## Arising Privacy Concerns of Hacking Drones and Mitigation

## Nathan Barker

## Air Force Institute of Technology, WPAFB, Untied States of America

## Nathan.barker@afit.edu

**Abstract**

Drones are opening an attack space that once was mitigated, by physical security. The growing capabilities and falling cost of commercial drones are a root cause. We use walls, fences, and gates to prevent unauthorized access to buildings. All these physical security measures also serve as a deterrence for would be attackers. If they are caught trying to circumvent them, they can be pursued and captured. One of the keys to circumvention of physical preventative measures is surprise and knowledge of vulnerabilities. For a technical savvy adversary, drones are an ideal solution to overcoming physical obstacles and the radio frequency spectrum is a particularly susceptible attack vector that can be exploited to great effect through them. Wi-Fi, Bluetooth, and cellular technology are things most people use every day. But, they emit signals that can be intercepted. Through this leakage of information, people can be tracked, networks can be mapped, and vulnerable devices can be hacked. Drones can provide a low cost of entry for these sorts of attack. The consequences for capture are lowered and can provide intelligence while leaving little to no footprint.

Over the last several years it has become clear that drones are presenting an increasing number of privacy concerns and there is a need for mitigation. This paper’s research aims to investigate the rising privacy concerns these devices present, why the radio frequency spectrum is particularly susceptible attack vector and make suggestions on how mitigation should be handled for these new privacy concerns. The current defences available to disrupt, capture, and destroy drones are deployable nets, jammers, counter drones, EMPs, lasers, projectiles, etc. Unfortunately, many of these defences are outlandishly expensive and others are not feasible in all the environments we operate in. Rather than focus on active defences, I hypothesize that security by denial is a more effective solution for mitigation of malicious drones using the radio frequency spectrum. Hardening building with radio frequency shielding is an ideal solution. This is something that can be applied on the governmental, commercial, and civilian level. But, first to be accepted the need must be communicated.

**Keywords**

Drones, Privacy, Radio Frequency, Mitigation,

# INTRODUCTION

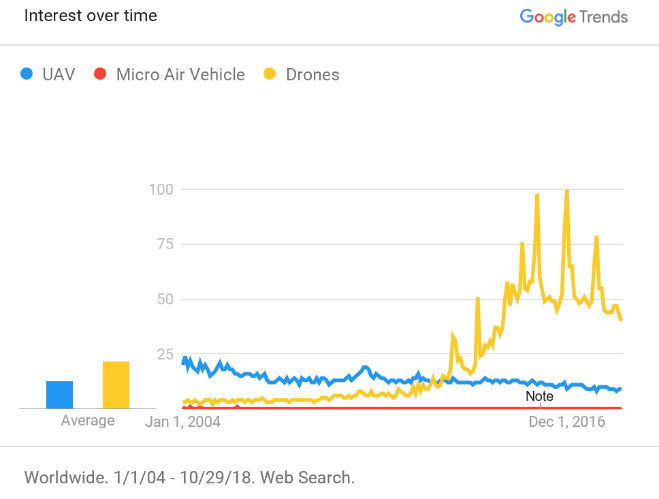
## What are drones?

Drone is a broad term that has been used in conjunction with unmanned aerial vehicles (UAVs). The magnitude of their sizes varies from mere centimetres [1] all the way to full scale planes with over one hundred foot wingspans [2]. For the purpose of this paper we will use the term drone to describe the small scale consumer accessible UAV. We will also identify several subsets of drones. Small Radio Controlled (RC) drone products have been available to the public for many years, but more recently have gained popularity due to several advancements in technology. One of the most popular subsets of drones are multi-rotor drones. There are also single-rotor, fixed wing, and hybrid drones. Drone use today ranges widely. They are used for farming, surveying, entertainment, sports, package delivery, and videography. The list continues to grow each year. Some of the most popular drones available today are camera equipped or capable.

## Starting Point

UAVs have been of great interest to the United States Military for many decades now, but rapid development only began after the U-2 downing incident over the Soviet Union [9]. The progressive developments now have been used with great success in multiple campaigns. But, the rate of development of UAVs has not been consistent. Despite this, the developments by the US eventually lead to the research of a new class of UAVs.

MAVs popped onto the scene in the mid to late 1990s, prompted by the United States Defence Advanced Research Projects Agency (DARPA) [7]. A few of the many developments are Lincoln Laboratory’s fixed wing MAV [3] and Georgia Institute of Technologies’ study of vertical take-off and landing (VTOL) with a MAV [4]. The motivation for this research was for them to provide a military capability that was cheap and disposable. These first explorations of MAVs were not exclusively rotor driven, but also included fixed wing vehicles and insect/animal like flapping wing vehicles [8]. From the multi-phase MAV program that DARPA initiated, several high quality UAVs for the time were produced. Two of those UAVs are the T-Hawk and Wasp [10].

