Emergence & Convergence

Research Paper No. 1

April 2018

The Age of Commercial Drones: Implications for National Security and Weapons of Mass Destruction

Ken Turner

Ken Turner is a former intern of the Center for the Study of Weapons of Mass Destruction at the National Defense University. Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Defense Department or any other agency of the Federal Government.

In March 2017, an unidentified small unmanned aircraft dropped a Russian ZMG-1 thermite grenade onto the world's largest ammunition depot near Balakleya, Ukraine, setting off a chain reaction that destroyed some seventy thousand tons of munitions and forced 20,000 people to flee the city.[1] Images of this explosion and its resulting damage suggest that unmanned aerial vehicles (UAVs) and more broadly advanced robotics may soon alter the nature of the WMD threat with which national security experts, lawmakers, and policymakers have to contend.[2]

UAVs have substantial potential for malicious use by state and non-state actors, e.g., as delivery platforms for conventional weapons and WMD, or even as weapons themselves. However, at the same time, they offer a nimble and modifiable remote-controlled or autonomous platform for use in countering WMD operations and in support of many other useful applications. Despite the many risks and opportunities for the WMD space related to advanced robotics, policymakers have yet to think holistically in addressing the governance challenges presented by UAVs or leveraging robotics for countering WMD. This paper provides an overview of the current technology for UAVs, an assessment of risks and opportunities, and a discussion of the governance challenges.

Technology Overview

The growth of advanced robotics has exploded in recent years, making it difficult for U.S. policymakers, lawmakers, and national security experts to keep up with the latest trends. Although the field of advanced robotics emerged several decades ago, early development remained sluggish due to the slow commercial maturation of related technologies such as computing power and energy storage. More recent developments in advanced robotics have tracked closely with advances in computing, artificial intelligence, and energy storage, leading to increasingly sophisticated unmanned systems with widespread commercial availability.

Commercialization

Historically, advancements in UAVs have taken place within the context of nation-state military programs. Today, the commercialization of the UAV technology has enabled new drivers of advancement. For example, in December 2013 Amazon unveiled plans for a UAV delivery service that could deliver packages weighing five pounds or less from a distribution center within line of sight less than 30 minutes after an order is placed. While Amazon has begun limited testing in the UK, the company has faced a number of hurdles in attempting to bring the service to fruition, including UAV regulations and the limitations of the technology itself. As Amazon works to make the UAV delivery service economically viable, the company is developing and patenting new innovations it believes will help make its delivery service a reality. As the wide range of commercial and industrial applications increases over the next several years, the UAV industry will likely see technological leaps forward in battery life, flight distance and time, and payload capacity, out of economic considerations rather than military ones.

Sources:

CBS, "Amazon unveils futuristic plan: Delivery by drone," CBS News, December 1, 2013, available at < https://www.cbsnews.com/news/amazon-unveils-futuristic-plan-delivery-by-drone/>.

Nathaniel Scharping, "Amazon Has Patented Some Wild Drone Technologies," *Discover Magazine,* December 29, 2016, available at < http://blogs.discovermagazine.com/d-brief/2016/12/29/amazon-drone-patents-motherships/#.WeEKmclUkS8>.

Among these unmanned systems, unmanned aerial vehicles (UAVs) or drones present the most immediate challenge. While there are other unmanned systems besides UAVs, such as unmanned ground, underwater, and surface vehicles that could pose national security threats, the development and commercialization of these other systems have proceeded more slowly than UAVs.[3] Though not as relevant in the near-term, policymakers should pay attention to advancements in the development of these other systems, which may serve to further enhance CWMD efforts across multiple operating domains.

To address the most pressing challenge at hand, this paper will focus primarily on commercially-available UAVs. Commercially-available UAVs are broadly-divided into two groups: consumer-grade and commercial-grade drones. Consumer-grade UAVs are small unmanned systems that are readily available off-the-shelf for purchase by any individual, cost no more than a few thousand dollars, and require little to no formal training to operate. Standard models come with a wide range of capabilities including GPS and waypoint navigation systems, autonomous flight capabilities, smartphone-based controls, high-definition cameras, and some advanced sensing capabilities.

Commercial-grade UAVs are systems a step above and not readily available for purchase by the average individual. Not only do commercial-grade UAVs cost significantly more than consumer-grade models, they require some level of training to operate and often involve more complex infrastructure on the ground.[4] Commercial-grade UAVs generally run larger in size and have greater capabilities than consumer systems, but this distinction is becoming increasingly blurred as relevant technologies mature. To contrast, advanced military-grade UAVs are primarily within the domain of the militaries of advanced nation-states, require substantial investments of capital, industry, infrastructure, and training to operate, and are thus inaccessible to most actors.

The development of the commercial market for consumer and commercial-grade UAVs has emerged alongside of the diffusion of relevant technologies originally developed to support the use of unmanned systems by the U.S. military. The commercial market has grown substantially both domestically and internationally within the last several years, benefiting from many years of experience with military systems. Affordability, off-the-shelf availability, and low barriers to entry have generated a diverse commercial market for UAVs with a growing number of platforms available for potential misuse by state and non-state actors.

