UNITED STATES AIR FORCE CENTER FOR UNCONVENTIONAL WEAPONS STUDIES at The Air University

Chemical/Biological-Capable RPA Threats and National Security Implications

By Lt Col Jason A. Lay, USAF

cuws.au.af.mil

> Where we are in terms of unmanned aerial vehicles is about the same place we were with biplanes right after World War I. We are at the very, very early stages of realizing what the potential of unmanned aerial vehicles are.
>
> David A Deptula, Lt. General, USAF (Ret.)
> "Rise of the Drones," *NOVA*

— Introduction —

The technological landscape of the 21st century is evolving at an ever-increasing pace. Autonomous remotely piloted aircrafts (RPAs) are becoming more and more sophisticated in size, range, and capability. With the progression of research and development, RPAs continue to increase in availability and utility among both civilians and the military, making them a prime candidate for use in irregular warfare by state and non-state actors. The US Air Force (USAF) predicts that one-third of its military and attack fighter planes will be unmanned within the next ten years.[1] In addition, emerging micro- and nano-technologies are exposing new potential threats in chemical and biological warfare (CBW) that were not possible just a few years ago, opening the door to previously unthinkable potentials. Further still, existing chemical and biological treaties, which have been widely adopted around the globe, do not adequately address these prospective and evolving threats, leaving room for potential exploitation by foreign players. The defense posture of the United States is not adequately prepared for the combined threat of today's cutting-edge advancements. The US government should address the growing risks introduced by these emerging technologies, which are generating new threats to US national security that are not thwarted by present-day defense capabilities and international treaties. Future national defense efforts must envelop critical vulnerabilities posed by emerging technologies in order to protect Americans and to deter adversarial use of chemical and biological-capable RPAs.

This paper will begin by highlighting many recent advancements contributing to the technological developments of RPA vehicles. Next will be a review of the existing defense capabilities of US forces and installations with respect to potential vulnerabilities, and a discussion of viable gaps contained in the Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) concerning 21st century capabilities. The conclusion will include analysis and recommended actions to address some of the presented concerns.

— Cause for Alarm —

In January 2015, a lone individual flew a small quad-copter onto the grounds of the White House. While the event was deemed an accident, it still resonates with implications of what might be possible if someone has hostile intentions. Do these small RPAs pose a realistic threat? If so, what are their capabilities, and how do you defend against them? Dr. Steven Huybrechts of Applied Minds—an innovative technical solutions company based in Burbank, California—says that "the threat to National Security is already here [and] we'll have to figure out something quite soon to deal with it."[2] As a primer to the following discussion, first consider this hypothetical scenario:

> On an October Tuesday afternoon, just outside the view of local Security Forces personnel near Joint Base Anacostia-Bolling, a lone terrorist walks along the treed fence line. Behind him, he pulls a wheeled footlocker through the grass. He stops beneath a large tree, covers the plastic case with camouflage netting, and then hides the package within the tree. Glancing around to be sure he is not being watched, he flips the master switch and walks away.
>
> A few minutes later, a small drone emerges from inside the footlocker; the miniature aircraft is only a few inches wide and even smaller in height. The drone hovers clear of the tree then climbs toward the tall perimeter fence, easily

Lt Col Jason Lay is a student at the Air War College at the Air University, Maxwell Air Force Base, Alabama.

passing over the triple-strand barbed wire. It is now on the base.

Guided by a combination of global positioning system, two-way radio communication, and an on-board inertial navigation unit, the drone travels above the rooftops of base facilities and vectors toward the large Defense Intelligence Agency (DIA) building just inside the main gate. Busy pedestrians walking below do not even notice the faint sound or small silhouette traversing the sky.

Back at the footlocker, additional drones emerge from the box and proceed onto the base—twenty in all. Five of them head to the DIA, while others depart for the Command Post and general officer housing. Upon arrival, each drone surveys its surroundings via an onboard camera, and transmits real-time data and imagery back to the central computer. The terrorist, miles away on a Metro bus, watches the events unfold from his smartphone.

The drones at the DIA swarm onto the roof and gather near the large air handler intakes. In unison, they excrete several clouds of atomized sarin liquid into the ventilation system, exposing hundreds of unsuspecting workers inside the facility.

