STATEMENT ON THE SECURITY THREAT POSED BY UNMANNED AERIAL SYSTEMS AND POSSIBLE COUNTERMEASURES

TODD HUMPHREYS
THE UNIVERSITY OF TEXAS AT AUSTIN

Submitted to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security

Date: March 16, 2015.

1. Summary

The nearly 100,000 football fans gathered in Texas Memorial Stadium last August to watch the Longhorn football season opener had trouble concentrating on the game. Hovering above the stadium was an unmanned aerial vehicle (UAV), a drone, with blue and red blinking lights. The University of Texas Police watched helplessly as the UAV shifted from one area of the stadium to another. When the UAV's operator finally recalled the device and landed it at his feet in a nearby parking lot, the police immediately took both UAV and operator into custody.

The situation turned out to be no more menacing than a devoted but ticketless UT football fan trying to watch the game through the video feed on his drone. But the police could not have known this beforehand, and so had to treat the incident as a potential chemical, biological, or explosive attack on the multitude of gathered spectators.

As we enter an age of highly capable and increasingly autonomous UAVs purchasable for a few hundred dollars over the Internet, the intrusion at the UT football stadium will be replayed in various forms at sites critical to the security of the United States. The great majority of these incidents will be accidental, such as the flyaway UAV that crashed on the White House grounds in January. But in the early stages of a UAV incursion, it will be impossible to distinguish the accidental from the intentional, the benign from the malicious. And the distressing truth is that even consumer-grade UAVs can be rigged to carry out potent attacks against which our defenses will either be only weakly effective or so militarized that the defenses themselves will pose a threat to the surrounding civil infrastructure.

UAVs have been around for a long time. The Academy of Model Aeronautics was founded in 1936 and since that time a vibrant and knowledgeable community of radio controlled model aircraft enthusiasts has been active in the U.S. and across the globe. What explains, then, the recent uptick in alarming UAV sightings near sensitive sites? The answer is clear: never before have highly-capable UAVs been so inexpensive and widely available. One can buy over the Internet today a UAV that rivals the increasingly autonomous surveillance and guidance capability of military UAVs. Many of these commercial UAVs can easily carry a payload of a couple of pounds or more.

In thinking about how to detect and defend against UAV incursions into sensitive airspace, it is useful to distinguish three categories. First are the accidental intrusions, whether the UAV operators are sophisticated or not. Second are intentional intrusions by unsophisticated operators. Third are intentional intrusions by sophisticated operators—those capable of assembling a UAV from components and modifying its hardware and software.

Detecting and safely repelling intrusions of the first two types is not simple but is quite possible. Commercial UAV manufacturers can play a key role here by implementing GPS-enforced geofences within their autopilot systems that prevent their UAVs from being flown within exclusion zones around airports, sports stadiums, government buildings, and other security-sensitive sites. The sites themselves could be equipped with radar, acoustic, and electro-optical sensors for UAV detection, and with powerful and agile interceptor UAVs, possibly working as a team, that could capture and carry off a small number of simultaneous intruders.

UAV intrusions of the third type will be much more difficult to counter. A sophisticated attacker could mount a kamikaze-style attack against a sensitive target using a fixed-wing powered glider with an explosive few-pound payload. The UAV glider could be launched tens of miles from the target.

It could cut its engine on final approach to evade acoustic detectors, and could be built of poorly-radar-reflective material (e.g., Styrofoam) to evade radar detection. With only minor changes to the UAV's autopilot software, of which highly capable open-source variants exist, an attacker could readily disable geofencing and could configure the UAV to operate under "radio silence," ignoring external radio control commands and emitting no radio signals of its own. The UAV would thus be difficult to detect and would be impervious to command link jamming or hijacking. Moreover, the attacker could configure the autopilot to ignore GPS/GNSS signals during the final approach to the target, relying instead on an inexpensive magnetometer-disciplined inertial navigation system. Such a modification would render GPS/GNSS jamming or deception (spoofing) useless during final approach.

It is not obvious how to protect critical civil infrastructure against such a UAV, or—worse yet—against a swarm of such UAVs. What is more, the skills required of operators in this third category are not uncommon: the do-it-yourself UAV and autopilot development communities are large and the documentation of both hardware and software is extensive. One should also bear in mind that the threshold for a successful attack is low when success is measured by the ability to cause widespread panic or economic disruption. For example, explosion of a UAV anywhere on the White House grounds could be seen as a highly successful attack even if it causes only minor physical damage.

