Drones: A 360 Degree View

Neil Jacobstein

World Policy Journal 2013 30: 14
DOI: 10.1177/0740277513506376

Drones: A 360 Degree View

NEIL JACOBSTEIN

BLACK PAW PHOTO

Drones belong to a broad class of accelerating technologies that are increasing in capabilities as they decrease in cost. Driving this acceleration of technical capability is the exponential growth of information. Computer hardware and software, advanced aircraft materials, and imaging technologies such as high-resolution video cameras are all benefiting from lower costs and higher performance. For some applications, what used to take a $1 million drone can now be accomplished with a drone that costs less than $1,000.

Technologies such as drones that undergo rapid technological acceleration have several patterns in common. They are often initially sponsored by the military but end up with the vast majority of their applications in the commercial sector, providing an astonishing variety of social benefits. The new capabilities can also be used for evil purposes by terror-

ists or for questionable purposes by the well-meaning. Attempts to relinquish or ban these new technologies often serve to push them underground, inhibit research and development on counter-controls, and provide competitive advantage to those who ignore the rules and evolve the technology quickly.

These technologies will eventually be controlled, albeit imperfectly, by multilayered and redundant methods that include professional guidelines and ethics, flexible and nuanced licensing laws and regulations, credible enforcement methods, legal consequences for abuse, embedded technical controls, and continuous monitoring and rapid response capabilities that mimic the way our immune system responds to external threats. The best way out of the danger posed by these technologies is to harness them to serve our constructive purposes, including policing them and responding to their abuse.

THE COMING WAVE

Drones, or unmanned aircraft systems (UAS), are constructed from readily available materials and used by hobbyists, governments, and businesses around the world. Indeed, military uses of drones are already well on their way to becoming a minority of unmanned aircraft system applications.

Drones are now being used in a broad range of applications from marine and land based wildlife protection to traffic monitoring; bridge, pipeline, and high rise inspection; climate monitoring; emergency drug delivery; crime detection; disaster response; aerial video shoots for movie productions; heat maps for fire fighters; hazardous materials assessments; and search and rescue missions on land and sea. Drones are inexpensive and extraordinarily capable flying robots. They have the ability to hover in one precise location, take off and land vertically, fly through narrow airspaces and burning buildings, and operate under gas, battery, or even solar power for light duty applications. Drones may take the form of an airplane, which tends to increase range for a given power source. They may also be highly maneuverable 24-to-48 inch rotorcraft, with one, four, six, eight, or more motors driving propellers.

THE DEVELOPMENT OF DRONE TECHNOLOGY IS TAKING A PARALLEL COURSE TO THE EARLY DEVELOPMENT OF THE INTERNET.

Drones can deploy a wide variety of sensor systems from high-definition video and still cameras, to infrared and multi-spectral imaging systems, 3D camera rigs, and lab-on-a-chip molecular sensors to detect hazardous substances. The data collected by these sensor systems can be channeled to cloud storage systems through a continuous, high-bandwidth Internet connection.

Meanwhile, drones are shrinking not just in cost, but also in the size of the package necessary to deliver high-resolution sensor based information. For example, California-based AeroVironment Corp., has recently developed a Hummingbird Drone for the Defense Advanced Research Project Agency (DARPA). Resembling a hummingbird and able to hover and fly with some precision, it incorporates a high-def-

Neil Jacobstein is co-chair of AI and Robotics at Singularity University, located inside NASA Research Park in Silicon Valley, whose aim is to "educate, inspire, and empower leaders to apply exponential technologies to address humanity's grand challenges."

inition video camera that can stream video from the remote-controlled "bird" flying through buildings. There are already bee-sized drones, and the trend of decreasing size and power consumption will eventually produce drones that are nearly impossible to detect by unaided human senses.

The shrinking cost and form factor of drones are as disturbing from a privacy point of view as they are useful from a security monitoring perspective. Drones can provide transparency at crime or emergency scenes, monitoring or responding to signs of trouble. Alternatively, they can be rigged with explosives or toxins by terrorists and flown into a building. This kind of conflict between competing uses and values is common with new multi-use technologies, and society is forced to sort out the balance of interests between innovation and security. But given the destructive power that new technologies, including drones, place in the hands of individuals and small groups, some loss of privacy and freedom to deploy without regulation is very likely inevitable. The key is to have thoughtful public oversight of systems that may violate public safety or privacy, and to take concerted steps to see that the privilege to use these systems is not abused.