Arriving at the general's housing, the other drones disperse throughout the neighborhood and settle out of sight near doors and walkways. They transition into 'sleep mode' while their proximity scanner waits to detect approaching activity, when they will burst from hiding and spray their lethal venom right in the face of an unsuspecting victim.

By this time, the DIA building is undergoing a mass exodus, and the base has initiated total lockdown at Force Protection Condition (FPCON) DELTA, Mission Oriented Protective Posture (MOPP) level 4. The Crisis Action Team (CAT) and Emergency Operations Center (EOC) are activated and key personnel are hurrying to their response locations while the remaining base population takes cover in-place, under blaring wavering sirens. As responding Airmen arrive outside the Command Post dressed in their MOPP gear, the nearby drones analyze infrared imaging to identify heat signatures, orientation, speed, and direction of incoming personnel. The Airmen's only defenses are designed against a passive airborne threat; however, these drones each employ a single hypodermic dart laced with a bioengineered virus—the needle easily penetrates their protective suits and into the skin.

It will be days before tensions ease and leaders are able to contemplate how America was once again surprised by a lethal attack on its own soil. Meanwhile, all the drones return to the footlocker off base and the terrorist, avoiding discovery, retrieves his deadly package without leaving a trace.

This chilling scenario may seem like a Hollywood-style fantasy, yet this threat is entirely plausible with existing and developing technologies. According to Mr. Clint Hope, Chief Scientist at Applied Minds, "swarms of autonomous inertially guided drones with speeds up to 400 mph, extended range, and enough payload to deliver traditional and non-traditional threats already exist, and we should be prepared for them targeting US installations."

— Current and Emerging Technologies —

Traditionally, the development, production, and employment of chemical or biological weapons required a large industrial footprint and sophisticated delivery systems only available to state actors. However, recent advances in technology allow for the precision distribution of CBW without the need for huge stockpiles or the randomness of large plume deliveries. Technology is beginning to overcome these prohibitive obstacles and open doors of possibility to those who wish to do harm by using chemical and biological weapons.

The review of current and emerging technologies will focus on several categories of application. First is an examination of the elements that make RPA technology a reliable and effective platform. Next is a look at the supporting technologies and factors complementing the continued sophistication of future RPAs, such as manufacturing technology and dedicated research, followed by a discussion of advances in nanotechnology and bioengineering and their impact on future chemical and biological weapons.

While RPA technology has existed in one form or another for decades, recent key advancements in micro-RPAs have synergized to improve their performance and reliability. Elements such as dedicated research and advanced microprocessors have combined to make this technological leap possible. Microprocessors are the integrated circuit chips that interpret software programming and serve as the brain of all computing devices. Since the dawn of the computer age, microprocessors have continued to shrink in both size and cost, while simultaneously growing in performance, capacity, and speed. Their widespread application in a multitude of products around the world has contributed to increased availability. Currently, a credit card-sized microprocessor that is 28 times faster than an Intel 486 processor and possesses 400 times more memory is commercially available for less than $35.[3] Ongoing research contributes to the evolution and overall progress of RPA development. Dozens of agencies are devoting hundreds of millions of dollars to RPA research and development. In 2016 alone, the US Air Force projects to spend approximately $123 million on unmanned aerial vehicles and RPA research.[4]

Several supporting technologies are also making a significant impact. For example, additive manufacturing (3D printing) is changing the way products are constructed. While 3D printing has been around since the 1980s, it took decades to mature and become a readily available and affordable process.[5] Today, commercially available 3D printers sell for less than $400. The process of 3D printing allows for rapid production of very complex components that used to take large amounts of time and money. Additive manufacturing advances micro-RPA technology due to its small, lightweight characteristics. An additional benefit of 3D printing allows a person on one side of the world to print a physical part on the other side of the world with the touch of a button. This capability is unique to additive manufacturing and represents a significant shift in the proliferation of fabrication processes.