What can be done? First, it is important to take stock of what should not be done. Imposing restrictions on small UAVs beyond the sensible restrictions the Federal Aviation Administration recently proposed would not significantly reduce the threat of rogue UAVs yet would shackle the emerging commercial UAV industry. In fact, even the FAA's current ban on non line-of-sight UAV control would be of little consequence to a malefactor capable of modifying an open-source autopilot. Likewise, restricting open-source autopilot platforms would hardly improve security but would stifle innovation. Powerful and persistent wide-area GPS/GNSS jamming would prevent inexpensive UAV attacks launched from miles away from reaching their targets, but this military-style defense would be disruptive to civil use of GPS over a wide area. Powerful GPS jamming around the White House, for example, would deny GPS aiding to commercial aircraft at nearby Reagan National Airport. Similarly, anti-UAV laser or electromagnetic pulse systems are a danger to nearby civil infrastructure and transport.

From a strictly technological point of view, the best way forward will be to adopt simple measures that sharply reduce the risk of category 1 and 2 incidents, such as voluntary manufacturer-imposed geofencing. For especially critical sites, detection and tracking systems based on electro-optical sensors will be most effective, particularly those applying infrared sensor pattern recognition to distinguish a UAV's warm motors and batteries from a bird's warm body. The output of such a detection and tracking system could be fed to an always-ready squadron of interceptor UAVs whose job would be to catch the intruder in a net and expel it, or, as a last resort, to collide with it and force it down. We should refrain from any more drastic measures than this until the threat of UAVs proves to be more of a menace than the recent incidents, which were alarming but harmless.

The following sections offer more detailed analysis of potential techniques for detecting, tracking, and repelling UAVs.

2. Detection and Tracking

This section gives an overview of techniques that may be used to detect and track UAVs operating in restricted airspace. Merits and drawbacks of each technique are noted.

2.1. **Conventional Surveillance: Radar and Beacon Transmitters.** Conventional aircraft surveillance techniques are based on radar and beacon transmissions from aircraft. The latter either respond to ground interrogation (as with secondary surveillance radar) or are broadcast from the aircraft without interrogation (as with ADS-B) [[1], Ch. 5].

2.1.1. *Advantages.*

(1) Primary surveillance radar (PSR) and secondary surveillance radar (SSR) systems are already installed at major airports across the U.S.
(2) PSR does not assume any cooperation from the target and so is well-suited for detecting malicious intruders.
(3) If an incoming UAV is broadcasting ADS-B squitters, detecting and tracking it would be trivial.

2.1.2. *Drawbacks.*

(1) UAVs do not typically carry SSR beacons, and it would be wishful thinking to expect Category 3 UAV intruders to be equipped with functioning ADS-B beacons.
(2) UAVs whose structure is made of poorly-radar-reflective materials (e.g., a fixed-wing glider made of Styrofoam) and having a wingspan less than a few meters would not be visible to PSR or would be hardly distinguishable from birds or bats. Moreover, UAVs flying at an altitude of less than 100 feet would be difficult to detect by PSR.

2.2. **Acoustic Sensing.** The motors of electric-powered rotorcraft and fixed-wing UAVs emit a characteristic whine that can be used to detect such UAVs. Gas-powered UAVs also exhibit a characteristic acoustic signature.

2.2.1. *Advantages.*

(1) Low cost, even when implemented as a network of sensing devices placed around the protection perimeter.
(2) Can be highly effective when combined with electro-optical sensing to distinguish UAVs from electric weed whackers.
(3) Forces a UAV wishing to evade detection to execute final approach as a glider or a free-falling rotorcraft.

2.2.2. *Drawbacks.*

(1) Leads to false positives due to electric weed whackers or spoofing via playback of an audio recording of a UAV if not combined with other sensing modalities such as electro-optical sensing.
(2) Incapable of detecting fixed-wing UAVs operating as gliders or rotorcraft UAVs in free fall.
(3) Unlikely to offer reliable detection at more than a 500-meter standoff range.

2.3. **Radio Emission Sensing.** UAVs typically send data back to their controller through a wireless data link. Using a directional antenna or a network of synchronized ground stations, such emissions can be detected and located [2].

2.3.1. *Advantages.*

(1) Can offer effective detection and accurate tracking of multiple UAVs with arbitrary emitted waveforms if the UAV emissions are sufficiently persistent and powerful.

2.3.2. *Drawbacks.*

(1) To be economical and offer rapid detection, the system must have some knowledge of the emission center frequency and bandwidth.
(2) Easily evaded by a UAV operating under radio silence, which would be trivial for a Category 3 attacker to implement.

2.4. **Electro-Optical Sensing.** Electro-optical (EO) sensors in the form of cameras that are sensitive to visible light or infrared radiation can be quite effective at detecting and tracking UAVs.

2.4.1. *Advantages.*

(1) An EO sensing network can be built from small, low-cost sensors with only mild synchronization requirements. The network could be geographically large (e.g., it could cover the area around the White House and the U.S. Capitol in Washington D.C.), which would increase the chance of detecting and the accuracy of tracking an overflying UAV.
(2) Infrared EO sensors can detect the warm motors or batteries of UAVs day or night and, with proper pattern recognition, would likely be reliable in distinguishing UAVs from birds, bats, and insects.
(3) A network of EO sensors can offer full three-dimensional target tracking.

