's Specifications - DJI." *DJI Official*. Web. Aug. 2017. <http://www.dji.com/mg-1/info#specs>.

38. "DJI Introduces New Geofencing System for its Drones." *DJI Official*. N.p., n.d. Web. July 2017. <https://www.dji.com/newsroom/news/dji-fly-safe-system>.

39. Dalton, Andrew. "DJI grounded its drones in Iraq and Syria to lock out extremists." *Engadget*. 27 Apr. 2017. Web. July 2017. <https://www.engadget.com/2017/04/26/dji-no-fly-zones-grounded-drones-iraq-syria/>.

40. Condliffe, Jamie. "Can a Chinese drone manufacturer's no-fly zone software stop ISIS from weaponizing drones?" *MIT Technology Review*. MIT Technology Review, 30 Apr. 2017. Web. July 2017. <https://www.technologyreview.com/s/604279/can-djis-no-fly-zone-software-stop-isis-from-weaponizing-UAVs/>.

41. Ibid.

42. "Drone Pilots Are Buying Russian Software to Hack Their Way Past DJI's No Fly Zones." *Motherboard*. Web. July 2017. <https://motherboard.vice.com/en_us/article/8x9jv4/drone-pilots-are-buying-russian-software-to-hack-their-way-past-djis-no-fly-zones>.

43. Molloy, Mark. "Missile worth $3m used to shoot down cheap drone from Amazon." *The Telegraph*. Telegraph Media Group, 16 Mar. 2017. Web. July 2017. <http://www.telegraph.co.uk/technology/2017/03/16/missile-worth-3m-used-shoot-cheap-amazon-drone/>.

    "US ally used Patriot missile to shoot down small drone." *Fox News*. FOX News Network, 15 Mar. 2017. Web. July 2017. <http://www.foxnews.com/tech/2017/03/15/us-ally-used-patriot-missile-to-shoot-down-small-drone.html>.

44. "US ally used Patriot missile to shoot down small drone." *Fox News*. FOX News Network, 15 Mar. 2017. Web. July 2017. <http://www.foxnews.com/tech/2017/03/15/us-ally-used-patriot-missile-to-shoot-down-small-drone.html>.

45. "Joining forces to counter the illegal drone threat with UAVs." *Security News Desk*. 03 Aug. 2016. Web. July 2017. <http://www.securitynewsdesk.com/joining-forces-to-counter-the-illegal-drone-threat-with-uavs/>.

    "Airbus Displays Counter-UAV System at CES 2016." *Research & Development*. 14 June 2016. Web. July 2017. <https://www.rdmag.com/news/2016/01/airbus-displays-counter-uav-system-ces-2016>.

46. "Airbus Displays Counter-UAV System at CES 2016." *Research & Development*. 14 June 2016. Web. July. 2017. <https://www.rdmag.com/news/2016/01/airbus-displays-counter-uav-system-ces-2016>.

47. Rathmell, Peter. "Navy successfully tests anti-drone laser weapon." *Navy Times*. 19 July 2017. Web. July 2017. <https://www.navytimes.com/articles/navy-successfully-tests-anti-drone-laser-weapon>.

48. Rassler, Don. "Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology." Oct. 2016. Web. June 2017. <https://ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf>.

49. "Iraq uncovers al-Qaeda 'chemical weapons plot'." *BBC News*. BBC, 01 June 2013. Web. Aug. 2017. <http://www.bbc.com/news/world-middle-east-22742201>.