Advancements in manufacturing technology continue to emerge as new concepts are demonstrated in the lab. Researchers at Massachusetts Institute of Technology are now developing 4D manufacturing, which adds the new dimension of self-assembly to the manufacturing process.[6] Efforts are also underway to expand the types of materials adaptable for printing. Besides plastic and some metals, researchers have developed capabilities to print functional materials, which include conductive and non-conductive components.[7] This achievement enables the printing of electrical circuitry directly onto three-dimensional parts during fabrication. Future projected enhancements include the ability to print resistors, diodes, and other electrical components. Enhancements such as these

have immediate application to the production of small and micro-sized RPAs. Continued future improvements could potentially develop the ability to print an assembled, fully-functioning RPA without any human intervention.

These technical capabilities all contribute to the overall enrichment of RPA development, and future advancements generated from dedicated research are also promising. New means of achieving lift and propulsion for small aerial vehicles are currently in development. In 2011, Defense Advanced Research Projects Agency (DARPA) made public the achievement of a flapping-wing RPA called "Hummingbird."[8] This small device, with a six-inch wingspan, is capable of vertical takeoff and landing, as well as controlled flight in all directions. It does not use rotational motion for lift; therefore, it does not require the tail section, elevator, vertical stabilizer, or counter torque propeller necessary with most common aircraft designs. Finally, in 2014, a team working at Harvard University successfully achieved flight with their nano-RPA device called "RoboBee."[9] The insect-like vehicle has a wingspan of only three centimeters and represents the smallest man-made device modeled after an insect ever to achieve flight. Current progress requires the tiny robotic insect to be tethered, but future designs are working toward autonomous, untethered versions that communicate with an entire "hive" of other RoboBees. These recent accomplishments are furthering the capabilities of micro-RPAs, yet such improvements could also allow for exploitation when combined with advances in other fields of study. Specifically, developments in nanotechnology and bioengineering are making strides into previously uncharted territories. While developers have beneficial intentions, the potential for misuse remains, and could introduce unforeseen utility in CBW employment.

Nanotechnology and bioengineering are advanced scientific fields of study with positive contributions in multiple disciplines, such as information technology, healthcare, and materials science. While primarily conducted under laboratory conditions, their contributions to the field of chemistry and biology have many practical applications. Nanotechnology is the manipulation of the physical makeup and structure of materials at the molecular level.[10] It enables direct control of atomic building blocks for influence over material properties. This level of control leads to the development of non-naturally occurring compounds, such as lighter and stronger materials. With regard to CBW, it also lends itself to the potential development and production of new chemical compounds without the large industrial processes required in the past. This capability could change the approach to manufacturing chemical weapons, enabling their availability to small-scale actors.

Like nanotechnology, bioengineering is capable of creating new types of microbial or biological organisms through controlled manipulation of biological compounds. In 2014, a researcher at the University of Wisconsin reportedly constructed a new version of the flu virus from the genes of a wild avian flu strain. This new virus proved capable of spreading from one host to another, and had more infectious properties than the original virus.[11]

Research in these fields has also yielded the creation of nanobots—tiny machines or organisms that perform medical tasks internally within the body or bloodstream. Nanobots are either entirely constructed of DNA proteins, which are genetically programmed to perform specific functions, or are made of inorganic materials capable of navigating through the body with magnetic motive propulsion to deliver medication to needed tissues.[12] Specific developments such as these could potentially be adapted for adversarial uses in CBW development and employment.

— Defensive Capabilities —

In consideration of the evolving threats posed by technological advances, it is necessary to evaluate the specific defense capabilities of US forces and facilities concerning their capacity to prevent, detect, and defend against future attack from CBW-capable RPAs. This review will specifically evaluate Anti-Access/Area Denial (A2/AD), chemical, biological, radiological, and nuclear (CBRN) detection, and Individual Protective Equipment (IPE).

Typical discussions of A2/AD focus on the ability of US forces to overcome the defenses of an adversary, but in this context we are referring to the ability of US military forces to impose A2/AD against an adversarial use of its own airspace. A2/AD relies on two major features: 1) the ability to detect the presence of an adversary, and 2) the ability to deny adversarial use of a given region of airspace. Therefore, we must answer two main questions: do we possess the ability to detect micro-RPAs, and are we able to prevent their use in a given airspace?