2.4.2. *Drawbacks.*

(1) The author is not aware of a commercial networked EO system that can provide 3-d UAV tracking and distinguish UAVs from wildlife. But there do not appear to be any serious technological roadblocks that would prevent such a system from being developed and deployed.
(2) It is unclear what the effective range of an infrared sensor network could be. This will depend on the strength of thermal emissions from a UAV and on the pattern recognition algorithm tasked with distinguishing the UAV from wildlife.

3. Electronic Defenses

For typical operation, UAVs capable of autonomous flight rely on two vital wireless links: the command link to the operator and the (passive) navigation signal link to overhead GPS/GNSS spacecraft [3]. In the event of a UAV attack, a defender can attempt to disrupt these links or feed false signals to the UAV's radios [4].

3.1. **Command Link Jamming and Appropriation.** Modern commercial UAVs are controlled by one or more wireless links to the operator's control equipment. Traditional RC controllers are still used as a backup means of control even for UAVs capable of a high degree of autonomy. These controllers send low-level commands to the autopilot system or directly to the UAV motors or to the servos that actuate the aircraft's control surfaces. These transmitters typically operate in unlicensed bands (often 2.4GHz), but do not typically use WiFi/802.11 protocols, preferring direct-sequence spread spectrum (DSSS) or frequency-hopped spread spectrum (FHSS) protocols that offer a large number of independent channels.

For control at a higher level of abstraction, a control station may communicate with a UAV independent of the RC controller. Like the RC controller, this link is often established within unlicensed bands. For example, the popular DJI drone establishes this link in the 2.4 GHz band using a standard WiFi/802.11 protocol. This link facilitates video downlinking and general control functionality such as parameter setting and high-level trajectory control.

In defending a sensitive site from UAV intrusion, a defender may attempt to jam or appropriate the command link.

3.1.1. *Advantages.*

(1) Command link jamming or appropriation is an effective means of denying a hostile operator the ability to execute an RC-controlled visual line-of-sight UAV attack or a first-person-viewer (FPV) UAV attack.
(2) Command link jamming forces an attacking UAV to operate independently from its human operators.
(3) Command link appropriation can enable a defender to obtain full control of an intruder UAV.

3.1.2. *Drawbacks.*

(1) Although the signals from today's commercially-available RC controllers are not encrypted or authenticated, the UAV is paired with the RC controller in such a way that the two agree on a communications channel selected from a large number (e.g., 100) of possible channels. Thus, to appropriate the RC link, a defender would need to determine at least (1) which communications protocol is being used (e.g., DSSS or FHSS), (2) which channel within the protocol is being used.
(2) Although the command and data link to the control station is not typically encrypted or authenticated, it can be encrypted with well-established cryptographic algorithms using openly available software [1], rendering appropriation of this link difficult at best.
(3) To avoid the effects of command link jamming or appropriation, an attacking UAV can simply transition to an autonomous operational mode soon after takeoff, accepting no further external commands.

3.2. **GPS/GNSS Interference.** Virtually all modern commercial UAVs capable of autonomous flight exploit navigation signals from overhead GPS satellites. The UAV's satellite navigation receiver may also be capable of exploiting signals from other Global Navigation Satellite Systems (GNSS) such as the European Galileo system and the Russian GLONASS system. It is well known that civil GNSS

[1] See, for example, `http://phantommods.info/effect-on-wifi-encryption-for-fpv-range/`

signals are weak and, to date, unencrypted and unauthenticated [5], although proposals exist to insert digital signatures into the broadcast GPS and Galileo navigation data streams [6, 7, 8]. In the face of a deliberate UAV attack guided by GNSS signals, a defender could take advantage of the weak security of GNSS signals to confuse or commandeer the attacking UAV.

3.2.1. *Advantages.*

(1) Three-dimensional hostile control of a UAV via GPS deception (spoofing) is possible: it has been demonstrated in the laboratory and in a government-supervised experiment at White Sands Missile Test Range [4].
(2) Even if the location of an incoming UAV is known only very approximately (e.g., it is only known that a UAV is approaching the White House grounds from the southwest), GPS deception can be effective at repelling an attack. If one sectorizes the area around the site to be protected into 4 quadrants, each quadrant covered by a directional transmission antenna, then a UAV approaching under GPS guidance, or a group of UAVs, can be made to believe it has overshot its target, causing the UAV to slow and eventually proceed away from the target site as if facing a stiff headwind. The University of Texas Radionavigation Laboratory recently demonstrated this defense in the laboratory against the GPS receiver used in a large number of commercial UAVs.
(3) Persistent and powerful GNSS jamming would force attackers to operate either by (1) line-of-sight (LOS) RC control, (2) first-person viewer (FPV) control, or (3) non-GNSS autonomous navigation. LOS control exposes the operator to visual detection and recognition. LOS and FPV control can be denied by control link jamming. And non-GNSS autonomous navigation in an unmapped environment is either expensive (e.g., a navigation- or tactical-grade INS initialized with GNSS), can only be applied accurately over short time intervals (e.g., a MEMS-grade magnetometer-disciplined INS [9]), or still in the research stage (e.g., autonomous visual navigation [10]).

