A WORLD OF PROLIFERATED DRONES:
A Technology Primer

By Kelley Sayler
Foreword by Paul Scharre & Ben FitzGerald
About the Author

Kelley Sayler is an associate fellow at the Center for a New American Security.

Acknowledgements

I would like to thank my colleagues at the Center for a New American Security (CNAS) and other organizations for sharing their insights and expertise throughout the writing of this paper. In particular, I am grateful to Paul Scharre and Ben FitzGerald for their substantive guidance and critical feedback. Thank you to Alex Velez-Green for providing excellent research assistance, to Melody Cook for her creative vision, and to Michael Horowitz and Matthew Fuhrmann for generously sharing their data on drone proliferation.

Readers should note that CNAS receives funding from some of the organizations mentioned in this report. CNAS maintains a broad and diverse group of more than 100 funders, including private foundations, government agencies, corporations, and private individuals, and retains sole editorial control over its ideas, projects, and products. A complete list of financial supporters can be found on CNAS’ website at www.cnas.org/content/cnas-supporters.

This project is possible thanks to the support of the Smith Richardson Foundation.

The views expressed in this report are solely those of the author, who is responsible for any error of fact, analysis, or omission.
A WORLD OF PROLIFERATED DRONES: A Technology Primer

By Kelley Sayler
Foreword by Paul Scharre and Ben FitzGerald

TABLE OF CONTENTS

I. Foreword 2
II. Executive Summary 4
III. Introduction 7
IV. Hobbyist Drones 10
V. Midsize Military and Commercial Drones 14
VI. Large Military-Specific Drones 19
VII. Stealth Combat Drones 24
VIII. Potential for Overmatch 28
IX. Conclusion 30
I. FOREWORD

While U.S. drone strikes have captured public attention, the United States does not have a monopoly on drones. Over 90 countries and non-state actors operate drones today, including at least 30 that operate or are developing armed drones. This global proliferation raises a number of challenging security issues. Are states more likely to engage in cross-border surveillance missions or attacks with drones than with manned systems? Are states more willing to shoot down a drone, since there is no one on board? If one nation shoots down another nation’s drone, is that an act of war?

The answers to these questions hinge not principally on the technology itself, but on the ways in which states and non-state actors will use drones and how they will perceive their use by themselves and others. The Center for a New American Security (CNAS) project A World of Proliferated Drones, a joint undertaking of the 20YY Warfare Initiative and the Technology and National Security Program, will examine these issues through a series of reports and war games engaging international audiences. Understanding and anticipating the likely contours of a drone-saturated world will help the U.S. government take steps today to influence, as best it can, a future landscape that is most conducive to American interests. In support of this objective, A World of Proliferated Drones will examine the challenges arising from this new strategic landscape and seek to provide policy options that the United States and its allies and partners could adopt in the near term to successfully manage these challenges.

Not all drones are equal in capability and consequence for their use, and assumptions about which types of drones are relevant from a military and national security perspective inform conclusions about the consequences of drone proliferation and possible policy responses. While much of the existing literature on drones has focused on the challenges arising from the proliferation of high-end military-grade systems, in reality, a far wider range of drones is already being used for disruptive purposes. As drones become increasingly accessible and affordable, it will be essential for policymakers to consider the full range of drone capabilities and their potential impact on military operations and international security.

This first report, an overview of the drone capabilities available to various actors at present and in the future, is intended to serve as a stand-alone primer for national security professionals on drone proliferation. Additionally, this report lays the technical foundation for further analysis and upcoming war games that will be conducted as part of this project, A World of Proliferated Drones.

Paul Scharre is a Senior Fellow and Director of the 20YY Warfare Initiative at CNAS.

Ben FitzGerald is a Senior Fellow and Director of the Technology and National Security Program at CNAS.
II. EXECUTIVE SUMMARY

We are living, increasingly, in a drone-saturated world. In recent years, drones, or unmanned aerial vehicles (UAVs), have proliferated rapidly around the globe in both military and civilian spheres. Today, over 90 nations and non-state groups are known to operate drones, including at least 30 countries that either operate or are developing armed drones. As this technology continues to proliferate, simple weaponized drones carrying explosives or chemical or biological agents will be increasingly within the reach of virtually any state, non-state actor, or individual. If used in large numbers, these systems could potentially enable states, non-state groups, and individuals to achieve overmatch against a significantly more capable adversary.

In an effort to describe the kinds of capabilities that will be available to various types of actors, this paper will examine and categorize UAVs based on two characteristics: (1) the degree to which they are accessible to any given actor; and (2) the technology base and infrastructure required to produce and/or operate them. Using this taxonomy, the paper identifies four categories of systems: hobbyist drones, midsize military and commercial drones, large military-specific drones, and stealth combat drones.

First, hobbyist drones include those that are readily available for purchase – generally for no more than a few thousand dollars – by any interested party. These systems may either be pre-assembled or assembled from component parts and do not require formal infrastructure or training to operate. Current commercial off-the-shelf technology enables hobbyist drones to perform aerial surveillance or deliver payloads – including explosives or chemical or biological agents – of a few kilograms at ranges up to a few kilometers. Eventually, however, hobbyist drones will be capable of GPS-independent autonomous flight and could be used for stand-alone strikes or, in large numbers, saturation swarming attacks against government, military, and civilian targets.

Second, midsize military and commercial drones are those that are not generally available to individuals due to cost or infrastructure requirements. These systems may, however, be sold or transferred to foreign militaries and non-state actors. While these systems are generally used for surveillance purposes at present, they are likely to be increasingly armed, either with an explosive payload that can perform a kamikaze mission or, in time, with releasable precision-guided munitions.