With regard to detection, the capability definitely exists. Airspace detection and radar equipment are technologically capable of locating insect-sized flying objects; the difficulty lies in the capacity to determine whether a detected object is an RPA or an actual insect or bird. In theory, this distinction is achievable with human or computational evaluations; however, the ability to detect and evaluate a small object in a large open field is not the same as being able to distinguish the same object operating in and among buildings and trees. Additionally, RPA control programming could mimic the flight characteristics of birds in order to fool detectors, analytic algorithms, and even humans. As long as low-flying micro-RPAs have the ability to blend in with birds and insects, the effort of detection will remain prohibitively difficult.

Assuming the challenges of detection are solvable, the next challenge to face is that of denial. Traditional airspace denial employs a combination of surface-to-air missiles and air-to-air combat aircraft at great standoff distances from critical assets, but these defensive measures would prove ineffective against any number of micro-RPAs. Current capabilities specialize in defeating large aircraft with precision kinetic weapons. In effect, the introduction of RPAs into US airspace defense reveals a significant gap in the air superiority model. The current threshold of US capabilities does not extend low enough to address these threats with traditional methods.

In practice, Security Forces personnel on the ground conduct the primary A2/AD effort at homeland USAF installations. Security Forces Airmen protect base perimeters and airfields to prevent unauthorized access, but while overall base defense is their responsibility, their security procedures do not include provisions for defending the airspace of the installation. Existing perimeter defenses are largely passive—consisting of fencing and barbed wire aimed at denial of personnel and vehicles. These defenses present little challenge for RPAs operating just ten feet above the ground, allowing complete and largely undetected access to an entire base complex. If an influx of micro-RPAs were to breach a base perimeter, local wing leadership would look to Security Forces personnel as the primary means of defense and quickly realize that they are ill-equipped to respond to such a situation. It is evident that US installations are not prepared to project A2/AD against the emerging RPA threat.

Existing CBRN detection equipment uses methods optimized for traditional CBW employment on the battlefield. Multiple detection stations distributed throughout a base act as a network of nodes for determining the presence of plumes of CBW over large areas. However, as demonstrated in the opening scenario, the use of RPA-distributed chemical or biological agents at precise locations would counter the value of these detectors. Their data would offer little certainty in determining affected or unaffected areas, creating serious limitations to their usefulness.

In the event of a CBW situation, USAF personnel are trained to don the Joint Service Lightweight Integrated Suit Technology (JSLIST) IPE ensemble and M50 Joint Service General Purpose Mask. These items are effective for operations involving exposures of short duration in environments affected by chemical and biological agents. The primary defenses provided by this ensemble are air filtering and prevention of skin contact. This defense method is effective against a passive fallout cloud, but simple aggressive measures could easily overcome the effectiveness of the CBRN IPE ensemble. The thin rubber gloves are a primary target of weakness against penetrating projectiles, which are conceivably dispersible from a micro-RPA. Additionally, the suit itself is easily penetrable, and is consequently susceptible to exploitation as well. Lastly, the critical value of the M50 mask makes it a natural target. Disruption of the mask seal, puncture of the lens, or saturation of the filter intake are all significant vulnerabilities. It is therefore plausible that current MOPP postures are not an adequate defense mechanism to oppose a technologically advanced RPA with CBW capabilities.

Finally, the potential psychological impact of CBW is high due to the powerful nature of fear. Throughout history, the employment of CBW has evoked fear due to the perception that it is an inhumane tactic. Acts of terrorism also use fear to accomplish strategic objectives over adversaries, making full use of this powerful influence. Therefore, the combination of terrorism and CBW creates an even greater dose of fear than either tactic used on its own. Even though there are only a few historical examples of terrorists using CBW, it is worth recognizing the influence of this probable combination. Past limitations to access, along with employment of large stockpiles of CBW and complex delivery systems, may have previously prevented terror groups from incorporating CBW; however, it is now conceivable that advancements such as RPA technology could eventually overcome the resistive hurdles of these weapon types and give rise to new methods of employment.