**Figure 1:** "Data source: Google Trends(<https://www.google.com/trends)>."

## Consumer Drone Boom

The term, “Micro Air Vehicles” never matched the popularity of either “UAV” or “Drones” according to Google Trends. But the divergence of interest in the term UAV and Drones began in the late 2000s. This is when drones came to the consumer forefront. A few of the technologies that spurred along the popularity of drones in the consumer market was the development of better brushless motors [5] and lighter weight batteries [6]. With these developments useful and more advanced hobby drones began to emerge. Starting in 2011, drones popularity began peaking in Google’s searches each holiday season.

## Performance Increases

**Table 1: DJI Phantom Specifications**



Helpful insight into the development of consumer drones can be found by looking at the specifications of one of the most popular drone companies. DJI produces the Phantom model drones for videography. Listed above is a table of the specifications of their models. As the release years progress, you can see that the weight, distance, and flight time all have been increasing. In fact, they are now meeting and exceeding some of the performance goals of the original MAV developments, like Lincoln Laboratory’s fixed wing MAV [3].

# Privacy and Hacking Concerns

## Video Taping and Taking Pictures

One of the more prevalent concerns with consumer drones is the ability to spy on locations outside public view. With drones now widely available and many of the popular consumer drones being equipped with high definition cameras, we continue to hear of these devices being abused. It has been reported by Mary Papenfuss from the Huffington Post, a couple was arrested in Utah after the police obtained the drone they had been using to film people in their homes. Another report from Carter Evans at CBS News pointed out that paparazzi were using drones to photograph celebrities. One final example comes from Eric Geller at the Daily Dot, a fan filmed parts of Star Wars: episode VII being shot in England and uploaded them to YouTube. If this much trouble can be caused by civilians, you can begin to appreciate the magnitude of the problem. Malicious actors could use drones to conduct surveillance on restricted areas like testing facilities, military bases, prisons, and more.

## Tracking

{TODO}

## Mapping Our Networks

Another concern can be derived from the work of Captain Law from the United States Air Force. His thesis is on the use of a direction antenna to locate and map different wireless access points out of audible range. The intent of this research is to be expanded on by mounting the antenna to create a drone-mounted wireless attack platform. The proof of concept was a success and shows us that it is possible for drones to maintain a certain level of stealth when preforming radio frequency surveillance and attack. The combination of drones taking high quality photographs and mapping access points, could give adversaries of companies, governments, or individuals a comprehensive view of their targets. With the commercial drones that now have the communication distance of more than 3 miles, it must be assumed that any radio frequency signal is susceptible to interception.

# Active Mitigation Techniques

## Jamming

Devices can be used to block signals controlling drones and are known as jammers. Jamming is a very effective way of taking drones out of the sky that use radio frequencies or GPS for navigation. However, in the United States it is illegal for individuals to jam these signals. While these may be ideal solutions for government entities, they are not a solution available to the general public or large companies. An example of this technology can be seen from the company Battelle. They have developed a gun that emits pulses of radio waves to disrupt both GPS and radio control signals. These are the two most prevalent kinds of signals that are used for drone control. The blockage of control signals removes the pilot from control and forces the drone to either land or crash.

## Netting

Some companies have created very agile drones to chase and capture enemy drones via a net. Other companies have gone with a deployable net approach. Each of these techniques can be successful in incapacitating a drone, but will not stop signals from being sent and received by a drone. They also require someone highly skilled to operate. One example of such system is Search Systems’ SparrowHawk drone. It is a drone armed with a net that once used for a capture can be released to the ground safely with an attached parachute. For the deployable net approach, OpenWorks’ Skywall 100 shoots projectiles carrying nets that parachute to safety upon capture. The biggest downfall of these systems is the cost and need for a highly capable pilot to operate successfully.

## Lasers

{TODO}

## Etc

{TODO}

# Radio Frequency Shielding

## Security by Denial

All of the active mitigation techniques have their own strengths and weaknesses. But, all of those techniques require the discovery of an adversary and cannot ensure that no signals were intercepted or an attacker’s job was not completed before capture. For this reason, I suggest the promotion of radio frequency shielding in buildings as a standard and a campaign to inform civilians and businesses alike of these immerging threats. This is a passive defence and once in place does not need manning or excessive maintenance. If buildings are hardened and citizens are informed, unintended wireless leakages can be reduced. In turn this, will hamper the use of drone-mounted wireless attack platforms and focus our defensive efforts elsewhere.