Third, large military-specific drones – often including armed drones – require substantial military infrastructure to operate and are not generally accessible to or operable by actors beyond major militaries. These systems represent a high level of technological sophistication, with greater range, endurance, and payload capacity than both hobbyist and midsize commercial and military drones. In addition, many large military-specific systems are capable of beyond-line-of-sight communications and signal-jamming and, if armed, can deliver payloads of over 1,000 kilograms at ranges of thousands of kilometers. Partnered with a secondary drone operating as a line-of-sight communications relay, these drones could reach several hundred kilometers into neighboring territory without the use of satellite communications. These factors enable large military-specific drones
to operate and strike deep inside an adversary’s territory. However, without stealth or electronic attack capabilities, they will remain vulnerable to advanced air defenses as well as to enemy fighter aircraft.

Finally, stealth combat drones include those that contain highly sophisticated technologies, such as low-observable features, and are not accessible to nonindigenous producers. While several countries — including Russia, Israel, China, India, France, Italy, Sweden, Spain, Greece, Switzerland, and the United Kingdom — are in the process of developing stealth combat drones, the United States is the only known operator of such systems at this time.

As drones at all levels of technological sophistication become increasingly available to responsible and disruptive actors alike, it will be vital for the United States to consider the implications of this new strategic landscape and to prepare for the challenges of a world of proliferated drones. Drone proliferation is happening now, and while the United States cannot stop drone proliferation, it can help influence how drones are used and perceived by others.
III. INTRODUCTION

We are living, increasingly, in a drone-saturated world. In recent years, drones, or unmanned aerial vehicles (UAVs), have proliferated rapidly around the globe in both military and civilian spheres. Today, at least 90 nations and non-state groups are known to operate drones, including 10 countries with armed drones. An additional 20 countries have armed drone programs in development. As this technology continues to proliferate, simple weaponized drones will be increasingly within the reach of virtually any state and many non-state actors. Already, non-state actors such as Hamas, Hezbollah, the Islamic State of Iraq and Syria (ISIS), and Libyan rebel groups have used drones to conduct tactical surveillance. Individuals also have access to increasingly sophisticated commercial off-the-shelf drones and components that can either be used for surveillance or weaponized. Indeed, even without missiles or releasable bombs, drones can be used as cheap precision-guided weapons to disperse chemical or biological payloads or simply to strike targets with explosives. If used in large numbers, these systems could potentially enable states, non-state groups, and individuals to achieve overmatch against a significantly more capable adversary.

As drones continue to proliferate, it will be vital for policymakers to understand the underlying technologies and the capabilities these technologies will provide to various actors. Current drones vary widely in affordability, accessibility, and capability – from inexpensive, commercially available systems flown by short-range joystick controls to multimillion-dollar, high-end military-grade systems that require substantial training and infrastructure to operate. This paper will therefore examine and categorize UAVs based on two characteristics: (1) the degree to which they are accessible to any given actor; and (2) the technology base and infrastructure required to produce and/or operate them. Using this taxonomy, the paper identifies four categories of systems:

- **Hobbyist drones** include those that are readily available for purchase – generally for no more than a few thousand dollars – by any interested party. These systems may either be pre-assembled or assembled from component parts and do not require formal infrastructure or training to operate.

- **Midsize military and commercial drones** are those that are not generally available to individuals due to cost or infrastructure requirements. These systems may, however, be sold or transferred to foreign militaries and non-state actors.

- **Large military-specific drones** – often including armed drones – require substantial military infrastructure to operate and are not generally accessible to or operable by actors beyond major militaries.

- **Stealth combat drones** include those that contain highly sophisticated technologies, such as low-observable features, and are not accessible to nonindigenous producers. While several countries are developing stealth combat drones, the United States is the only known operator of such systems at this time.
Increasing Availability
Decreasing Technology Base and Infrastructure

HOBBYIST
- Limited payload capacity
- Limited range/persistence
- High-definition imagery/video transmission
- Autonomous GPS and waypoint navigation

MIDSIZE MILITARY & COMMERCIAL
- Moderate payload capacity
- Moderate range/persistence
- Advanced radar
- Encrypted, high-bandwidth data links
- Limited jamming/electronic warfare
- Target identification and designation
- Communications relay function

LARGE MILITARY-SPECIFIC
- Larger payload capacity
- Long range/persistence
- Low-probability-of-intercept radar
- Enhanced jamming/electronic warfare
- Beyond line-of-sight communications
- Releasable missiles/bombs

STEALTH COMBAT
- Low observable features
- Low-probability-of-intercept/low-probability-of-detection data links
- Higher resistance to adversary jamming

LARGE MILITARY-
SPECIFIC
(e.g., IAI Heron, Northrop Grumman Global Hawk)

MIDSIZE MILITARY & COMMERCIAL
(e.g., Boeing Insitu Scan Eagle, Ghods Ababil)

HOBBYIST
(e.g., DJI Phantom)
IV. HOBBYIST DRONES

While military-support drones have been in use since the early 1960s, hobbyist drones have only recently exploded in popularity. Between 2011 and 2013, SZ DJI Technology Co., the largest manufacturer of hobbyist drones, saw an almost 3,000 percent increase in annual revenue – to $130 million. Continuing this pattern of growth, the company’s revenue reached $500 million in 2014 and is expected to reach as much as $1 billion in 2015. As sales of hobbyist drones continue to increase, we are likely to see an attendant reduction in cost and increase in drone capabilities. This development will in turn grant individuals and non-state actors – particularly those without existing state patrons – unprecedented access to highly advanced technologies.

Capability Overview

While hobbyist drones have been on the market for some time, recent technological advances have moved the systems’ capabilities well beyond the relatively crude models previously operated by joystick consoles and constrained by line-of-sight operating restrictions. Indeed, current commercial drone technologies – available for purchase in either pre-assembled or customizable, component form – enable a number of high-end capabilities that were formerly the monopoly of major military powers.