In 2014, UAV sales in the United States reached $84 million and 250,000 units sold.[5] By 2016, the market ballooned to nearly $481 million and roughly 2.5 million units sold.[6] The Federal Aviation Administration (FAA) estimates domestic sales could reach nearly 7 million units by 2020, with the industry experiencing a compounding annual growth rate of about 68% each year.[7] This exponential growth is being driven by falling unit prices, improved features such as cameras, batteries, and navigation software, and greater overall ease of use.[8] At the same time, the commercial-grade UAV market is expected to expand significantly in response to demand across diverse industries such as aerial photography, agriculture, emergency management, real estate, insurance, and construction, industrial, and utility inspections.[9] These statistics do not even capture the large number of UAVs sold on the international market for which there is little verifiable data and few agencies reporting data similar to the FAA. For example, China is one of the largest manufacturers of consumer-grade UAVs in the world, claiming over 400 different manufacturers with over $413 million in exports in 2015 alone.[10] Some experts estimate that by 2026 the global UAV market could constitute a $90 billion industry.[11]

Consumer and commercial-grade UAVs with increasingly advanced capabilities continue to become more accessible. These commercially-available UAVs remain constrained by the capacity of the system's battery, which restricts the range, flight time, and payload. Depending on the size of the UAV, the payload could potentially range from a few ounces (small-handheld UAV), to a few pounds (average consumer UAV), to several dozen pounds (large agricultural UAV). Likewise, the range and flight time of the UAV averages from a few minutes, covering only a few hundred feet, to several hours, reaching distances of dozens of miles. Trade-offs exist between range/flight time and payload, with one often inversely affecting the other. Though many of these systems remain limited when compared with the UAVs of most nation-state military programs, their onboard computing and navigation systems, physical capabilities, and overall quality of the equipment continue to improve.

Today's commercially-available UAVs are light years ahead technologically of many unmanned systems from only a decade ago. While much of the promise of advanced robotics remains unfulfilled, this emerging technology could experience near-term leaps forward as a result of advances in computing and energy storage. Onboard computing and navigation systems of consumer and commercial-grade UAVs are becoming more sophisticated through advances in artificial intelligence, though limitations in areas such as autonomy persist. As the field of advanced robotics continues to develop and mature, increasingly complex UAVs will be within reach of a wide range of non-state actors, both in the United States and abroad.

The Risks

While the U.S. military has largely maintained unchallenged airspace dominance in conflict zones over the last decade, the development and/or procurement of increasingly advanced UAVs by both state and non-state actors threatens to erode that asymmetric advantage. Although consumer and commercial-grade UAVs have limited payloads and ranges, they can still be used in inventive ways to cause disproportionate and even catastrophic effects.

Commercially-available UAVs circumvent several of the large initial barriers of entry to aerial delivery, such as acquisition cost, training, and support facilities needed to operate traditional aircraft. Though typically far smaller than traditional aircraft, the size, agility and relative stealth of these UAVs enable them access to smaller and more protected areas. Both consumer and commercial-grade UAVs can overcome or slip through many of the aircraft countermeasures that have protected the airspace for years. These drones are too small and fly too low to be detected by ordinary radar.

By providing easy access to targets in ways previously considered unfeasible, commercial and consumer-grade UAVs present a number of new risks. Below are highlighted four potential risks that these UAVs pose to the security of the United States.

The first, and perhaps the most traditional, risk is the use of UAVs as delivery platforms for WMD. The threat posed by state or non-state actor use of consumer or commercial-grade UAVs represents a more immediate threat for the WMD space than advanced military-grade UAV programs. While traditional aircraft would provide a better platform for spreading large amounts of agent over as wide an area as possible, UAVs could be utilized to deliver smaller payloads.

While we are unlikely to witness a small UAV carrying a nuclear weapon in the near-term due to payload constraints and other obstacles to acquiring a device, UAVs carrying a payload of biological, chemical, or radiological weapons are not beyond the pale of consideration. Use of WMD by non-state actors, such as Aum Shinrikyo's 1995 Tokyo subway sarin attack and the 2001 Amerithrax attacks, utilized small amounts of the agents to cause considerable casualties and massive effects. The Tokyo sarin attack caused 12 deaths and hundreds of injuries, while the Amerithrax attacks resulted in five deaths and cost the government several hundred million dollars to cleanup.