BEYOND THE INTERNET

The development of drone technology is taking a parallel course to the early development of the Internet. DARPA first developed the Internet as the ARPANET in 1968 with the aim of building a military communication system that could be resilient in the face of unreliable network hardware. The potential for hacking, spying, privacy invasion, viruses and worms, cyber crime, and even Skynet-like runaway artificial intelligence science fiction scenarios were all explored in the 30 years leading up to the dramatic growth of the commercial and industrial World Wide Web. During the first few years of operations, Internet applications were largely sponsored by military contracts.

If the government had opted to ban or tightly control the Internet (limit it to classified operations for example), due to fear of potential abuse, every advance in commercial online systems, from Amazon and iTunes to Netflix, Google, and tens of millions of business web sites would never have happened. The growth of social media such as Twitter, Facebook, or LinkedIn would have been impossible or severely restricted. Indeed, the military usage of the Internet eventually took a backseat to social media traffic and commercial applications. Children born after 1995 typically do not associate the Internet with a military system at all. Many are surprised that the military had a major role in inventing something so commercially revolutionary. The trajectory of drone technology seems destined to head in a similar direction of rapid commercialization.

In less than 10 years, most of the world's drone applications will be obviously useful commercial systems. Military applications will likely not rank in the top 10 most frequent use of drones. Certainly, the debate over the military use of drones is fundamental to the United States' moral standing in the world. But it is critical not to hobble an important technology and emerging new industry because we have legitimate concerns about the rules governing the ethical use of drones in military and counter-terrorism operations, or the potential for their abuse. Clearly, there is potential for abuse, including by U.S. citizens, or groups that have experienced our drone attacks and want to retaliate. However, the best way to respond to those potential threats is to anticipate them and innovate faster than the attackers.

EVALUATING RISK

It is important to get some perspective on the deaths caused by drones. Compared to terrorism, counterterrorism, drone attacks, or even recent wars, automobile technology is far more lethal. In 2010, 33,000 people were killed in automobile crashes in the United States, and 1.2 million people were killed worldwide. And yet, we don't ban cars or regulate them into being permanently parked. We know they are useful. Instead, we attempt to regulate them via built-in safeguards, such as seat belts, air bags, collapsible steering wheels, child seats, and structural crash protection. We also take steps to license pilots of cars, test them periodically, check their eyesight, monitor their driving record, forbid them from texting while driving, and sample their breath and blood for intoxication. And still we manage to kill more than a million people world wide, and maim many more. It is notable that this is not the subject of a huge public debate about "lethal automobile technology."

Accidental deaths due to drones appear to horrify us more than traffic fatalities, but not due to the quantity of blood and suffering. Both represent genuine tragedies. We have become habituated to the horror of avoidable accidents in human-piloted, ground-based vehicles. However, there are alternative technologies. The Google self-driving car has driven over 500,000 miles on U.S. roads and highways, and it has an outstanding safety record.

If we focused on making cars radically safer via well-tested autopilots that can communicate with each other and avoid crashes systematically, we could save lives, traffic time, and energy. The problem is not the lethal potential of the cars per se, it is the lethal potential of the drivers. It all depends on the way automobile technology is framed and utilized. Likewise with drones.

We find the limited destruction via drones far more disturbing than the vastly greater death and destruction on our roads, partly because we find death raining from the skies more salient, novel, and creepy. Ground-based tanks would get less attention. In addition, people find the deliberate but imperfect targeting of terror suspects via drones in the sky more disturbing than the random slaughter of innocents on the road. Status quo bias aside, drones do enable the risk of moral hazard and will be challenging to control.

A STYMIED AND LARGELY MILITARY AND INTELLIGENCE DRIVEN DRONE COMMUNITY WILL NECESSARILY FALL BEHIND.

ACCOUNTABILITY

The policies surrounding the use of drones for targeted assassination of terrorist suspects have been cloaked in secrecy and executed under conditions that make them less than fully accountable to the public. Some argue that the American public just wants the government to make the homeland safe, and they don't want to know the details of how this is attempted, however imperfectly. Others claim to want full disclosure and transparency of actions taken in their name and with their tax dollars. One side claims that the military and intelligence drone program has been extraordinarily successful in disrupting terrorist networks and leadership. Others claim that the drone attacks were minimally effective, resulting in questionable targeting, considerable collateral damage in the death and dismemberment of innocents, and the ultimate loss of the hearts and minds of the very groups that western democracies most want to influence. Let's

stipulate that each of these perspectives has some merit. If that is true, then what?

Few on either side of the drone debate would contend that targeting terrorists wouldn't benefit from a more inclusive and thoughtful process with well-informed public representatives. At the very least, it would make clear that the process is not capricious or unaccountable. We can't rely on the friction of deploying weapons systems to prevent us from having to confront the policies for their use. Drones are relatively easy to deploy compared to troops, but drones don't make policy. We do, and we are responsible for their use. There is simply no escape from that responsibility—delegated or otherwise.