Many commercial off-the-shelf (COTS) drones – including the best-selling model, the DJI Phantom – are now equipped with GPS and waypoint navigation systems. These systems enable the drone to accurately determine and hold its position, in turn removing the need for line-of-sight communications and allowing for autonomous flight. In the event that the operator loses contact with the system, this feature can return the drone to a predetermined location.

Operators of pre-assembled systems can also take advantage of smartphone-based control systems, dramatically improving ease of use. Such systems enable the user to navigate the drone simply by selecting a destination on a map or even by merely tilting the user’s phone. While some COTS drones contain firmware that restricts flight in designated “no-fly zones,” skilled programmers could remove these restrictions. Furthermore, such restrictions do not apply to drones assembled from component parts.

High-definition video cameras are also widely available on COTS drones and, when combined with video downlinks, can provide real-time intelligence, surveillance, and reconnaissance (ISR) capabilities to multolocation receivers, though these capabilities are often limited by range and battery life. As an alternative, operators can extend the drone’s range by recording higher-resolution video footage and still photographs for later viewing. Operators can additionally use a control module to make in-flight adjustments to the camera’s tilt and resolution, thus optimizing ISR capabilities. Infrared thermal cameras,
enabling heat detection, are also available for commercial purchase.

While not yet fully integrated into existing systems, camera-, laser-, and sensor-based sense-and-avoid capabilities will likely be introduced on hobbyist drones within the next several years. These capabilities will enable the drone to identify and maneuver around obstacles in its flight path when in autonomous flight, rather than restrict it to a set path determined by pre-programmed GPS coordinates or waypoints that may contain otherwise impassable objects. These technologies will, in turn, lead to a dramatic improvement in drone autopilot features.

Over time, hobbyist drone capabilities will become increasingly accessible to non-state actors and individuals and increasingly sophisticated – ultimately approaching currently available small military-grade capabilities and blurring the line between civilian and military systems.

Today, relatively capable COTS drones are widely available for purchase, ranging in price from several hundred to several thousand dollars. While most are used for recreational purposes, they have also been used for public nuisance – generally in the form of unauthorized surveillance or flights over private property or restricted government areas, notably including the White House and nuclear facilities in France, Belgium, and the United Kingdom.

Commercially available drones are also known to have been used for warfighting purposes by both state and non-state actors. The Ukrainian military has made extensive use of commercial systems, including modified DJI Phantoms and other reconfigured hobbyist drones, in its conflict with the self-declared Donetsk People’s Republic, a rebel group backed by Russia. Reports indicate that ISIS has also used a commercial drone, the DJI Phantom FC40, for surveillance purposes. Usage of these systems will almost certainly continue to expand in conjunction with falling prices and improved ease of use.

Though most COTS drones have relatively short range and limited payload capacity, they have been successfully used to smuggle drug packages and could be modified to carry explosives, firearms, or other damaging objects instead.

With this proliferation will come increased prospects for the disruptive employment of hobbyist systems by both individuals and non-state actors. Most concerning is the potential that such systems could be weaponized. Though most COTS drones have relatively short range and limited payload capacity, they have been successfully used to smuggle drug packages and could be modified to carry explosives, firearms, or other damaging objects instead. To date, The Wall Street Journal reports, “authorities in the U.S., Germany, Spain, and Egypt have foiled at least six potential terrorist attacks with drones since 2011,” and more can be expected. The difficulty of monitoring and regulating the sale of such systems in the future – a major contributor to their appeal to disruptive actors – is compounded by the fact that they are dual-use, with both military and civilian applications, and unlike firearms do not require registration.

Furthermore, given the construction material, small size, and flight altitude of most hobbyist systems, they are rarely visible on radar and are therefore particularly difficult to detect. For this reason, defenses against them often require either visual or possibly auditory identification or concerted signal-jamming to disrupt the operator’s communications link with the system and/or the system’s GPS. Most such detection methods,
however, require either a pre-existing knowledge or expectation of the system’s presence in a given area and thus are markedly less effective against unanticipated use. And as future systems begin to incorporate GPS-independent means of navigation, such as visual-aided or inertial navigation, signal-jamming will cease to be an effective countermeasure. For these reasons, hobbyist systems hold significant disruptive potential.

**Summary**

Relatively affordable hobbyist drones, costing no more than a few thousand dollars, are widely available for purchase by states, non-state actors, and individuals alike. These systems have a comparatively lower level of sophistication than higher-end systems and require no standing infrastructure to operate.

**CAPABILITIES:**
- Deliver payloads, including explosives, of no more than a few kilograms at ranges up to a few kilometers
- Capture high-definition images and video; real-time transmission at ranges of up to a couple of kilometers
- Persist for limited periods (no more than approximately 15 minutes)
- Operate in communications-denied environments using fully autonomous GPS and waypoint navigation
- Limited navigation in GPS-denied environments using low-cost inertial navigation systems

**LIMITATIONS:**
- Limited payload, endurance, and range
- Vulnerable to electronic countermeasures, including GPS-jamming and spoofing
- Vulnerable to small-arms fire
- Unencrypted data links and video feeds vulnerable to intercept
- No ability to release missiles or bombs

**TECHNOLOGY TRENDS:**
- Sense-and-avoid systems to navigate autonomously around obstacles
- Encrypted communications links
- Multivehicle cooperative control, allowing one operator to control several vehicles in flight simultaneously
- Increased range, payload, and endurance
- Visual-aided navigation to allow precision GPS-independent navigation, eliminating vulnerability to jamming and spoofing attacks
MIDSIZE MILITARY & COMMERCIAL DRONES
V. MIDSIZE MILITARY AND COMMERCIAL DRONES

Beyond individual recreational use, drones are now used for a wide range of commercial and military activities. In the commercial sphere, they increasingly serve as low-cost alternatives to helicopters for the purposes of professional photography and videography. Drones are used by the agriculture industry to survey and spray crops, by aid groups to monitor disaster zones and deliver humanitarian assistance, by conservationists to track animal populations and land use, and by oil and gas companies to map and model infrastructure. They are also being considered for commercial deliveries – most famously by online retailer Amazon.com – though their use in this capacity is restricted within the United States by Federal Aviation Administration regulations.