There already is cause to worry about UAVs delivering biological, chemical, or radiological payloads. In April 2015, a Japanese man landed a UAV carrying radioactive sand on the roof of the Japanese Prime Minister's residence, in protest of the government's handling of the Fukushima Daiichi nuclear disaster.[12] The Islamic State has both a chemical weapons and UAV capability. It has used chemical agents in at least 52 attacks in Iraq and Syria.[13] Islamic State also has utilized

Non-State Actors

Traditionally airpower has been considered a capability afforded to the militaries of nation-states; however, UAVs present non-state actors with access to a de-facto air capability. Several non-state actor groups in the Middle East and South and Central America have experimented with UAVs over the last couple of years, yet few groups have been as prolific or successful in adapting consumer and commercial-grade UAVs to the battlefield as the Islamic State. At one point U.S. military forces in Iraq documented over 100 UAV operations by Islamic State forces within a 60-day timeframe and even recovered documents that indicated the group sought to standardize UAV operations. The Islamic State utilized commercially-available UAVs as ISR platforms, rigged them to drop grenades and mortars on troops, laden them with explosives and kamikazed them into buildings, and booby-trapped UAVs to explode when attempting to access the internals of the system. At the same time, the Islamic State promulgated these techniques on social media and the internet to demonstrate the effectiveness of these systems and spread the knowledge of their experiments to a larger audience. This spread of accrued knowledge, coupled with the ease of access to commercially-available UAVs, may embolden non-state actors to imitate utilizing the systems on soft targets far away from the battlefield.

Sources:

Mark Pomerleau, "How the Military is Defeating Drones,"C4ISRNET, March 21, 2017, available at < https://www.c4isrnet.com/unmanned/uas/2017/03/21/how-the-military-is-defeating-drones/>.

Ben Watson, "The Drones of ISIS," Defense One, January 12, 2017, available at < https://www.c4isrnet.com/unmanned/uas/2017/03/21/how-the-military-is-defeating-drones/>.

an increasingly capable UAV program for both reconnaissance and to deliver small explosive payloads.[14] It would not be unrealistic to consider that they have at least contemplated bringing the two capabilities together. Loading a single commercially-available UAV with sufficient quantities of a WMD in order to cause a massive number of injuries and deaths would be difficult. However, the use of multiple UAVs laden with small amounts of chemical, biological or radiological agents against crowded spaces or important targets could still cause significant casualties or effects.

The second risk is the use of UAVs to target critical infrastructure or industry, thereby creating WMD-like effects. A UAV does not need to be strapped with any cargo to cause substantial damage to a target; it could simply crash into it and render the target inoperable. However, a UAV laden with even a small amount of explosive could be used with significantly greater effect.

Non-state actors have already been experimenting with the use of UAVs to threaten critical infrastructure. Between October and November 2014, there were 14 unattributed illegal UAV flights over nuclear plants across France, which were considered by French authorities to be an act of "organized provocation."[15] In August 2016, a Swiss citizen flew an UAV inside the cooling tower of a nuclear plant in protest of lax security measures.[16] Hezbollah has used Iranian-made UAVs armed with explosives in both its 2006 and 2012 wars with Israel and has repeatedly attempted to probe Israel's Dimona nuclear complex with UAVs over the last several years.[17] These fly-bys should be taken seriously. Historically, small ignitors have quickly led to disproportionately large destruction and numerous casualties in some of the most famous industrial disasters. The 2015 Tianjin explosions that killed 173 and injured nearly 800 were caused by the ignition of stored chemicals and were powerful enough to register as magnitude 2.3 and 2.9 earthquakes.[18] India's 1984 Bhopal disaster, which killed thousands through the accidental release of toxic chemicals into the atmosphere, suggests the damage that could result if an explosive-laden UAV penetrated a major chemical storage facility.

A coordinated UAV attack could create similar or even greater levels of casualties and destruction depending on the chosen target. While the aforementioned attack on the Ukrainian arms depot in Balakleya garnered international attention for the sheer level of destruction, it was far from the first such incident. Since October 2015 there have been at least a half-dozen unattributed attacks by UAVs armed with grenades against Ukrainian weapons depots and ammunition storage facilities.[19] While these attacks have thus far only caused limited casualties, the chain reactions of explosions and fires they set off have caused more than $1 billion in damage.[20] UAVs armed with even small amounts of explosive allow the capability to 'bring the detonator,'[21] so to speak, to targets where the larger 'explosive' is already present, with very little difficulty and with comparatively large effects.[22]

The third risk, following on the concept of using UAVs to 'bring the detonator,' involves the use of unmodified or explosive-laden UAVs to target other aerial assets. A UAV could be used to crash into or detonate upon another aircraft in order to damage or bring down the aircraft during the ascent/descent phases or to cripple them on the ground. The aviation industry considers the threat from UAV collisions, colloquially referred to as "metal geese from hell," against aircraft a major and serious concern.[23]

In the United States, the FAA reported 'UAV sightings' near aircraft or facilities and 'proximity dangers' when a UAV comes within 500 feet of an aircraft. Between February and September 2016, there were more than 1,200 such UAV sightings, up from over 800 in 2015 and nearly 300 in 2014.[24] Additionally, between December 2013 and September 2015, the FAA identified over 300 proximity danger incidents reported, of which nearly 30 forced the aircraft to maneuver to avoid impending collision with a UAV.[25] In September 2017 a small UAV accidentally collided with a U.S Army Black Hawk helicopter operating over New York's Staten Island, causing damage to the main rotor blade and forcing the helicopter to land at a nearby civilian airport.[26] The danger of UAVs colliding with commercial or military aircraft in flight is a pervasive concern, even without having to factor in the possibility of explosives.