— International Treaty Language —

With the constant progress of technological advances, is the language of the CWC and BWC still relevant for these current and emerging challenges? On the surface, the CWC appears to address the development, production, acquisition, stockpile, retention, transfer, use, and preparation of chemical weapons.[13] Likewise, the CWC definition of chemical weapons is broad enough to encompass unforeseen methods and equipment that might be developed with future technologies. Further, the definition of "Toxic Chemical" in Article II, Paragraph 2 includes a very broad scope, regardless of origin or production method, which would seem to be sufficiently protective as well.[14] However, upon further review, there appears to be an anomaly subject to exploitation with regard to incapacitants and riot control agents (RCAs).[15] Article I, Paragraph 5 specifically states that RCAs will not be used for warfare, yet leaves other implemented uses of RCAs, such as for law enforcement purposes, unrestricted by the CWC. This gap in coverage allows a signatory member of the CWC to develop, store, and use chemical RCAs for non-warfare purposes (e.g., internal security operations). In addition, the definition of RCAs in Article II, Paragraph 7 includes the phrase "disabling physical effects" of a temporary nature, which is difficult to distinguish from incapacitants. The CWC expressly covers temporary incapacitants as chemical weapons and prohibits their use, yet the definition of incapacitants is not clear in Article II and thereby allows for the possible misinterpretation of this element. While it is not directly related to technological advancements, a small loophole such as this one permits rogue actors to exploit the use of chemical weapons—potentially without reprisal.

With regard to the BWC, it likewise is extremely thorough in addressing the breadth of definitions for microbial and biological agents.[16] In fact, it sufficiently covers the improper development or use of any bioengineered organisms or viruses that may emerge in future warfare. Yet the field of nanotechnology could conceivably advance to produce non-organic autonomous mechanisms designed for internal uses, which could have devastating and perhaps lethal results. This kind of weaponry, while not biological in nature, could produce effects similar to those seen with biological warfare agents. Since the structural makeup of these nanobots is neither a microbial, a toxin, nor a biological agent, their development, production, and employment are clearly outside the defined boundaries of the BWC. The emerging risks associated with this new technology present a completely new subject requiring further investigation for national and international policy decisions.

— Analysis—

It is clear that recent scientific and technological advancements are introducing new potential threats, but what is the likelihood of these threats manifesting into real-world events from an adversary? Is it reasonable to expect that a signatory foreign state would seek to take advantage of seemingly minute loopholes in the international chemical and biological conventions? And what techniques or procedures are likely to decrease US vulnerability to such actions?

The cataclysmic events of 9/11 unmistakably demonstrated that advanced technology (long-range aircraft) in the hands of just a few skilled terrorists is capable of imposing large-scale, deadly, and destructive effects on thousands of people, and of devastating communities and impacting an entire nation. The attack on that day was arguably unexpected, and few preventative measures were in place that could have stopped it from occurring. While future adversarial threats may continue to be unique and consequently elusive, efforts to identify and respond to remote-chance, emerging dangers should increase to an all-time high. While attempting to prevent every foreseeable threat can be an extremely costly proposal, it is imperative that as many threats as possible be identified to allow for compilation, analysis, and prioritization of each according to their merits. Identified threats should undergo thorough exploration and consideration in terms of their severity and potential. Likewise, counter-measures to impede their effects should be developed and assessed for practicality of implementation and effectiveness. This method is the best way to evaluate existing and impending dangers, and to determine the appropriate measures of response.

— Recommendations —

Despite the vast array of technological advances imposing new threats to US national security, several options are available for consideration in order to minimize, reduce, or possibly eliminate these threats. In the area of RPA technology, the US government must stay on the leading edge of research and development. Dedicated research through agencies like DARPA, Defense Threat Reduction Agency, universities, and research grants will help ensure US forces have the best technology available in the field of RPAs.

Enhancements in defense capabilities are also a necessary consideration in order to address the growing threats imposed by RPAs. US installations and high-profile facilities need low-level radar detection with the capability to distinguish between organic and inorganic objects, and to identify potential drone operation within a given airspace. Along with enhanced detection capabilities, the United States should implement both active and passive area denial methods for small, micro-, and nano-sized RPAs. A simple, low-tech, passive solution would protect facilities by installing netted or fenced cages to impose fixed standoff distances away from fresh-air intake vents.