Midsize commercial and military systems frequently offer an additional level of sophistication when compared with hobbyist drones, and their accessibility is generally more restricted. Their cost – ranging from hundreds of thousands of dollars to millions of dollars – is also generally prohibitive for individual use. There are, however, a growing number of midsize commercial and military systems available to state actors through foreign military sales. Certain producers of such systems – Iran, in particular – have additionally transferred them to non-state actors.

**Capability Overview**

Compared with hobbyist drones, most midsize commercial and military systems are larger, with longer range and endurance, and carry more sophisticated payloads and communications technologies. Similar to hobbyist drones, they are primarily used as ISR platforms, though they could additionally be used to deliver dangerous payloads, including explosives or chemical or biological weapons.

Like hobbyist drones, midsize commercial and military systems are capable of either manual or autonomous flight and can carry high-definition cameras, including night-vision infrared cameras. Many of these systems can also carry advanced electro-optical cameras that are capable of capturing high-resolution images. Furthermore, synthetic aperture radar and/or ground moving target indicator radar are being increasingly integrated onto tactical UAVs, allowing for all-weather terrain mapping, target tracking, and even improvised explosive device (IED) detection. Feeds from these sensors can then be transmitted in real time over high-bandwidth, encrypted data links that increase the difficulty of unauthorized access by third parties.

Furthermore, many midsize commercial and military systems can create a beyond-line-of-sight communications relay for ground-based radios, thus extending the communications range for associated ground forces and improving situational awareness and coordination. For example, Boeing Insitu’s ScanEagle, operated by a number of countries including Yemen, has successfully received ground control station data at a range of over 28 kilometers; it has then relayed that data to ground forces an additional 10 kilometers away.
In addition, the range and endurance of midsize commercial and military systems are significantly greater than those of hobbyist systems. While most advanced hobbyist systems are limited to around 20 minutes of flight and an operating distance of no more than a couple of kilometers, midsize commercial and military systems often have an endurance of over an hour at a range of at least 10 kilometers. For example, AeroVironment’s RQ-11B Raven – the most common military UAV in operation – has an endurance of 60 to 90 minutes, depending on operating conditions and payload, and a range of between eight and 10 kilometers. Ghods’ Ababil-3 – variants of which Iran has reportedly transferred to Hamas and Hezbollah, among others – has a claimed endurance of up to four hours and a range of 100 kilometers. These performance characteristics enable increased loiter time and further improve targeting and ISR collection capabilities.

Targeting can be further enhanced by laser range finders and illuminators, which are found on many midsize military systems, including newer payload modules for the RQ-11B Raven. These capabilities allow the system to gauge the distance of a given object and to lock on to the coordinates of a stationary or mobile target. This information can then be passed to laser-guided munitions carried by other armed platforms. Additional enablers such as Sentient’s Kestrel, an automated detection software designed to provide persistent target identification, are under development.

Finally, some drones in this category, such as Elbit Systems’ Hermes 450, have limited electronic intelligence and jamming capabilities that allow the drone to intercept or disrupt adversary communications or to neutralize adversary tracking radar.
Given their relative affordability, accessibility, and ease of use, midsize commercial and military systems – with varying degrees of sophistication – are operated by a number of state and non-state actors. Today, 87 countries – ranging from major military powers such as the United States and China to smaller nations such as Cyprus and Trinidad and Tobago – operate [drones] and this number is likely to grow in the years to come.

Nor are these systems confined to nation-states alone. Both Hamas and Hezbollah are known to operate midsize military-grade systems, believed to be variants of the Iranian-supplied Ababil-1 and Mohajer 4, respectively. They have repeatedly flown these systems into Israeli airspace, penetrating as far as 225 kilometers into Israel. Indeed, Hezbollah’s Mohajer 4, which it calls the Mirsar, was able to elude Israeli radar on several occasions due to its small size.

Similarly, Libyan rebels employed a tactical, night vision-equipped commercial surveillance drone – the Aeryon Scout – in their fight against Moammar Gadhafi’s forces. Weighing in at just over a kilogram and capable of being transported in a backpack, the Scout provided the rebels with a portable ISR option that enabled them to identify and collect information on government artillery positions. In addition, the drone was controlled via a map-based touchscreen console and required less than a day of training to operate, further contributing to the Scout’s utility to the rebels.

While these midsize commercial and military systems were originally intended as reconnaissance platforms, like hobbyist systems, they can be – and have been – weaponized. Though these systems may not be large or sophisticated enough to carry a releasable bomb or missile at present, they can carry explosives or other hazardous materials and can thus function as precision-guided kamikaze weapons, blurring the line between UAVs and small missiles.

For example, in 2013, Palestinian security forces detected a Hamas plot to launch armed UAVs into Israel. Hezbollah met with greater success during the 2006 Lebanon War, when it managed to fly drones laden with a total of 27 kilograms of explosives and projectiles near major cities in Israel and Lebanon. Though the drones were ultimately shot down, they held the potential to inflict significant damage on civilian populations. While both Hamas and Hezbollah have large quantities of unguided rockets that they have launched into Israel on numerous occasions, UAVs could increase the precision of an attack, resulting in a greater ability to inflict casualties or strike specific high-profile targets. In addition, drones can be more challenging to shoot down than rockets since they do not follow a high, ballistic trajectory – a factor that complicates detection and interception. This threat will only increase as such organizations gain access to systems that are capable of launching missiles, or as miniaturized missiles such as Raytheon’s Pyros (small tactical munition) or Textron’s Fury become more accessible.