For a very long time the US government has recognized the threat of signals emitted from devices. The NSA has code named the signals threat as TEMPEST and it has been large part of the espionage world for many years according to, Friedman[18]. Buildings that handle classified material must meet certain criteria to be certified and one of the shields they employ is against radio frequency. Due to high rate of corporate espionage throughout the world, companies have begun to follow the governments lead and harden their buildings.

## Different Options

{TODO}

## Informing the Public

As of now, outside the US government, some of our allies, and commercial clients there is not much demand for radio frequency shielding. For this technology to be widely adopted it will be important to lower the cost through demand and create that demand by announcing the privacy concerns clearly. Everyone is susceptible to wireless attack at some point and the public even more so.

## Shortfalls

{TODO}

# Conclusion

Drone technology introduces a wide gamete of potential risks. One of these emerging threats is invasion of privacy and exploiting wireless signals. While these are not the only threats adversaries may take advantage of, they are problems that we have an effective solution for in use by the government and some large companies. With the proper education and promotion of these techniques, I believe we can effectively mitigate the threat of hacking drones.

**TO WATCH:**

<https://www.facebook.com/techstars/videos/vb.14729035542/10160129352215543/?type=2&theater>

<http://afwerxdc.org/wp-content/uploads/2018/04/Press-Release-TS-AT-Demo-Day.pdf>

**References**

[1] Smallest Quadcopter Drone

<https://aerixdrones.com/products/aerius-the-new-worlds-smallest-quadcopter>

[2] Global Hawk Fact Sheet

<https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/>

[3] Davis, W.R., Kosicki, B.B., Boroson, D.M. and Kostishack, D.E., 1996. Micro air vehicles for optical surveillance. *Lincoln Laboratory Journal*, *9*(2), pp.197-214.

[4] Morris, S.J., 1997, February. Design and flight test results for micro-sized fixed-wing and VTOL aircraft. In *Proceedings of the First International Conference on Emerging Technologies for Micro Ai Vehicles, Georgia Institute of Technology, Atlanta, GA*.

[5] Murray, A., Kettle, P. and Moynihan, F., 1997, June. Advances in brushless motor control. In *American Control Conference, 1997. Proceedings of the 1997* (Vol. 6, pp. 3985-3989). IEEE.

[6] Yoshio, M., Brodd, R.J. and Kozawa, A., 2009. *Lithium-ion batteries* (Vol. 1). New York: Springer.

[7] Ammoo, M.S. and Dahalan, M.N., 2006, July. Micro air vehicle: technology review and design study. In *Proceedings of the 1st Regional Conference on Vehicle Engineering & Technology, Kuala Lumpur, Malaysia.*

[8] Pines, D.J. and Bohorquez, F., 2006. Challenges facing future micro-air-vehicle development. *Journal of aircraft*, *43*(2), pp.290-305.

[9] Longino, D.A., 1994. *Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios* (No. AU-ARI-92-12). AIR UNIV MAXWELL AFB AL AIRPOWER RESEARCH INST.

[10] Prabhakar, A., 2015. Breakthrough Technologies for National Security. *Defense Advanced Research Projects Agency (DARPA), Tech. Rep.*

[11] Guri, M., Zadov, B. and Elovici, Y., 2017, July. LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 161-184). Springer, Cham.

[12] https://www.huffingtonpost.com/entry/peeping-tom-drone\_us\_58a6847fe4b045cd34c03e56

[13]<https://www.cbsnews.com/news/paparazzi-take-to-the-skies-to-pursue-stars-with-drones/>

[14] https://www.dailydot.com/parsec/star-wars-set-filmed-drones/

[15]<https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS-technologies/dronedefender>

[16] Mellendick, R. (2018). Corporate America is Being Attacked and the Entry Vector May Be Surprising. *United States Cybersecurity Magazine*, [online] (Fall 2014), pp.72-73. Available at: https://www.uscybersecurity.net/csmag/corporate-america-is-being-attacked-and-the-entry-vector-may-be-surprising/ [Accessed 18 Nov. 2018]. [17] Mellendick, R. (2018). Wireless Security: Not just 802.11 Anymore. *United States Cybersecurity Magazine*, [online] (Spring 2014), pp.9-10. Available at: https://www.uscybersecurity.net/csmag/wireless-security-not-just-802-11-anymore/ [Accessed 18 Nov. 2018].

[18] Friedman, J., 1972. Tempest: A signal problem. *NSA Cryptologic Spectrum*, *35*, p.76.

[19] https://www.wired.com/story/watch-anti-drone-weapons-test/