3.2.2. *Drawbacks.*

(1) Persistent and powerful GNSS jamming would cause substantial collateral damage, denying the use of civil GNSS in a wide area around the protected site, which possibly encompasses airports [5]. Powerful GPS jamming around the White House, for example, would deny GPS aiding to commercial aircraft at nearby Reagan National Airport. Such jamming would alter civil operational procedures in the area: automobile commuters would be denied use of their in-car navigation systems, cell towers could no longer be synchronized by GPS, and approaches to airports could no longer benefit from GPS for safety and efficiency. While it is not out of the question to engage in powerful GNSS jamming to protect extremely sensitive sites such as the White House, it is the opinion of the author that this would need to be a last resort. It would need to be carefully coordinated with the DOT and DHS.
(2) Even intermittent GNSS jamming powerful enough to deny UAV use of GNSS would be problematic for the surrounding civil infrastructure. UAV GNSS receivers are typically high-sensitivity receivers capable of operating at carrier-to-noise ratios (CNRs) as low as 15 dB-Hz (e.g., [11]). By contrast, the GPS receivers used in commercial aviation typically fail to track signals below a CNR of 29 dB-Hz. Therefore, to effectively jam a UAV located 1 km from the White House would require a jamming power that would also effectively deny GNSS to a commercial aircraft along the same line of sight more than 5 km from the White House.

(3) GNSS spoofing would potentially be even more damaging to surrounding civil systems than GNSS jamming, and thus would need to be carefully coordinated with the DOT and DHS. Moreover, to be absolutely reliable, a GNSS spoofer would have to create simulated signals for all available civil GNSS, including Galileo and GLONASS.

(4) An attacking UAV can simply disregard GNSS signals during the final approach to the target, relying, for example, on a low-cost magnetometer-disciplined MEMS-grade inertial navigation system, which, over a 60 second interval, may only exhibit a 5-meter drift in perceived location [9].

4. Kinetic Defenses

Kinetic defenses encompass all techniques that involve mechanical contact with the UAV intruder such as interceptor UAVs, rubber bullets, shotgun shot, or nets.

4.0.3. *Advantages.*

(1) Net capture of UAVs by interceptor UAVs has been demonstrated (though it cannot yet be considered a mature technology). Net capture has the additional benefit of enabling eviction of the intruder UAV from the vicinity of the site to be protected.

(2) Commercial UAVs are, in general, fragile in the face of kinetic attacks.

4.0.4. *Drawbacks.*

(1) All kinetic defenses require reliable detection and accurate tracking of the UAV intruder.

(2) Hard-contact kinetic defenses such as collision with an interceptor UAV may cause an intruder UAV carrying an explosive payload to explode.

(3) Interceptor UAV technology is currently immature.

5. Acknowledgments

The author is grateful to Mark Psiaki, Christopher Hegarty, Andrew Kerns, Nathan Green, Michael Szmuk, and Daniel Shepard for insightful conversations on how to protect critical civil sites from UAV intrusion.

References

[1] K. Wesson, *Secure Navigation And Timing Without Local Storage Of Secret Keys*. PhD thesis, The University of Texas at Austin, May 2014.

[2] J. A. Bhatti, T. E. Humphreys, and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Proceedings of the IEEE/ION PLANS Meeting*, pp. 1209–1220, April 2012.

[3] K. D. Wesson and T. E. Humphreys, "Hacking drones," *Scientific American*, vol. 309, no. 5, pp. 54–59, 2013.

[4] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[5] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing." `http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf`, July 2012.

[6] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[7] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[8] I. F. Hernandez, V. Rijmen, G. S. Granados, J. Simon, I. Rodriguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service," in *Proceedings of the ION GNSS+ Meeting*, 2014.

[9] O. Woodman, "An introduction to inertial navigation," *University of Cambridge, Computer Laboratory, Tech. Rep. UCAMCL-TR-696*, 2007.

[10] G. Chowdhary, E. N. Johnson, D. Magree, A. Wu, and A. Shein, "GPS-denied indoor and outdoor monocular vision aided navigation and control of unmanned aircraft," *Journal of Field Robotics*, vol. 30, no. 3, pp. 415–437, 2013.

[11] u-Blox, *Datasheet: NE0-6 GPS Module.*

The University of Texas at Austin

E-mail address: `todd.humphreys@mail.utexas.edu`