A recent example demonstrates the potential for malicious use of UAVs to threaten aircraft. In September 2012, Taliban forces raided Camp Bastion in Afghanistan's Helmand province, targeting and damaging or destroying eight U.S. Marine Corps' AV-8B Harriers on the ground. [27] Armed with guns, rudimentary explosives, and RPGs, 15 Taliban fighters caused more than $200 million in damage and the single largest loss of U.S. aircraft since the Vietnam War.[28] Weaponized UAVs could provide a cheap and readily available platform to strike expensive or populated aircraft when they are vulnerable and cause disproportionate damage for relatively low cost.

Open Hardware
One of the important challenges of unmanned systems is the relative openness of the technology's hardware and software and its convergence with other emerging technologies. Not dissimilar to the tinkerers of the early years of automobile production in the 1910s-1930s, hobbyists today are encouraged by the 'drone community' and industry to modify and augment their UAVs with hardware and software upgrades tailored to meet their own unique requirements. The convergence of UAVs with additive manufacturing further enables hobbyists to download and print their own custom UAV parts or entire UAVs. Printed in a relatively short amount of time using off-the-shelf materials, these UAVs offer a wider range of capabilities at a fraction of the cost than most commercially-available systems. The open-source nature of many of the software experiments in autonomy, guidance, and navigation, can be expected to increase the general level of the systems capabilities in the future. The spread of this knowledge through the open-source domain will likely enable bad actors to acquire increasingly advanced or custom capabilities without needing to attain the expertise themselves, further enhancing their capabilities beyond the acquisition of new systems and beyond the control of potential governance measures aimed at the manufacturing or sale of UAVs.

The fourth risk consists of converting UAVs into flying improvised explosive devices (IEDs) to threaten soft or high-value targets. For a variety of reasons, non-state actors gravitate toward low-tech means to incite terror, and the use of consumer-grade UAVs appears to be a natural evolution in terrorist tactics. The ground-emplaced IEDs that dogged coalition forces in Iraq and Afghanistan and the pressure cooker bombs used in the 2013 Boston Marathon Bombing, were passive systems that relied on optimal placement and timing to achieve maximum effect. However, weaponized UAVs would create the capability to actively hunt a soft or high-value target, choosing the proper place and time to strike, and at minimal risk to themselves. The number of UAVs used could be scaled to achieve a mass effect. Properly delivered, even a limited payload of a few kilograms of explosive distributed among multiple systems could cause significant casualties.

A range of non-state actor groups have experimented with using weaponized UAVs with a certain level of success, including Hezbollah, Hamas, Jabhat al-Nusra, and the Islamic State.[29] Between 2011 and 2015, no fewer than six potential terrorist attacks utilizing explosive armed UAVs were foiled in the U.S., Germany, Spain, and Egypt.[30]

UAVs may also offer terrorists an agile tool for assassination. In September 2013, a political rally in Germany was interrupted when a small UAV crash-landed in protest next to a group of

German statesmen that included German Chancellor Angela Merkel and Defense Minister Thomas de Maiziere.[31] While Chancellor Merkel reportedly laughed off the interruption, her security detail likely did not; even a small amount of explosive could have been used to maim or kill two members of Germany's leadership.

The thread connecting the four risks highlighted above is the potential use of consumer or commercial-grade UAVs to provide state and non-state actors access to an expanding range of targets, allowing them to threaten a variety of targets, some of which might otherwise have been considered inaccessible to all but the most dedicated and capable of adversaries.

The accessibility and ease of use of many consumer and commercial-grade UAV systems allow novices to be able to purchase and fly a UAV with very little training, while advances in onboard computing are increasingly allowing the operator to turn over control of many advanced functions to the UAV itself.

Recent developments in autonomy, human-machine teaming, and swarming are allowing individual actors the ability control more than one UAV at a time by automating many basic functions and coordinating them to work together to perform increasingly complex tasks. While these developments could be considered cutting edge at the moment, it may not be long before an individual is capable of controlling multiple UAVs simultaneously, greatly increasing the destructive capacity and capability of lone actors. As the technology matures, so too does the potential that it may be used in increasingly inventive ways against the United States, including to create WMD effects.

The Opportunities

Though the near-term WMD threat space is largely dominated by consumer and commercial-grade UAVs, the unmanned systems available to the U.S. government offer several platforms that perform a variety of dangerous tasks to support the CWMD mission. Unmanned systems can perform intelligence, surveillance, and reconnaissance (ISR) duties, detection, decontamination, and other CWMD operational tasks, offer some tangible benefits over other means or platforms, and reduce risks to warfighters and first-responders. The affordability, off-the-shelf availability, and ease of use of many consumer and commercial-grade UAVs could make them attractive platforms for some CWMD missions.