These capabilities hold substantial destructive potential that terrorist organizations and other disruptive actors are likely to exploit. Indeed, as Yochi Dreazen has written, the world is fast...
approaching "the next evolution of warfare-by-remote-control, when weaponized robotic planes give terrorist groups de facto air forces."38

Summary

Midsize commercial and military drones, ranging in cost from tens of thousands of dollars to no more than a couple million dollars, are widely available for purchase by states and industry. They may also be procured and operated by more established or well-organized non-state actors with limited supporting infrastructure.

CAPABILITIES:

- Deliver payloads of up to a couple hundred kilograms at ranges of up to a couple hundred kilometers
- Capture high-definition images and video at ranges of up to a couple hundred kilometers; real-time transmission at ranges of up to around 30 kilometers
- Persist for moderate periods (generally between 60 minutes and a few hours)
- Operate in communications-denied environments using fully autonomous GPS and waypoint navigation
- All-weather terrain mapping and target tracking via advanced radar
- Identify and designate targets via laser range finders and illuminators
- Transmit data via encrypted, high-bandwidth data links
- Limited jamming and electronic intelligence-gathering
- Communications relay function
- Ability to perform a kamikaze mission using an explosive payload

LIMITATIONS:

- Vulnerable to countermeasures, including GPS-jamming and spoofing, small-arms fire (at lower altitudes), and man-portable air-defense systems (MANPADS) (at higher altitudes)
- Not survivable in contested or denied airspace
- Line-of-sight communications
- Data links vulnerable to interception
- No current ability to release missiles or bombs

TECHNOLOGY TRENDS (in addition to the technologies available to hobbyist drones):

- Increased range, payload, and endurance
- Releasable missiles or bombs
LARGE MILITARY-SPECIFIC DRONES
VI. LARGE MILITARY-SPECIFIC DRONES

Large military-specific systems represent the next step along the continuum of technological sophistication. In contrast to hobbyist and midsize drones, large military-specific drones require substantial infrastructure to operate and – at this time – are neither accessible to nor affordable for non-state actors and many state militaries, as they cost in the millions of dollars.

Capability Overview

In addition to the capabilities found on midsize commercial and military systems, large military-specific systems have a number of relatively sophisticated features, including increased range, endurance, and payload capacity. For example, General Atomics’ Predator – variants of which are operated by several NATO countries and additionally cleared for export to the United Arab Emirates39 – has an endurance of between 18 and 40 hours,40 while Israel Aerospace Industries’ Heron – flown by over 20 countries – has an endurance of up to 45 hours.41 This level of endurance dramatically increases the persistence of the platform, allowing for greater time on target and improved ISR collection.

Some large military-specific systems, such as Northrop Grumman’s RQ-4 Block 40 Global Hawk, also operate active electronically scanned array radars that deliver higher resolution than that available in baseline systems, as well as integrated sensor suites that synthesize inputs from the system’s radar, cameras, and other sensors. This further improves the system’s ability to conduct air-to-air surveillance and track both individuals of interest and ground vehicles.42 Some large military-specific systems also feature enhanced jamming capabilities that enable broader, beyond-line-of-sight electronic warfare. Indeed, the U.S. Army recently tested the Networked Electronic Warfare Remotely Operated pod, a beyond-line-of-sight communications jammer, on the MQ-1C Gray Eagle.43

Large military-specific systems offer a number of additional improvements in communications capabilities. Many include wide-band satellite communications (SATCOM) that expand the amount and extend the range of transmittable data, providing distant ground stations with real-time ISR. Like some baseline systems, high-end systems are generally capable of line-of-sight communications with other platforms operating in their area and, for this reason, are often employed as communications relays.44 Perhaps the most vivid example of the force-multiplying effects of such capabilities is the EQ-4 – what is essentially an RQ-4 Global Hawk outfitted with the Battlefield Airborne Communications Node (BACN). BACN serves as a universal translator for a diverse set of U.S. aircraft that are not otherwise capable of communicating with each other due to incompatible data links – providing a vital connection between, for example, fourth-generation F-16 fighter jets, B-1 bombers, and stealthy, fifth-generation F-22s.45

Communications relay capabilities will also allow states to operate drones at extended ranges (300 to 800 kilometers) without satellite communications, allowing significant penetration into neighboring countries or contested areas.46
*Actual line-of-sight communications range is dependent upon terrain, atmosphere condition, antenna size, power, and data rate.
Additionally, many military-specific systems have the capacity for a weapons payload. Indeed, 10 countries currently possess armed drones, with at least 20 more openly reported to have active development programs.47 It should be noted, however, that there is a range in the sophistication of armed drones – from Israel’s and the United States’ highly advanced systems to Nigeria’s less-sophisticated Chinese-origin models. For example, General Atomics’ MQ-9 Reaper carries “up to 14 [AGM-114] Hellfire missiles … or various combinations of the GBU-12 Paveway II laser-guided bomb, the AIM-9 Sidewinder, or the GBU-38 JDAM.”48 Systems such as the armed Reapers, currently operated by only the United States and the United Kingdom, thus provide a flexible menu of options for precision-guided air-to-air, anti-personnel, and armor-piercing capabilities that can be delivered at a range of approximately nine kilometers, from altitudes of up to 50,000 feet.49 This range, in turn, increases the difficulty of detection and neutralization from a counter-air perspective, falling outside the range of, for example, many widely operated MANPADS. This stands in contrast to Nigeria’s CH-3, which reportedly carries only two air-to-ground missiles and can reach altitudes of no more than 20,000 feet.50 In addition, while large military-specific drones offer a relatively high level of sophistication, without stealth or electronic attack capabilities they will remain vulnerable to advanced air defenses as well as to enemy fighter aircraft.