50. Ibid.

51. Zelin, Aaron Y. "Al-Furqān Media presents a new video message from the Islamic State of Iraq and al-Shām: "Clanging of the Swords, Part 4"." *A clearinghouse for jihādī primary source material, original analysis, and translation service*. N.p., 01 June 2014. Web. July 2017. <http://jihadology.net/2014/05/17/al-furqan-media-presents-a-new-video-message-from-the-islamic-state-of-iraq-and-al-sham-clanging-of-the-swords-part-4/>.
52. Stalinsky, Steven. "A Decade Of Jihadi Organizations' Use Of Drones – From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones." *MEMRI - The Middle East Media Research Institute*. N.p., 21 Feb. 2017. Web. June 2017. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>.
53. Tadjdeh, Yasmin. "ISIS Used A Miniature Surveillance Drone In Its Biggest Syria Victory Yet." *Business Insider*. Business Insider, 28 Aug. 2014. Web. July 2017. <http://www.businessinsider.com/isis-has-demonstrated-drone-capabilities-2014-8>.
54. Ibid.
55. Caleb Weiss, "Islamic State Uses UAVs to Coordinate Fighting in Baiji," Long War Journal, April 17, 2015.

    Rassler, Don. "Remotely Piloted Innovation: Terrorism, Drones, and Supportive Technology." Oct. 2016. Web. June 2017. <https://ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf>.
56. Stalinsky, Steven. "A Decade Of Jihadi Organizations' Use Of Drones – From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones." *MEMRI - The Middle East Media Research Institute*. N.p., 21 Feb. 2017. Web. June 2017. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>.
57. Michael S. Schmidt and Eric Schmitt. "Pentagon Confronts a New Threat From ISIS: Exploding Drones." *The New York Times*. The New York Times, 11 Oct. 2016. Web. July 2017. <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.
58. Friese, Larry. "Special Report No. 2: Emerging Unmanned Threats." *Armament Research Services*. Feb. 2016. Web. 14 June 2017. <http://armamentresearch.com/special-report-no-2-emerging-unmanned-threats/>.
59. Watch, Heavy Terror. "WATCH: New ISIS Video Shows Them Using Drones to Conduct 'Airstrikes' in Mosul." *Heavy.com*. N.p., 24 Jan. 2017. Web. July 2017. <http://heavy.com/news/2017/01/new-isis-islamic-state-video-knights-of-bureaucracy-mosul-iraq-wilayat-ninawa-modified-weaponized-drones-bombings-airstrikes-uncensored-video/>.
60. Rassler, Don, and Muhammad Al-`Ubaydi, Vera Mironova. "CTC Perspective--The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft." N.p., 31 Jan. 2017. Web. June 2017. <https://ctc.usma.edu/posts/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft>.
61. Rassler, Don, and Muhammad Al-`Ubaydi, Vera Mironova. "CTC Perspective--The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft." N.p., 31 Jan. 2017. Web. June 2017. <https://ctc.usma.edu/posts/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft>.
62. Ibid.
63. Jackson, Brian A., David R. Frelinger, Michale J. Lostumbo, and Robert W. Button. "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles." 2008. Web. June 2017. <https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf>.
64. Jackson, Brian A., David R. Frelinger, Michale J. Lostumbo, and Robert W. Button. "Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles." 2008. Web. June 2017. <https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf>.

65. Corrigan, Fintan. “Mavic Pro – Highlights You Need to Know.” *DJI Buying Guides*. 11 July 2017. Web. Aug. 2017. <https://store.dji.com/guides/mavic-pro-highlights-need-know/>.

66. Wilkinson, Interview Conducted by Jake. “The Future of Drone Technology - Autonomy, Collision Avoidance and Advanced Sensors.” *AZoSensors.com*. 16 May 2017. Web. Aug. 2017. <http://www.azosensors.com/article.aspx?ArticleID=782>.

67. “Intel Drones Light Up Lady Gaga Performance During Pepsi Zero Sugar Super Bowl LI Halftime.” *Intel Newsroom*. 5 Feb. 2017. Web. July 2017. <https://newsroom.intel.com/news-releases/intel-drones-light-lady-gaga-performance-pepsi-zero-sugar-super-bowl-li-halftime/>.

68. Ibid.

69. Hambling, David. “Future - The next era of drones will be defined by 'swarms'.” *BBC*. BBC, 27 Apr. 2017. Web. July 2017. <http://www.bbc.com/future/story/20170425-were-entering-the-next-era-of-drones>.