Drones used for military and intelligence purposes have been remarkably reliable mechanically and electronically. The primary problem is not that they don't fly well, or that they typically get lost, or that they can't shoot straight. The fundamental problem, and the core of the ongoing debate, is over the policies governing military and intelligence use of drones. The entire future ecosystem of peaceful commercial and government use of drones should not be threatened or destroyed because we need a more nuanced and effective set of policies.

Commercial drone flights are scheduled to begin in the United States in 2015, but the current policies and laws promulgated by the Federal Aviation Administration are not workable for most commercial drone operations. They are being revised because they are inflexible, complex, and old-fashioned. Laws may attempt to keep a lid on the risks of drone technologies, but severe restrictions will cause us to forfeit many of the benefits of commercial drones, without providing meaningful operational security.

POLICY PRIORITIES

A more effective set of policies with respect to the use of drones would encompass a number of priorities that a bipartisan group could probably agree on.

First, these policies need to address the reality that the people living in the areas where the United States has focused its drone attacks are suffering mightily. Developing a public-private coalition to help them develop their own access to food supplies, education, and health care could go a long way toward winning their hearts and minds. Such initiatives can't eliminate the negative blowback from the military use of drones, but over time, they can reduce the need for military intervention and provide tangible evidence that the United States is not "all bad."

Second, as President Barack Obama noted in his May 23, 2013 speech on the use of drones, the terrorist threat is real in sectors of the Middle East, especially Yemen, and the Afghanistan-Pakistan frontier region. The United States and its allies cannot simply ignore the threat. In some select cases, we will need to send in "boots on the ground" or drones. Each alternative has strengths and weaknesses, and the tradeoffs are difficult. Sending in troops may seem more humane, until the troops are your close relatives. The process for deciding on the actions to be taken needs to be clear, transparent (at least to government representatives outside the defense and intelligence community), and ethical. It should have a high probability of being able to stand up to critical review a decade or two later.

Third, the United States and its allies should expect that the use of military drones will be unpopular, even when used under the most legitimate, limited, transparent, and ethical circumstances. Policies about the use of these drones need to clearly distinguish military drones from what will

be the vast majority of unmanned aircraft systems that will also be used for more anodyne purposes even in the areas targeted for military operations.

Fourth, we need to accelerate technical programs that could actually enhance commercial drone security. It is true that all drones are potentially "dual use" technology, in the sense that they could all be converted to lethal purposes. However, this is also true for cars, computers, electric saws, matches, and the Internet. Rather than simply banning these technologies, we try to embed technical control systems, and put thoughtful restrictions on their abuse. And when legal restrictions don't work, we have methods for rapid detection and intervention. We track and shut down rogue cars, people, fires, and computer viruses.

Commercial drones can be required to have encrypted code transponders and redundant forms of kill switches that could allow a law enforcement agency to shut them down if they present a threat or are a clear public nuisance. If they are rogue drones without the proper transponder credentials or switches, they could be taken down by other unmanned aircraft systems. This requires building rapid detection and response systems, not unlike the anti-virus software "immune systems" on computers. We can't stop all of those with criminal intent from embracing drone technology, but we can monitor their drones' activities in a new age of transparency and provide rapid responses. That is not just possible. It is mandatory because we simply will not be able to stuff this accelerating, inexpensive, and ubiquitous technology back in the box.

Criminals and terrorists have already embraced drone technology. Criminals have flown drones with drugs over borders and dropped cell phones over prison walls. We will inevitably have to defend against drones being directed towards us. We should therefore not be defenseless or noncompetitive against the best globally-developed, open source drone technologies launched by small groups of malevolent individuals. This will likely become a predator-prey cycle of offensive capabilities and defensive innovation as the systems on both sides become more sophisticated.

Some future drones will be almost invisible, nearly silent, and difficult to kill. Others may embed limited artificial intelligence to do situation assessment, planning, and pre-approved actions. Military policy requires a person in the loop for lethal actions. Drones haven't yet earned the right to operate weapons autonomously. The potential to lose the edge commercially and militarily is a very good reason to ensure that the United States and its allies not fall behind in the commercial development of drones, which will proceed globally and develop innovative capacities at a blistering pace.

A stymied and largely military and intelligence driven drone community will necessarily fall behind the accelerating learning curve in the global economy. Most of the world's drone innovators will work outside government walls. Only a vibrant industrial research and development community can make the vast majority of unmanned aircraft systems commercial, competitive, and socially useful in 10 years. ●