Furthermore, the proliferation of armed systems – either through indigenous production or transfer – shows no signs of slowing. Pakistan recently announced that it successfully fired a laser-guided missile from its Burraq UAV.51 And with the State Department’s recent amendment of U.S. export control policy, long-standing requests for armed Reapers by Italy and Turkey will now be reviewed.52 There are additional reports that Australia, already training with armed Reapers,
is interested in purchasing the system as well.\(^{53}\)

While armed drones accounted for just 2.6 percent of all global UAV transfers from 2010 to 2014 (or 11 of 428), the number is steadily increasing—up from 1.5 percent from 2005 to 2009 (5 of 317 systems transferred) and 0 percent from 1985 to 2004 (of 813 systems transferred).\(^{54}\) In the years to come, the number of countries with armed drones can be expected to increase further.

CAPABILITIES:
- Deliver payloads of over 1,000 kilograms at ranges of several hundred to a few thousand kilometers
- Real-time transmission of high-definition images and video at global ranges
- Persist for lengthier periods (up to 24 hours or more)
- Operate in communications-denied environments using fully autonomous GPS and waypoint navigation
- Identify and designate targets via laser range finders and illuminators
- All-weather terrain mapping and target tracking via low-probability-of-intercept radar
- Transmit data via encrypted, high-bandwidth data links
- Enhanced jamming and electronic intelligence-gathering
- Higher resistance to adversary jamming
- Wide-band, beyond-line-of-sight satellite communications
- Releasable missiles or bombs
- Communications relay to enable extended-range (300 to 800 kilometers) operations without relying on SATCOM

LIMITATIONS:
- Vulnerable to countermeasures, including GPS-jamming and spoofing
- Not survivable in contested or denied airspace with advanced enemy air defenses\(^{55}\)
- Vulnerable to enemy fighter aircraft

TECHNOLOGY TRENDS (in addition to the technologies available to hobbyist and midsize military and commercial drones):
- Increased range, payload, and endurance
- Beyond-line-of-sight electronic warfare
- Simple air-to-air capabilities against slow-flying aircraft, such as other drones

Summary
Highly sophisticated military-specific drones, costing in the millions of dollars, currently require substantial training and infrastructure to operate. Because of that, they are neither accessible to nor affordable for non-state actors and many state militaries. Nonetheless, the increasing number of indigenous producers and growing international market suggest that an increasing number of countries will possess armed drones in the next 5 to 10 years.
STEALTH COMBAT DRONES
VII. STEALTH COMBAT DRONES

Stealth combat systems, including ISR and armed UAVs, represent the highest levels of technological sophistication – akin to the most advanced, fifth-generation fighter aircraft. While a number of countries have development programs for such systems, only the United States is known to operate them. Furthermore, due to the sensitivity of stealth combat drones, the United States does not export them and rarely discusses their existence or capabilities in public.

**Capability Overview**

Although many stealth combat systems are classified, defense officials have confirmed the existence of two: Lockheed Martin’s RQ-170 Sentinel and Northrop Grumman’s RQ-180 – short- and medium-range stealthy ISR UAVs, respectively. Both systems are reportedly designed to minimize their radar cross-section via low-observable features such as stealth coatings that absorb the radio waves of adversary radar and shaping measures that minimize radar reflection. Indeed, neither system has the radar-reflective vertical stabilizers found on most manned aircraft; the systems are instead shaped like tailless flying wings with, according to open-source reporting, specially designed inlets and exhaust – features that improve broadband, all-aspect stealth.

Like fifth-generation aircraft, these and other stealth combat drones are also likely to feature low-probability-of-intercept/low-probability-of-detection communications that can transmit data while in stealth mode, as well as an array of passive sensors. This suite of technologies, in turn, enables stealth combat systems to operate in contested and denied environments that contain advanced, integrated air defense systems – a capability not resident in less sophisticated UAVs.

Although no other currently operating, publicly acknowledged drones feature such technologies, reports indicate that BAE Systems’ Taranis and Dassault Aviation’s nEUROn – jointly developed by France, Italy, Sweden, Spain, Greece, and Switzerland – will have similar stealth features when they eventually become operational, as will systems being developed by Russia, Israel, China, and India. Furthermore, while the RQ-170 and RQ-180 are being used for ISR purposes, according to open-source reporting, many international development programs such as the Taranis and nEUROn are intended to produce strike platforms. Similarly, the now-cancelled Defense Advanced Research Projects Agency (DARPA) Joint Unmanned Combat Air System (J-UCAS) – genesis of the X-47B carrier-capable technology demonstrator – included a penetrating strike capability in addition to ISR and electronic warfare capabilities, as do some concepts for the U.S. Navy’s Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) system.

In the years to come, UAVs may feature a number of even more sophisticated technologies. For example, DARPA’s Collaborative Operations in Denied Environment program is designed to enable multivehicle control, both by expanding...
the number of systems that can be supervised by a single operator and by allowing those systems to “collaborate to find, track, identify, and engage targets” in a denied environment. This technology would additionally allow operators to employ swarming tactics to overwhelm adversary defense systems. DARPA is also exploring Distributed Battle Management to ensure coordinated operations, guided by automated decision tools, in a communications-denied environment, as well as High Assurance Cyber Military Systems, a program intended to protect systems from cyber-hacking and hijacking. Similarly, DARPA is exploring high-resolution, GPS-independent positioning, navigation, and timing systems that will allow for continued operations in a GPS-jammed environment. Finally, future stealth combat drones will likely have the ability to conduct autonomous aerial refueling, as demonstrated by the X-47B, further extending their operational reach and enabling deep strikes within an adversary’s territory.