A possible active defense method for neutralizing small RPAs is the use of a shotgun or similar weapon to thrust an array of projectiles at a target. However, depending on the environment, and especially near flying operations, shooting firearms into the air would impose serious drawbacks and concerns. High-tech sentry guns, such as the Phalanx Close-In Weapons System (CIWS) utilized by the US Navy, provide autonomous, computer-guided tracking and firing capable of destroying small and fast inbound enemy projectiles, rockets, and aircraft. Similar versions of this weapon system are in operation around active airfields and populated areas, utilizing complex algorithms for detection and aiming to avoid unwanted damage to friendly or coalition assets. Targeting capabilities include detection of small profile objects measuring less than one meter in length and at velocities over 300 miles per hour. With a firing rate of 3,000 rounds per minute, and utilizing mid-air exploding projectiles in order to limit the range and potential for collateral damage, this system has a high potential for application in defending against an RPA threat. However, kinetic defensive measures are limited in their capacities for simultaneous effect. Systems like the CIWS can only effectively defend against a single target at a time, and firearms require maintenance and reloading, which causes interruptions in defense capabilities. These drawbacks can be overcome by means of a network of multiple systems, which increases their overall capacity.

Other high-tech solutions capable of RPA defense include incapacitating directed energy (e.g., acoustic or microwave radiation), sensory overload devices to confuse or overwhelm RPA inputs and cause disorientation, electronic or electromagnetic disruption, or a defensive swarm of RPAs designed to target and destroy intruding RPAs of various sizes and capabilities. While these unconventional defensive methods require further testing and development, they offer the distinct advantage of having broad simultaneous effects over large areas, and are capable of continuous operation without the delays imposed by kinetic defensive measures.

Blighter Surveillance Systems, a UK-based company, sells the Anti-UAV Defense System (AUDS) capable of detecting, tracking, and neutralizing unmanned aircraft systems. AUDS uses directional radio frequency (RF) inhibition to take down its objectives. While this defensive solution might appear to be viable, its drawbacks are rooted in its one-dimensional method of disruption. RF communication is a common control method for RPA operation, but it is not the only process available. Unfortunately, the AUDS would prove ineffective against an advanced RPA equipped with on-board inertial navigation, and not reliant on outside signals for routing and control. Successful employment of RPA defensive measures will likely utilize multi-dimensional efforts capable of delivering a family of impedances to thwart unwanted RPA operations.

Protection of personnel in the CBRN environment must also be improved. JSLIST ensemble upgrades could include anti-piercing membranes to resist targeted injections; glove materials require similar upgrades as well. A protective clip-on screen installed over the air intake of the M50 mask would prevent filter targeting intended to clog or overwhelm the wearer's breathing process. Modernization of IPE to include defensive measures against active threats, rather than only passive ones, would allow for greater protection of personnel.

Lastly, the identified loopholes in the international chemical and biological conventions must be closed. This action will dispel ambiguity surrounding the use of chemical agents for nonwarfare activities and provide definitive clarity on RCAs and incapacitants. Similarly, it will define and prohibit employment of inorganic objects—such as nanobots capable of causing harmful or lethal effects—within humans or animals. Alternatively, the United Nations Convention on Certain Conventional Weapons, which already deals with lethal autonomous weapons systems, is another potential mechanism to encompass the prohibition of inorganic biological devices. Since many countries have already ratified these conventions, the best mechanism for change may be through annexation of additional protocols at an upcoming UN review conference. These revisions will likely take a great deal of time and effort to implement, so immediate action is necessary.

— Conclusion —

The continually evolving landscape of technology is producing new threats to US national security. This process of change allows for the emergence of adversarial capabilities only made possible within the past few years. Of highest concern is the employment of CBW-capable RPAs. The expansive and ever-pressing force of technological progress is unstoppable; therefore, the best response is to observe and acknowledge the vulnerabilities it exposes and take appropriate action to close the gaps.

