Major General (Ret.) Frederick F. Roggero, USAF
President & CEO Resilient Solutions, Ltd.
Statement For:
The Subcommittee on Oversight and Management Efficiency
U.S. House Committee on Homeland Security, Chairman Michael McCaul, R-Texas
18 March, 2015
"Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies"

SECURITY ISSUES & POSSIBLE SOLUTIONS FOR HOMELAND SECURITY AND LAW ENFORCEMENT

The Current Environment

Aviation is undergoing a global revolution. With advances in unmanned system technology that are moving at the speed of "Moore's Law," while their associated prices continue to fall, "Class 1" small, unmanned aerial systems (sUAS) have become high-tech, universally available tools. Coupled with advances in autopilots, telemetry, sensor and camera miniaturization, and corresponding increases in battery and engine capacities, sUAS's are delivering capabilities that were once only the purview of nation-states, corporations and wealthy individuals. Now, almost anyone can experience the advantages and thrills of aviation without ever leaving the ground, taking a flight physical, spending hours and considerable funds to hone a skill, or complete a rigorous training and certification processes. As these barriers-to-entry continue to fall, we will witness the democratization of aviation.

This combination of new, expanding, technologies delivers a limited version of the unique characteristics of aviation (speed, range, flexibility, and altitude) enjoyed by every air force directly to individuals and groups around the globe. And, as drone technologies improve, airpower concepts such as "stealth" and "air supremacy" could even become available to more common operators. It's true that sUAS are capable of making our lives better by helping us to imagine new, more safe, ways to do jobs that are dangerous, dull and dirty. They are also a terrific means to enhance commerce, save lives, gain different perspectives and even to provide recreation. But, as with all revolutions, there are risks that must be dealt with. And, the safety and security risks of small drones are no exemption. However, as the risk of these types of aircraft are reviewed, we must also strive to preserve and protect the overwhelming benefits that this rapidly expanding technology will bring for generations to come.

The risk inherent in the drone revolution can be divided into two sections – safety and security. Although the Academy of Model Aeronautics does a terrific job of providing voluntary safety standards, the exploding growth of this market means that many new recreational users of small drones simply do not understand that there is an aviation culture of safety. The days of the remote-control flying field with noisy gas motors and plenty of mentors is disappearing. The new group of "park flyers" haven't received education or training in safety, airspace, weather, air traffic control, emergency procedures, or even basic airmanship. Because of that, a few in this segment will eventually pose a safety hazard by unknowingly flying in areas that they are not allowed to operate, not out of malice, but because they simply do not understand the rules. But this type of safety risk can, and should, be dealt with through education, regulation, and enforcement.

Next on the ladder of safety risk are those drone operators that know the rules but decided to violate them. Perhaps they feel the need to test out the new technology, to see how high, fast or far it can go, or to obtain video from perspectives not allowed, usually for good reason. It is operators from this class that will most likely cause the first collision between an aircraft and a drone in the United States. But,

once again, standard, clear regulation and enforcement are the best remedies for these types of transgressions.

At this point, we move into the risks to our security. This revolutionary technology can be an affordable asymmetric tool for those who want to use its capabilities for illegitimate purposes. For less than $1,000 one could purchase a system that would allow you to conduct traditional "air force" missions, at limited, but still effective, levels of success. Tasks such as intelligence gathering, surveillance, reconnaissance, attack, and mobility can all be conducted with commercially available systems. These actions could be directed at national critical infrastructure points, factories, VIPs, military bases, prisons, large public gatherings, the borders, or simply, a neighborhood.

The Challenge

The U.S. government must be able to protect its sensitive critical infrastructure, personnel and citizens from the malicious use of small drones, while preserving the best aspects of using small sUAS's commercially and recreationally. There will be a balancing act as we deter, mitigate and defeat these types of security threats while preserving the benefits that sUAS's bring. Much work has already been done in this area by our international partners and allies and we should take advantage of those developed solutions and "lessons learned."

The Threat

Small UAS's are easy to make, cheap to buy, simple to fly, hard to detect, carry small versatile payloads, have a disruptive capability, and are evolving and proliferating quickly. "Lone Wolves," activists, thieves, terrorist groups, etc. could use this reliable and inexpensive capability to conduct intelligence gathering or execute missions against a variety of targets using explosives, chemicals, powder, etc. to deliver a disruptive attack via a single aircraft, or through more sophisticated coordinated, or multi-platform, attacks. Since 2013 smugglers have already tried to use the mobility capability of sUAS's to deliver 6.6 lbs. of crystal met across the Mexico-US border and to deliver tobacco and cell phones into a prison in Georgia and marijuana into a South Carolina prison.