Summary

While the United States is the only country known to operate stealth combat systems, a number of others – including Russia, Israel, China, India, France, Italy, Sweden, Spain, Greece, Switzerland, and the United Kingdom – have active development programs. These systems represent the highest level of technological sophistication and, as such, are tightly controlled by indigenous producers. Furthermore, stealth combat systems feature a number of low-observable characteristics that enable them to operate in environments with advanced integrated air defense systems.
CAPABILITIES:
• Real-time transmission of high-definition images and video at global ranges
• Persist for lengthier periods (between 5 hours and 24 hours, depending on size)
• Operate in communications-denied environments using fully autonomous GPS and waypoint navigation
• Operate in contested and denied airspace with advanced enemy integrated air defense systems as a result of low-observable features
• All-weather terrain mapping and target tracking via low-probability-of-intercept radar
• Enhanced jamming and electronic intelligence-gathering
• Higher resistance to adversary jamming
• Wide-band, beyond-line-of-sight satellite communications
• Transmit data via low-probability-of-intercept/low-probability-of-detection data links
• Releasable missiles and/or bombs

LIMITATIONS:
• Some vulnerability to countermeasures, including GPS-jamming and spoofing

TECHNOLOGY TRENDS (in addition to the technologies available to other drones):
• Increased range, payload, and endurance
• Autonomous aerial refueling
• Air-to-air combat
• Coordinated operations in communications-contested environments
• High-resolution precision GPS-independent navigation systems to allow operations in GPS-denied environments
POTENTIAL FOR OVERMATCH
VIII. POTENTIAL FOR OVERMATCH

While much research to date has focused on military UAVs, hobbyist drones are often less discussed within a security context, though they perhaps hold the greatest potential for achieving overmatch against the United States in the near term. Indeed, hobbyist drones are growing increasingly sophisticated—offering autonomous flight, high-end ISR capabilities, and ever-expanding payload capacity, range, and endurance. They are also widely accessible to potentially disruptive actors and, because drones assembled from component parts generally do not have identifiable markings, could increase the difficulty of attribution if used in an attack. In addition, due to their size, construction material, and flight altitude, hobbyist drones are difficult to defend against if their presence in a particular area is unknown or unexpected. These factors could in turn increase the likelihood that hobbyist drones—particularly those assembled by the operator, and thus not subject to manufacturer-installed geofencing—could be weaponized and autonomously deployed in a terrorist attack against civilians or in an IED-like capacity against patrolling military personnel.

While such systems may not appear sophisticated in a traditional military sense, ground-emplaced IEDs have caused thousands of American deaths in Iraq and Afghanistan and proved profoundly hard to defeat. Drones will enable airborne IEDs that can actively seek out U.S. forces, rather than passively lying in wait. Indeed, low-cost drones may lead to a paradigm shift in ground warfare for the United States, ending more than a half-century of air dominance in which U.S. ground forces have not had to fear attacks from the air. Airborne IEDs could similarly be used in a terrorist attack against civilians or in precision strikes against high-profile individuals or landmarks.

As autonomy and multivehicle control become more mature, it is also possible that an adversary could deploy swarming attacks of inexpensive, expendable drones against U.S. ships and bases. While this approach would produce a large, easily detectable radar cross-section, it would additionally complicate U.S. targeting. In this way, swarms of UAVs could be used to temporarily deny the United States access to airspace within a given area of operations or to overwhelm U.S. air defense systems for ships and bases. These approaches could enable an individual, non-state actor, or state to achieve capability overmatch against the United States.

... low-cost drones may lead to a paradigm shift in ground warfare for the United States, ending more than a half-century of air dominance in which U.S. ground forces have not had to fear attacks from the air.
IX. CONCLUSION

As technology progresses and drone exports and sales continue to rise, highly sophisticated technologies will be available to an ever-growing number of actors. Increasingly, we find ourselves in a world of proliferated drones, in which any interested party can buy and operate an autonomous flying robot, albeit with varying degrees of sophistication.

For a few hundred dollars, anyone will be able to purchase a small hobby drone with the ability to perform aerial surveillance or deliver payloads of a few kilograms at ranges up to a few kilometers. Eventually, however, hobbyist drones will be capable of GPS-independent precision navigation, including indoors. In large numbers, they could be used for saturation swarming attacks against an array of government, military, and civilian targets.

Today, nearly 90 states and non-state actors have access to midsize drones that have greater range, endurance, and payload capacity than their hobbyist counterparts. Increasingly, these systems will be not only armed but also capable of carrying more sophisticated, releasable munitions that will, in turn, enhance their ability to conduct precision attacks. While midsize systems will continue to be vulnerable to small-arms fire and air defenses, the difficulties of defending against their unanticipated use will likely remain for some time to come. Similar to hobbyist drones, large numbers of these systems could be used to attack and overwhelm bases or ships, but at longer ranges and faster speeds, and with larger payloads.

Larger military-specific systems will also continue to proliferate, though their use will be restricted to trained militaries with some degree of standing infrastructure. These systems will provide operators with an additional degree of sophistication in range, endurance, and payload capacity. They will be capable of beyond-line-of-sight communications relay and electronic warfare as well as delivering payloads of over 1,000 kilograms at ranges of thousands of kilometers. Partnered with a secondary drone operating as a line-of-sight communications relay, these drones could reach several hundred kilometers into neighboring territory without the use of satellite communications. These capabilities will enable large military-specific systems to operate and strike deep inside an adversary’s territory. However, without stealth or electronic attack capabilities, they will remain vulnerable to advanced air defenses as well as to enemy fighter aircraft.

Finally, stealth combat drones, currently operated by only the United States, will combine the features of midsize and large military-specific drones with low-observable technologies that will allow them to conduct surveillance and strike missions in contested or denied air environments. In the years to come, a number of other indigenous producers – including Russia, Israel, China, India, France, Italy, Sweden, Spain, Greece, Switzerland, and the United Kingdom – will likely join the United States in operating stealth combat drones.

