Drones Within the Federal Government

Summary of Roundtable, hosted by ATARC in August 2022

WHITE PAPER

Emerging technologies are evolving faster than ever, creating revolutionary opportunities for Government agencies to collect data and serve the public in new modern ways. Some of these applications, however, also present a host of challenges, including significant security implications.

Drone technology has greatly impacted day-to-day mission delivery at many agencies. Once found only on the battlefield, drones are now used for various non-military applications across the Federal Government. The use cases range from public safety to research, often replacing human workers in hazardous environments.

However, domestic drone production lags behind other countries, especially China. Drone operators frequently prefer the more user-friendly foreign-made devices to their American-manufactured counterparts. While restrictions on DJI have hurt the front-running Chinese drone giant, the company maintains 54% of global market share, says DroneAnalyst.

To encourage a government-wide open conversation, ATARC recently hosted a roundtable on using drones in government work. Experts across several State and Federal agencies and industry shared insights about the obstacles and challenges of using drones safely within and beyond their entities.

Current State of Drone Use in Agencies

Participants at the roundtable shared how drones had changed their day-to-day work. All agreed that there is much broader variety of use cases than their traditional military and surveillance use.

The devices are frequently used to work in or monitor hazardous or hard-to-access areas. For example, moving toxic material samples, taking measurements, searching for victims and survivors, and so on. Of course there are many public safety uses: law enforcement has turned to drones as it is far more cost-effective than the traditional helicopter patrol.

Drones – More than Just Aerial Vehicles

Undoubtedly, the wide variety of potential drone use cases in government work has created a lot of excitement. However, participants also noted that the surface level enthusiasm might obstruct a more holistic view of incorporating drones.

Leveraging drones for their aerial capabilities is an easy, but limited approach. Drones capture an incredible amount of data, making them as lucrative of a target for cybercriminals as the traditional smart device. Consequently, drone use by Government agencies should be treated no differently than an Internet of Things (IoT) device. It is critical to understand where and how drone-sourced information is being transmitted, to avoid the security risk of sending massive amounts of data to foreign based or otherwise ill-natured platforms.

Balancing Innovation and Security

While using Chinese-made drones presents serious security concerns, participants acknowledged that the U.S. drone market still has a considerable amount of work to do to catch up to their Chinese counterparts. One the one hand, they expressed a desire to transition to American-made drones, or at the minimum implement a more formal device authorization process. On the other, they recognized the potential impediment to the agency's mission if suddenly banned to use "unauthorized" drones.

Manage Risks in Drone Use

Participant recommendations to limit the risk of drone use:

- Consider drone insurance to limit liability
- Know how and where data is being stored
- Vet, train, and certify all drone operators
- Screen vendors for integrity and expertise
- Communicate openly with the public about intended drone use

A logical compromise might be to 'lock down' the drone with limitations on data collection and transfers. However, participants noted that this often renders some functionality useless, to the detriment of the mission.

Agencies looking to use drones need to make a managed risk decision if they cannot find suitable domestic options, participants agreed, and recommended weighing value to the mission against potential security risks. Using unauthorized drones for gathering and transmitting non-sensitive data may not present a huge issue. However, law enforcement will need to be far more careful when incorporating foreign-made drones into their fleet.

Acknowledging Public Concern

Agencies cannot ignore public concern over government drone use. Justified or not, some constituents will always approach this with high suspicion. With local law enforcement already embracing aerial surveillance by drone, the absence of a federal framework to govern the technology and its use is triggering much discussion about regulating these activities.

Other participants pointed to the vast data pool created by drones as a potential resource for conducting citizen science. This additional value demonstration could help change the perception of how drones are used in the Federal Government.

Drone Safety

Participants ended the roundtable discussing how to operate drones securely and safely. While drone use has increased dramatically over the past few years, the level of piloting proficiency has not.

Flying an airplane requires hours of training and pilots must pass regular mental and physical fitness checks. Meanwhile, becoming a licensed drone operator is simple. Current regulations only require that a drone be registered, with no proficiency requirements.

Unlike the dozens or hundreds of hours of experience commonly possessed by an airplane or helicopter pilot, a drone operator may have just started flying that day. This is by design: most drones are built to grow with the operator, all but flying themselves at the beginning. The operator will begin to control more of the drone's flight as he or she becomes more proficient. As a result, no level of proficiency can be assumed, just because a drone is in the air.

Safer Drone Operations

Participant suggestions to promote drone operation safety:

- Enable and prioritize training. Drones suitable for government use are more complicated to operate than consumer-grade models. They should be treated more like small airplanes – with significant proficiency required for safe operation
- •Enforce a screening process for drone operators. Consumer drone manufacturers have popularized the term "pilot," but most drone operators have far less experience than airplane pilots. Most operator applicants will likely have little to zero training in non-commercial drone operation
- •Equalize drone mishaps with other types of work accidents. Consider drone insurance to protect all parties from potential liabilities

Promoting Drone Use in Federal Space

Drones are an exciting new opportunity for Local, State, and Federal government agencies to advance their missions to serve constituents. This roundtable is only the beginning of an effort by ATARC and its public and private partners to kickstart a government-wide discussion on drones and encourage secure and effective adoption.

In addition to future drone focused events, we are pleased to announce the creation of the Drone Working Group, which aims to promote agency cross-collaboration and cooperation in developing guidelines and best practices for the safe and secure use of drones.

Please contact workinggroups@atarc.org for more information and to join!