Commercial and Personal Drone Usage Abroad

Date Published: September 18, 2025

Summary

Unmanned Aircraft Systems (UAS), also known as Unmanned Aerial Vehicles (UAVs) and drones, are becoming ubiquitous across the world. Rapid advancements have made these systems portable, lightweight, and multifaceted, allowing for numerous business and personal functions. However, regulations around the transport and usage of drones and threats associated with their security have resulted in an international patchwork of risks to business operations and travelers' security. This report examines the risks associated with commercial and personal uses of UAS and provides recommendations to mitigate these risks.

Commercial Drone Usage

Advancements in the size, range, and capabilities of UAS continue to appeal to the private sector, and the systems often present a cost-effective and easy way to deploy new technologies. Natural resource companies use drones equipped with scanning technologies to identify above and below-ground resource deposits. Shipping companies offer drone delivery services. Manufacturing firms may use drones for engineering projects and autonomous assemblies, and many companies across sectors are using drones as surveillance and security tools. For commercial facilities, drones can be used to scan surrounding areas for threats, to visualize damage from vandalism or attacks, and to identify suspicious individuals in or around their area of operations.

However, many foreign governments either partially or totally restrict the deployment of commercial UAS. Barbados, Nicaragua, and Egypt have outright banned the use of commercial or personal drones. In Bahrain and Kuwait, the import of drones is heavily regulated with significant penalties for non-approved commercial use. In Kenya and India, only citizens can operate UAS, and these countries require certificates for operators that make commercial usage expensive and tenuous.[1] Because of this non-standard legal framework, organizations that operate in multiple countries should work closely with local government contacts to determine the legality of drone operations; simply importing UAS for commercial use can result in detainment, arrest, and heavy fines.[2]

Once commercial UAS arrive in a foreign country (whether imported or purchased locally) and are permitted for use, they remain susceptible to threats. Thieves may steal drones, giving them access to proprietary hardware or sensor data, and malicious actors may follow drones to identify critical infrastructure, new commercial projects, or executive staff members. Aside

[1] Yahoo Finance, *19 Countries Where Drones are Banned*, August 2023.
[2] Embry-Riddle Aeronautical University, *Civil Aviation Authorities by Country (by Region) / UAS Law*, 2023.

from physical risks, even commercial-grade drones can be susceptible to cyber-intrusions. Some UAS can be remotely accessed, and once compromised, can be taken over and flown by a third-party. Their data can be mined, giving hackers access to video/sensor and location information. Drones, especially those that connect to an organization's Wi-Fi or physical hardware devices, can be weak points for hackers to access private networks. UAS manufactured overseas may also be equipped with backdoor access, allowing the manufacturer or other entities access to the drone and its data. For these reasons, many organizations, including the U.S. Army, operate drones from dedicated (and separate) servers, and some have banned the use of foreign-made UAS.

Personal Drone Usage

UAS have several personal uses including photography, videography, and deliveries. With many nations regulating personal drone imports even more strictly than commercial import, bringing UAS to foreign nations presents a risk of detainment, arrest, or seizure. In nations where drones are permitted for individual use, it should be noted that some locales, especially around airports or military installations, have heavy restrictions on usage.

When used in approved spaces, drones can be a useful tool in taking aerial photography. However, personal-use drones are often manufactured with fewer security features, making them more susceptible to cyber-attacks.[3] Drones are often targeted by criminals for theft, and UAS usage sometimes indicates a level of wealth that may attract petty criminals.[4] Coupled with the focus and effort required to fly many drones, usage may expose travelers to an increased risk of experiencing burglary or robbery.

Private-Sector Impact

Commercial UAS are an exceptional tool for reconnaissance, surveying, and autonomous deliveries. However, OSAC members should take steps to be well informed of the local criteria to import drones and should consider contacting local governments to clarify any regulations. Having clear lines of communication with local governments may also reduce the risk of breaking usage regulations. Consider the following:

- Once in use, critical information should never be stored on UAS.
- Avoid connecting drones to personal devices when possible.
- Additional steps should be made to ensure drone footage and software is only accessed on secure networks, and OSAC members should consider the origin of their UAS.

[3] John Hopkins University, *Scientists show how easy it is to hack a drone and crash it*, June 2016.
[4] Aerial Defense, *International Stolen Drone Database*, 2025.

- Drones should be carefully flown and landed.
- UAS should be launched from a secure location to reduce the risk of theft.
- Both commercial and personal drone pilots should take considerations to obscure launch/landing locations as well to avoid being perceived as wealthy, especially in countries with high petty crime rates.
- While some countries require insurance on drones, OSAC members should consider purchasing full-value insurance on UAS.

Additional Information

Please see OSAC's report on Drone Threats Abroad.

For more information on this topic, please contact OSAC's regional teams.

- OSACAsia@state.gov
- OSACEurope@state.gov
- OSACMENA@state.gov
- OSACAfrica@state.gov
- OSACAmericas@state.gov