As drones at all levels of technological sophistication become increasingly available to responsible and disruptive actors alike, it will be vital for the United States to consider the implications of this new strategic landscape and prepare for the challenges of a world of proliferated drones.
As drones at all levels of technological sophistication become increasingly available to responsible and disruptive actors alike, it will be vital for the United States to consider the implications of this new strategic landscape and prepare for the challenges of a world of proliferated drones. Understanding the range of capabilities that actors will have access to not only has implications for military operations and defending against drone attacks but also for policy issues.

For the United States, these include U.S. actions in response to drone incursions or acts of brinkmanship by adversaries using drones, U.S. statements and actions in response to the downing of a U.S. drone, and U.S. export control policies on transfers of U.S.-made drones.

Drone proliferation is happening, and while only a handful of countries will have the ability to operate stealth combat drones, many will have access to armed drones that can penetrate disputed regions or the sovereign territory of other nations. Preventing the proliferation of armed drones is impossible – the drone is here to stay. What this means for international security, however, is an open question. Drones could increase tensions in conflict zones by enabling cross-border attacks or incursions, or they could increase international security by reducing states’ ability to give safe haven to terrorists and other proxies. In crises, drones could create a new step on the escalation ladder, increasing the potential for conflict, or they could potentially defuse crises by increasing transparency on all sides. While the United States cannot stop drone proliferation, it can help influence how drones are used and perceived by others. U.S. statements, targeted transfers of drones to like-minded partners, and above all, U.S. actions will help shape the contours of an increasingly drone-saturated world.
ENDNOTES


2. For the purposes of this paper, the terms “UAV” and “drone” are used interchangeably. Other terms include remotely piloted aircraft (RPA), unmanned aircraft systems (UAS), unmanned aircraft, unmanned combat aerial vehicles (UCAVs), and unmanned combat air systems (UCAS). In other reports, CNAS has frequently used the more precise term “uninhabited” to refer to aircraft that operate under human control, with varying degrees of automation, but do not have a human onboard. For a humorous rundown of the varying terminology, see Joe Trevithick, “Learn to Speak Air Force: A public service announcement regarding drones,” War Is Boring, May 27, 2014, https://medium.com/war-is-boring/learn-to-speak-air-force-e6ebc5614b25.

3. Countries operating armed drones include the United States, United Kingdom, United Arab Emirates, France, Nigeria, South Africa, Iran, Israel, China, and Pakistan. Horowitz and Fuhrmann, “Droning on: Explaining the Proliferation of Unmanned Aerial Vehicles.”


6. It should be noted that this taxonomy is being used for organizational purposes within the discussion. Actual drone capabilities represent a continuum of sophistication, in which the lines both between military and commercial technologies and between the stated categories of systems are increasingly blurred.

7. For more on the history of military drones, see Thomas P. Ehrhard, “Air Force UAVs: The Secret History” (Mitchell Institute for Airpower Studies, July 2010).


12. The DJI Inspire, for example, has a maximum battery life of 18 minutes and a maximum video downlink range of approximately 2 kilometers.


20. Ibid.


30. The U.S. Navy plans to install Kestrel on the MQ-8C Fire Scout, a maritime reconnaissance drone. The software has also been integrated with the ground control systems of a number of small U.S. UAVs, including the MQ-11B Raven. Sydney J. Freedberg Jr., “Teaching Drones How To See: Fire Scout & Kestrel,” BreakingDefense.com, March 13, 2015, http://breakingdefense.com/2015/03/teaching-drones-how-to-see-fire-scout-kestrel/.


36. Dreazen, “The Next Arab-Israeli War Will Be Fought with Drones.”


38. Dreazen, “The Next Arab-Israeli War Will Be Fought with Drones.”


45. This capability has played a prominent role in the United States’ fight against ISIS. Cenciotti, “U.S. Air Force disclosed some details about gigantic Global Hawk unmanned aircraft operations against ISIS.”

46. Range using line-of-sight communications is limited by the curvature of the Earth. Actual maximum range with line-of-sight communications will depend upon the altitude of the aircraft, altitude of the ground control station antenna, terrain or other obstacles between the aircraft and ground control station, atmospheric conditions affecting radio propagation, and the power of the radio signal relative to any other electromagnetic interference or jamming. For an aircraft operating at 23,000 feet, a maximum range of 300 kilometers using line-of-sight radio communications is assumed. If a second UAV is used in a communications relay capacity without satellite communications, operations could extend out to 700 to 800 kilometers. This assumes that the communications relay UAV is operating 200 to 300 kilometers from the ground control station and that both UAVs are operating at 20,000 to 25,000 feet. In this case, the distance between the two UAVs could be greater than 300 kilometers, since they would both be at high altitudes, thus allowing greater visibility over the horizon.

47. Horowitz and Fuhrmann, “Droning on: Explaining the Proliferation of Unmanned Aerial Vehicles.”


52. Shalal and Stephenson, “U.S. establishes policy for exports of armed drones.”


56. While the U.S. Air Force has released limited information about the RQ-170, it has said little about the RQ-180, confirming only that the system will give the United States “better access to contested airspace.” David Axe, “The Air Force JustCopped to Its Secret Stealth Drone,” War Is Boring, June 10, 2014, https://medium.com/war-is-boring/the-air-force-just-copped-to-its-secret-stealth-drone-342453e109f.


72. Scharre, *Robotics on the Battlefield Part II: The Coming Swarm*.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

© 2015 Center for a New American Security. All rights reserved.

Production Notes

**Paper recycling** is reprocessing waste paper fibers back into a usable paper product.

**Soy ink** is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.