It should come as no surprise that UAVs and other unmanned systems are especially useful in performing ISR duties, yet the benefits of their use to perform that role in a CBRN environment cannot be underscored enough. Relatively cheap, expendable, and readily available, small UAVs can be utilized for ISR in potentially or known contaminated environments, where recovery of the system might be considered undesirable or unfeasible.

In the aftermath of the Fukushima Daichii nuclear disaster, the Tokyo Electric Power Company (TEPCO) used UAVs to inspect the inside of their highly radioactive reactor site without placing humans at risk.[32] Additionally, first responders have used UAVs to search remote or dangerous areas and structures during natural disasters, in order to rapidly target rescue, relief, and aid efforts. Converging with additive manufacturing, the U.S military has experimented with 3D printers to print custom UAVs or modify existing ones to meet the requirements of a contaminated mission space as the situation evolves over time. By deploying UAVs into contaminated environments, personnel can orientate themselves towards performing more specialized tasks where human labor or input is necessary.

Unmanned systems are ideal tools for the detection of CBRN materials. Unmanned systems equipped with lightweight detection and collection equipment can assess the presence of CBRN materials in the air, on the ground, or on the surface of water. These UAVs provide a rapidly deployable CBRN detection capability that could be used to actively track and collect suspected CBRN materials in hostile or inaccessible areas and analyze them inflight and/or return them to a lab for analysis. For example, dispatching multiple unmanned systems with detection capability to perform route and area reconnaissance duties in a suspected CBRN environment would allow active collection of more consistent and accurate data. This would reduce the need for warfighters to suffer degraded performance in full CBRN protective gear while operating in areas of suspected but unconfirmed contamination. The Defense Threat Reduction Agency, Edgewood Chemical Biological Center, and the Army are developing this capability, through systems like the WMD Aerial Collection System.[33]

Advances in nanomaterials and additive manufacturing may further improve upon this capability by embedding detection systems directly into the unmanned system itself. Capable of operating independent of ground conditions, these unmanned systems could perform vital CBRN detection duties without placing the warfighter or first-responder at risk.

Unmanned systems also can be used to reduce risk, time, and effort related to decontamination. The process of decontamination is often dangerous, dirty, and exhausting work that can take significant time and manpower; unmanned systems, could significantly reduce the burden. A human-machine teamed system could employ an unmanned system to perform the majority of the decontamination work, with humans focused on quality control. Such a system would allow combat and logistics assets to be restored back to battlefield readiness with significantly less effort. Unmanned systems would also be prime candidates for area and terrain decontamination efforts of critical infrastructure such as airfields, ports, and supply depots where tying up a large amount of time and manpower may not be practical. The medical sector plans to leverage automated unmanned systems with detection, decontamination, and disinfecting capabilities to clean hospitals, labs, and emergency vehicles in the event of exposure to virulent pathogens.[34] TEPCO has used unique and advanced unmanned systems in the decontamination and clean-up process of their Fukushima Daichii reactor site.[35] They have also used UAVs that can survey building interiors, collect particle samples, and recharge their own batteries, all autonomously.[36] Further development of these capabilities could prove immensely beneficial to the safety of the warfighter and the rapid renewal of combat power in theater.

Unmanned systems may also present additional opportunities to perform other CWMD operational tasks beyond what has already been considered. Reducing incentives, increasing barriers, managing risks, and denying the effects from WMD are all areas that could benefit to some degree from the utilization of unmanned systems. Monitoring and verification of suspected or known WMD facilities, disrupting and defeating WMD through neutralization, safeguarding WMD or materials of concern, and defensive capabilities against WMD use are but a few other areas of opportunity for further consideration.

Governance Challenges

Within the last several years, the development, maturation, commercialization, and proliferation of unmanned systems has increased substantially, yet the governance of these systems has lagged behind significantly. While the challenges associated with the proliferation of consumer and commercial-grade UAVs worldwide are a global issue demanding international attention, overcoming domestic governance challenges in the United States should serve as a first step to inform later international governance efforts.

In the United States, the FAA has assumed the lead role in establishing the rules and regulations governing the use of UAVs. FAA regulations, such as the Small UAS Rule and the Special Rule for Model Aircraft, are intended to set limitations on the use of UAVs in the national airspace system. Until recently the FAA required a one-time registration with an FAA database for all hobbyist UAV users, which then allowed their registration to apply to multiple UAVs.