And, we are not the only country to feel this threat. A July, 2013, NATO Industrial Advisory Group, Study Group 170, "Engagement of Low, Slow and Small Aerial Targets by Ground Based Air Defense," concludes that, "If appropriate measures are taken in the near future it will be possible to significantly mitigate the threat that LSS [low, slow, small] platforms pose to any future military conflict or from the terrorist attack of national infrastructure." Other NATO study groups have jumped into this issue, but participation by U.S. companies and the government in these ongoing studies appears underrepresented.

The United Kingdom took this threat so seriously in 2012 that the Royal Air Force, and Selex ES, designed and deployed an integrated counter sUAS system in London to defend the Olympic Stadium, particularly during the opening ceremonies. This system was further improved and used to defend world leaders during the 2013 G8 Summit in Enniskillen, Scotland, and, most recently, at the 2014 NATO Summit in Wales. Certainly, the lessons learned from these efforts should inform our actions as we address this common threat.

Roadmap Towards a U.S. Solution

Technology typically outstrips policies, and this technology has certainly stretched the capacity of the US government's bureaucracy to swiftly provide a counter drone strategy. Thus, we find ourselves behind

in strategy, policy, and the technological capabilities needed to counter-sUASs. Hence, this two-pronged problem requires a simultaneous, two-track solution.

First, a search should be conducted to find technology that has already been developed, tested, refined and used operationally. By using a combination of radar, networked electronic support measures, infrared, electro optical cameras, and engagement solutions of electronic attack, or hard kill options, the threat can be neutralized and the physical and electronic forensic evidence can be preserved for arrest and prosecution.

This system should consist of an integrated network of multiple layered means of defense to find, fix, track, identify and classify, then engage and assess the result. It should also be designed for persistent, low-profile surveillance and be operational 24/7/365. This system should also incorporate a rapid decision-making process that can be used to quickly prosecute a response since one of the unique abilities of sUAS's is to quickly close on a target with little notice. The system must also possess a range of "soft" and kinetic responses, both with a high "Probability of Kill." The counter system that is selected must also be able to capture and preserve the appropriate incident information that will inevitably be used for prosecuting the sUAS operators.

Additionally, the system must be able to fully operate without interfering with security, law enforcement, or first responder networks and communications. Thus, the system must be able to comply with Federal Communication Commission rules, if not operating under special rules for highly sensitive areas. The system should also have a variant that is mobile (man-portable and air-transportable) for temporary setups. Of course, the system must be designed with open architecture in order to allow for spiral, scalable and modular developments as drone technology continues to evolve (i.e., 5G LTE will almost immediately offer new capabilities to command and control drones). Finally, any system must be economically proportionate to the threat and available almost immediately.

The second step of this two-pronged solution starts with interagency cooperation to draft an overarching strategy and linked policies that have a legal and regulatory basis to deal with drones. A single department or agency should be charged with leading this effort using the experiences and lessons learned from our international allies as they have already wrestled with these issues. In any case, it will take a joined effort across all government departments since it will require navigating through current rules and regulations in the face of the unique capabilities of sUAS's and recommending changes to those base documents. For example, even though drones are unmanned, they are currently considered "aircraft" by the FAA and are protected by all of the laws and rules associated with manned flight when they are airborne. This is just one example of where current policy could severely limit options in reacting to a drone attack.

Once formalized, the overarching goals of the strategy and individual polices would then lead to identifying the correct supporting tactics, techniques, and procedures needed to guide security and law enforcement personnel during their response to any threat. The goal, of course, is to mitigate the safety and security risks while steering this technology towards its positive and productive uses.

Recommendations

1) Draft a single strategy and supporting policies that clearly guide government agencies in regards to Rules of Engagement and ensure that all responses are proportionate to the threat.
2) Simultaneously work with allies and international partners to discover "lessons learned" and best practices for solutions to the counter-drone issue.

3) Rapidly acquire proven technical solutions that can immediately provide protection to national critical infrastructure and personnel.
4) Train and educate federal law enforcement, and state and local law enforcement, personnel on the legal uses of drones, and potential threats.
5) Conduct a campaign to educate the public (sUAS operators and non-operators) on the use, and potential misuse, of drones.
6) Work closely with commercial drone manufacturers to install geo-fencing and traceability codes into drones of specific capabilities (i.e., size, weight, battery/motor size, flight times, etc.)
7) Draft appropriate legislation and regulations that govern the registration, licensing, etc. of any manufactured, or home-built, drone that fall above a specified weight and/or capabilities.
8) Establish, and fund, an on-going research and development program to devise counters to new drone technologies before they widely appear in the marketplace.

With last week's announcement by the Secret Service that the White House grounds would be used to conduct a series of exercises involving drones, it is clear the United States is not fully ready to deal with the threats that could come from this emerging technology today. However, there is a path to success. By capitalizing on "best practices" already discovered by our international allies, such as the United Kingdom, we could be ready to deal with today's threats immediately, while we draft the correct policies and spin up U.S. industries and laboratories to rapidly explore ways to counter tomorrow's drones and their unique, new, threats.