In order to stay ahead of these growing threats, and to thwart would-be abusers of advanced technologies, the US government must consider changes to how it defends its own airspace. The longstanding dominance of US air superiority is only sustainable as long as key leadership remains brave enough to support the continual evaluation of its weaknesses. Maintaining both active and passive measures of defense with multi-dimensional capabilities is the best approach to achieving this objective; however, defense of the airspace is not enough. We should also modernize the protection of personnel with advanced IPE improvements that address the current operational environment, and we must consider modifications to the international chemical and biological conventions to close existing gaps and keep pace with the ongoing advances of science and technology. No nation can afford to have a hole in its umbrella of legal protection.

As technology continues to advance, it will simultaneously introduce and expose new threats and vulnerabilities to US national security, and national strategic leaders always face the difficult task of determining the appropriate response. One thing is certain: eventually disaster will strike, and failure to respond to known threats is a never-ending gamble against time. However, swift and proper implementation of the recommended actions will result in the improved defense and protection of US forces from this emerging danger.

— NOTES —

1. "Rise of the Drones," *NOVA*, directed by Peter Yost (Public Broadcasting Service, 2013), http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html.

2. Dr. Steven Huybrechts (Applied Minds, LLC), interview by the author, 23 November 2015.

3. "Raspberry Pi 2 Model B," Raspberry Pi, accessed 4 October 2015, https://www.raspberrypi.org/products/20raspberry-pi-2-model-b.

4. Dan Gettinger, "Drones in the Defense Budget," Center for the Study of the Drone at Bard College, accessed 5 October 2015, http://dronecenter.bard.edu/drones-in-the-defense-budget.

5. "History of 3D Printing: The Free Beginner's Guide," 3D Printing Industry, accessed 5 October 2015, http://3dprintingindustry.com/3d-printing-basics-free-beginners-guide/history.

6. "4D Printing: Multi-Material Shape Change," Self Assembly Lab, accessed 5 October 2015, http://www.selfassemblylab.net/ 4DPrinting.php.

7. "Functional Materials," Voxel8: 3D Electronics Printing, accessed 8 October 2015, http://www.voxel8.co/materials.

8. "AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA," AeroVironment, 17 February 2011, accessed 5 October 2015, http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird.

9. "RoboBees," Projects at Harvard, accessed 4 October 2015, http://robobees.seas.harvard.edu.

10. "Nanotechnology and You: Benefits and Applications," Nano.gov, accessed 7 October 2015, http://www.nano.gov/you/nanotechnology-benefits.

11. Tatyana Novossiolova and Malcolm Dando, "Making viruses in the lab deadlier and more able to spread: an accident waiting to happen," Bulletin of the Atomic Scientists, accessed 6 October 2015, http://thebulletin.org/making-viruses-lab-deadlier-and-more-able-spread-accident-waiting-happen7374.

12. Evan Ackerman, "Robotic Micro-Scallops Can Swim Through Your Eyeballs," 4 November 2014, http://spectrum.ieee.org/automaton/robotics/medical-robots/robotic-microscallops-can-swim-through-your-eyeballs.

13. "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction," United Nations Office for Disarmament Affairs, accessed 5 October 2015, http://disarmament.un.org/treaties/t/cwc/text.

14. Ibid.

15. "Chemical weapons convention fails to address key issues," SciDevNet, accessed 6 October 2015, http://www.scidev.net/global/governance/news/chemical-weapons-convention-fails-to-address-key-issues.html.

16. "The Biological Weapons Convention," United Nations Office for Disarmament Affairs, accessed 6 October 2015, http://www.un.org/disarmament/WMD/Bio.

The mission of the **U.S. Air Force Center for Unconventional Weapons Studies** is to develop Air Force, DoD, and other USG leaders to advance the state of knowledge, policy, and practices within strategic defense issues involving nuclear, biological, and chemical weapons.

The Trinity Site Papers present key discussions, ideas, and conclusions that are directly relevant to developing defense policy and strategy relating to countering weapons of mass destruction and developing the nuclear enterprise.

The opinions, conclusions, and recommendations expressed or implied in this article are those of the author and do not necessarily reflect the views of the Air University, Air Force, or Department of Defense.