The sheer volume of systems and users, coupled with their expected growth over the next several years, complicates the governance challenge. By 31 December 2016, over 626,000 hobbyist users had registered their UAVs online, yet the FAA estimated there were over 1.1 million hobbyist users in the United States alone.[37] Additionally, over 440,000 commercial-grade UAVs had also been registered, with more than 29,000 Remote Pilots Certificates having been issued by the FAA to operators within the United States.[38] Although a lawsuit brought in May 2017 successfully challenged the FAA's authority requiring users to register their small UAVs, Congress later restored the FAA's rules in December 2017 as part of the National Defense Authorization Act for Fiscal Year 2018.[39]

The FAA lacks the authority and more importantly the resources to enforce its regulations across the country, but instead relies upon law enforcement to pursue violations. The FAA has identified hundreds of No Drone Zones, i.e., areas in which UAV flight is severely restricted or illegal, which must be monitored and enforced by state and local law enforcement. As the number of UAVs and users continues to balloon, federal, state, and local law enforcement officers will require additional training, equipment, and capacity in order to deal with the potential threat.

Adding further complications, there are also 133 state and local UAV-specific ordinances and regulations that restrict areas where UAVs may be operated (public vs private property) and determine the ways that UAVs may be used (surveillance, privacy, and improper operation). [40] Yet many of these ordinances directly conflict with aspects of federal regulations.[41]

Countermeasures

The use of weaponized UAVs presents an interesting challenge for security and operational planning, which has often relied on deterring and preventing access to a target through a series of barriers that combat the human element of a threat. Many of the traditional security measures established to deal with airborne threats can be circumvented by UAVs, primarily due to the small size of many consumer-grade UAVs being difficult to detect and defeat, especially if their presence in an area is unexpected. As the UAV threat to U.S. military forces fighting the Islamic State increased, the DoD and the individual services tested more than 20 different counter-UAV systems and sought to reallocate some $20 million in funding to help fill the immediate gap. A motley range of active and passive countermeasures emerged, such as small arms, missiles, directed-energy systems, net guns, trained birds of prey, hunter UAVs, radio frequency jammers, and GPS spoofers, which have been marketed by companies attempting to offer an answer to the growing problem. Unfortunately there is currently no one-size-fits-all solution and complete protection against the range of potential UAV threats is not feasible, even with an array of different and sometimes costly systems attempting to protect a target against a relatively cheap, evolving threat.

Unfortunately, many of these existing governance measures are already being undermined. The rules and regulations pertaining to UAVs are largely arbitrary restrictions and imposed without any meaningful mechanism for enforcement beyond law enforcement prosecution. The efficacy of the rules largely depends on the willingness of good actors to comply with the rules and treat any infringing UAVs as potential bad actors. Many of the countermeasures currently in use are intended to prevent or defeat the use of UAVs by countering their guidance or control systems. Yet as UAVs become increasingly less reliant on GPS guidance and are instead aided by autonomy and visual or inertial guidance systems, the effectiveness of these countermeasures will decrease sharply.

Many of the efforts undertaken by manufacturers to keep UAVs in compliance with federal regulations, such as geofencing coded into a UAV's software, can be subverted by reprogramming the system to remove these restrictions.[42] For as low as $200 a Russian company will sell operators of DJI-manufactured UAVs a software or hardware modification that bypasses the safety features that prevent operators from flying in No Drone Zones.[43] Yet hobbyists do not necessarily have to buy their way around the safety restrictions, as tips and tricks from fellow hobbyists that teach how to bypass safety features for some UAV models are readily available for free on internet forums. As the number of governance measures grows, so too will a market that services those operators who want to subvert restrictions placed by manufacturers.

The U.S. currently lacks a whole-of-government approach to address the challenge that UAVs present, and as the skies become increasingly crowded the problem will only become more difficult to manage. Yet as both the hardware and software of UAVs continues to evolve, it may prove progressively more difficult to place or enforce restrictions that target the system by itself. Going forward, the U.S. may have to devote greater effort towards governance that targets the user alongside the system.

Conclusion

Advanced robotics offers a powerful, and often cheap, platform for state and non-state actors to engage and threaten the United States in the WMD space. At the same time, advanced robotics also offers the U.S. opportunities to help confront, manage, and defend against a broad range of WMD threats. As an emerging technology, the field of advanced robotics poses a governance challenge through its ability to make aerial capability available to a large number of new pilots, for which there are few current mechanisms able to properly manage them. While the national security community tends to focus on the risks posed by emerging technologies, the mindset for approaching advanced robotics should expand to include consideration of the significant benefits that this technology can bring to the CWMD mission and leveraging those to the greatest extent possible.

About the Author

Mr. Kenneth B. Turner is a defense contractor. Mr. Turner has previously worked with the Center for the Study of Weapons of Mass Destruction at the National Defense University, the U.S. House of Representatives, and a foreign policy think tank. Mr. Turner holds a Master's Degree in Defense and Strategic Studies from Missouri State University, where he completed a graduate thesis comparing the international effort to control lethal autonomous weapons systems with previous efforts at international arms control, and a Bachelor's Degree in History from Mississippi State University. Mr. Turner has published several pieces on WMD issues and unmanned systems, including with the Bulletin of the Atomic Scientists, Missouri State University, and the NDU Press. The author is indebted to the following individuals for their reviews and insightful comments on earlier drafts of this paper: Natasha Bajema, John Caves, Seth Carus, and T.X. Hammes.

Emergence & Convergence Study

In its multi-year study entitled *Emergence and Convergence (E&C)*, the WMD Center is exploring the risks, opportunities, and governance challenges for countering WMD introduced by a diverse range of emerging technologies. Toward this end, the WMD Center has developed an exploratory framework for first identifying the emerging technologies that will have greatest impact on the WMD space for state and non-state actors and then for evaluating the nature of that impact on the current tools and approaches for countering WMD. The E&C research paper series will explore specific topics highlighting the impact of additive manufacturing, advanced robotics, nanotechnology, and synthetic biology on the WMD space as well as potential governance challenges and solutions.

Dr. Natasha E. Bajema, Senior Research Fellow is the principal investigator for the Emergence & Convergence study, which is supported by several offices within the Office of Secretary of Defense (OSD) and receives its primary funding from the CWMD Systems Program Office within the Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs/Threat Reduction and Arms Control (NCB/TRAC/CWMD Systems). The support by Mr. Jim Stokes, Director, CWMD Systems Program, has been critical to the project's success.

[1] David Hambling, "Russian Drones Attack With Grenade Weapons," *Warrior Scout,* July 18, 2017, available at <http://scout.com/military/warrior/Article/Small-Russian-Drones-Do-Massive-Damage-WIth-Grenade-Weapons-103103172>.

[2] The Department of Defense uses less well-known terminology to describe UAVs including unmanned aircraft and unmanned aircraft system. An unmanned aircraft (UA) is defined as "an aircraft that does not carry a human operator and is capable of flight with or without human remote control. An unmanned aircraft system (UAS) is defined as "that system whose components include the necessary equipment, network, and personnel to control and unmanned aircraft. See the DoD Dictionary of Military and Associated Terms, March 2018, Available at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-03-27-153248-110

[3] Due to slower development and more limited commercialization than UAVs, the cost and accessibility of other unmanned systems has largely limited their use to advanced nation-states, industry, and research. Barring a sudden acceleration, it is unlikely these other systems will reach similar levels of proliferation within the same timeframe.

[4] As commercial- grade systems develop and mature, they are likely to become more accessible, lower in cost, and require increasingly less training to operate, potentially being able to launch, operate, and recover autonomously to meet the needs of industry and businesses.

[5] Larry Downes, "America Can't lead the World in Innovation if the FAA Keeps Dragging Its Feet on Drone Rules," *Washington Post*, October 8, 2014, available at <https://www.washingtonpost.com/news/innovations/wp/2014/10/08/america-cant-lead-the-world-in-innovation-if-the-faa-keeps-dragging-its-feet-on-drone-rules/>.

[6] Greg Sandoval, "Sales of Commercial Drones Will Soar 84% in 2016 — Despite Safety Concerns," *Geek Wire*, January 18, 2016, available at <http://www.geekwire.com/2016/sales-of-commercially-used-drones-will-soar-84-in-2016-despite-safety-concerns/>.

[7] Federal Aviation Administration, "FAA Aerospace Forecasts FY 2017-2037: Unmanned Aircraft Systems," *Federal Aviation Administration*, March 21, 2017, available at <https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2017-37_FAA_Aerospace_Forecast.pdf>.

[8] Federal Aviation Administration, "FAA Aerospace Forecasts FY 2017-2037: Unmanned Aircraft Systems."

[9] Ibid.

[10] Miriam McNabb, "Will China Dominate the Drone Market," *DroneLife*, January 14, 2016, available at <http://dronelife.com/2016/01/14/will-china-dominate-the-drone-market/>.

[11] Craig Smith, "10 Interesting Drone Statistics," *DMR*, February 6, 2016, available at <http://expandedramblings.com/index.php/drone-statistics/>.

[12] BBC, "Japan radioactive drone: Tokyo police arrest man," *BBC*, April 25, 2015, available at <http://www.bbc.com/news/world-asia-32465624>.

[13] Eric Schmitt, "ISIS Used Chemical Arms at Least 52 Times in Syria and Iraq, Report Says," *New York Times,* November 21, 2016, available at <https://www.nytimes.com/2016/11/21/world/middleeast/isis-chemical-weapons-syria-iraq-mosul.html?_r=0>.

[14] Joby Warrick, "Use of weaponized drones by ISIS spurs terrorism fears," *Washington Post,* February 21, 2017, available at <https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?utm_term=.81e21bf4efd1>.

[15] Dan Bilefsky, "France Arrests 3 With Drones by Power Plant," *New York Times,* November 6, 2014, available at <https://www.nytimes.com/2014/11/07/world/europe/3-found-with-drones-near-nuclear-plant-are-questioned-in-france.html?_r=0>.

[16] SmartDrone, "Terror Fears Grow As Drone Flies Over Nuclear Power Plant," *SmartDrone,* August 13, 2016, available at <http://www.smartdrone.com/terror-fears-grow-as-drone-flies-over-nuclear-power-plant.html>.

[17] Milton Hoenig, "Hezbollah and the Use of Drones as a Weapon of Terrorism," *Federation of American Scientists,* June 5, 2014, available at <http://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/>.

[18] Heather Chenn, "China explosions: Tianjin blasts on seismic scale," *BBC,* August 13, 2015, available at <http://www.bbc.com/news/world-asia-china-33901206>.

[19] Kyle Mizokami, "Kaboom! Russian Drone With Thermite Grenade Blows Up a Billion Dollars of Ukrainian Ammo," *Popular Mechanics,* July 27, 2017, available at < http://www.popularmechanics.com/military/weapons/news/a27511/russia-drone-thermite-grenade-ukraine-ammo/>.

[20] Ibid.

[21] The prospect that UAVs armed with explosives could be used to produce larger event by "bringing the detonator," is a concept that has been put forward by National Defense University's Dr. T.X. Hammes.

[22] T.X. Hammes, "Cheap Technology Will Challenge U.S. Tactical Dominance," *NDU Press,* March 29, 2016, available at <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/702039/cheap-technology-will-challenge-us-tactical-dominance/>.

[23] David Hambling, "What Really Happens When a Drone Strikes an Airplane," *Popular Mechanics,* available at <http://www.popularmechanics.com/flight/drones/a24467/drone-plane-collision/>.

[24] April Glaser, "U.S. airplane pilots are reporting more drone sightings, but no collisions yet," *Recode,* February 23, 2017, available at <https://www.recode.net/2017/2/23/14717964/pilots-faa-drones-airplane-regulation-flying-accidents-collisions>.

[25] Brakkton Booker, "New Drone Study Finds 327 'Close Encounters' With Manned Aircraft," *NPR,* December 11, 2015, available at <http://www.npr.org/sections/thetwo-way/2015/12/11/459366656/new-drone-study-finds-327-close-encounters-with-manned-aircraft>.

[26] Associated Press, "Feds Are Investigating a Crash Involving Drone, Army Helicopter," *Popular Mechanics,* October 8, 2017, available at <http://www.popularmechanics.com/flight/drones/a28551/drone-black-hawk/>.

[27] Alissa Rubin, "Audacious Raid on NATO Base Shows Taliban's Reach," *New York Times,* September 16, 2012, available at <http://www.nytimes.com/2012/09/17/world/asia/green-on-blue-attacks-in-afghanistan-continue.html?pagewanted=all&_moc.semityn.www>.

[28] Ibid.

[29] Don Rassler, "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology," *Combating Terrorism Center at West Point,* October 2016, available at <https://www.ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf>.

[30] Jack Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," *The Wall Street Journal,* January 28, 2015, available at <https://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268>.

[31] Friederike Heine, "Merkel Buzzed by Mini-Drone at Campaign Event," *Der Spiegel,* September 16, 2013, available at <http://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html>.

[32] Matt Smith, "Flying drone peers into Japan's damaged reactors," *CNN,* April 10, 2011, available at <http://www.cnn.com/2011/WORLD/asiapcf/04/10/japan.nuclear.reactors/>.

[33] Cubic, "WMD Aerial Collection System (WACS)," accessed April 26, 2017, available at <http://globalsecurity.cubic.com/?q=node/43>.

[34] Lisa Thomas-Laury, "Local Company Builds Robot to Disinfect Areas Exposed to Ebola," *ABC,* October 22, 2014, available at <http://6abc.com/health/robots-used-to-disinfect-ebola-areas/361817/>.

[35] Rachel Gross, "Decontamination Bots Are Dying on Our Behalf in Fukushima," *Slate,* March 10, 2016, available at <http://www.slate.com/blogs/the_slatest/2016/03/10/these_fukushima_decontamination_bots_are_dying_trying.html>.

[36] BBC, "Japan: Autonomous drone developed for Fukushima reactors," *BBC,* June 11, 2015, available at <http://www.bbc.com/news/blogs-news-from-elsewhere-33096077>.

[37] Federal Aviation Administration, "FAA Aerospace Forecasts FY 2017-2037: Unmanned Aircraft Systems."

[38] Ibid.

[39] April Glaser, "Americans no longer have to register non-commercial drones with the FAA," *Recode,* May 19, 2017, available at <https://www.recode.net/2017/5/19/15663436/us-drone-registration-rules-faa>.

[40] Arthur Holland Michel, "Local and State Drone Laws," *Center for the Study of the Drone at Bard College,* March 2017, available at <http://dronecenter.bard.edu/files/2017/03/CSD-Local-and-State-Drone-Laws-1.pdf>.

[41] Ibid.

[42] Geofencing creates a dynamic or established virtual perimeter for a real-world geographic area, which can be utilized to alert or override the commands of a UAV operator when they enter restricted airspace.

[43] Ryan Whitwam, "Russian Company Is Selling Mods to Bypass DJI Drone Safety Features," *Extreme Tech*, June 22, 2017, available at <https://www.extremetech.com/electronics/251369-russian-company-selling-mods-bypass-safety-features-dji-drones>.