I. INTRODUCTION

The small unmanned aircraft systems (SUAS) threat is not emerging. It is real. It is international. It is varied. A quadcopter landed on the White House lawn.¹ A SUAS hovered in front of German Chancellor Angela Merkel while she stood on a public podium.² Numerous unidentified SUAS have conducted surveillance of French nuclear facilities.³ A man recently crashed his SUAS into the Empire State Building, asked Security to give it back, and live tweeted the entire event.⁴

Solving the SUAS threat problem, particularly in the United States (U.S.) homeland, is complex from a technological and legal standpoint. Technologically, the ability to accurately and timely detect, identify, track and respond to SUAS threats remains elusive, yet within reach. However, the legal, regulatory, and policy structures to enable SUAS threat response options have not kept pace with the technology. To date, the focus of legislators, regulators and policymakers has been on government actors, privacy and flight safety.⁵ Yet, the real threat in the homeland will come from non-government actors who wish to do harm.

This article explores both the technological and legal challenges in countering the SUAS threat. To do this, in Part II, we provide a brief overview of SUAS threat scenarios. In Part III, we discuss possible detection and response options, including their shortfalls and areas for further exploration. In Part IV, we view the legal and policy challenges related to responding to the SUAS threat through the lens of a U.S. domestic military installation commander to illustrate how laws, regulations, and policies are not currently suited to address the problem in a meaningful way. In Part V, we conclude by summarizing the complexity of the SUAS threat problem and suggesting a cross-disciplinary, inter-agency and public-private approach to enable protective actions within an appropriate legal framework.

II. THE THREAT

What started as a radio-controlled aircraft hobby has evolved into an inexpensive and effective means to project force. Today, SUAS pose a burgeoning threat, defined by their mechanical characteristics as well as the nature of air power.
The SUAS threat is diverse. As witnessed on battlefields throughout the past century, air forces have played an increasingly pivotal role in warfare. However, with the increasing prevalence of SUAS, the advantages of airpower, such as mobility, speed, range and altitude, is no longer solely within the province of a nation-state’s air forces. As SUAS become increasingly functional and affordable, the barriers to entry into the world of aviation will continue to decrease. As a result, we are witnessing the democratization of aviation, and with it, the democratization of the threat. Today individuals have access to the same tactical advantages traditionally reserved for a nation’s air forces, without the same training, flight discipline, or ethos.

Additionally, the same enablers and capabilities that make SUAS so versatile and valuable for a multitude of benign uses also make them potentially dangerous. New and innovative uses for SUAS have spurred the growth of technologies that enable data driven decisions. As a result, SUAS are now able to sense, access, and transform information. One unintended consequence of the democratization of aviation: surveillance in private hands. In the summer of 2014, when the Los Angeles Air Force Base was placed on lockdown due to reports of a suspicious man carrying a large bag on base, a local man decided to fly his SUAS over the base to watch the events. An amateur journalist imaging a crime-scene with a SUAS might be considered a harmless use of UAS technology; however, imaging critical infrastructure or national leaders for unknown purposes provides cause for concern. That same year, for example, multiple coordinated SUAS flights breached restricted air space over thirteen of France’s nineteen nuclear power plants. In another SUAS surveillance incident, German Chancellor Angela Merkel was speaking during a campaign event when a SUAS hovered in front of her and several other leaders, before it crashed to the ground. These incidents illustrate the surveillance capability and maneuverability of SUAS, as well as the vulnerability of national structures and icons to their presence.

These surveillance examples also illustrate another aspect of the SUAS threat: anonymity. Utilizing advanced technologies, some SUAS are capable of self-determination in decision making, with only minimal human oversight. Without direct human oversight, SUAS can be more precise by relying upon highly automated system paths with preprogrammed actions. These autonomous features distance the pilot away from the SUAS’ activities, making such flights essentially anonymous. During a soccer match between Serbia and Albania, a SUAS was flown over the match and used as a platform for anonymous speech, displaying a provocative nationalistic message. This incident resulted in the cancellation of the match and flared diplomatic relations. Had the perpetrator been identifiable, he or she would have simply been ejected from the stadium. Exploiting the anonymity provided by SUAS, the actor was able to broadcast his or her message through a means that divorced personal identity from the message.

SUAS are able to carry much more than anonymous messages. They can carry a relatively large payload, while using accurate altitude and positional information. A popular video on YouTube shows a SUAS fitted with machine guns destroying human-looking targets. One could imagine taking this one step further, and rigging up other materials to a SUAS to transform it into a flying improvised explosive device. The advantage to utilizing a SUAS as a weapon system is its compact size and maneuverability vis-à-vis its
capability to deliver a weapon system or kinetic effects with devastating impacts.\textsuperscript{15}

SUAS do not need to deliver a payload to wreak havoc. Their intentional or negligent use can also have disastrous results. One such instance occurred in Dayton, Ohio where an emergency medical helicopter’s landing was delayed for nearly ten minutes by a SUAS in its flight path.\textsuperscript{16} Commercial airline pilots have increasingly reported similar incidents to the U.S. Federal Aviation Administration (FAA).\textsuperscript{17} According to the FAA’s most recently released UAS sightings reports, from August of 2015 until January of 2016, there were almost 600 UAS reports from 45 states and the District of Columbia and Puerto Rico.\textsuperscript{18} These reports describe a variety of incidents ranging from small private aircraft having to take evasive maneuvers to avoid collision with a SUAS to SUAS flying within only a few feet of commercial airliners at some of the nation’s busiest airports.

These are but a few examples that underscore how SUAS’ decreasing size, rapidly increasing state of the art technological capabilities and growing niche of private users makes for a prevalent threat. Next we discuss the potential detection and response options with regard to this threat.

III. Detection and Response Options

SUAS are technologically difficult to detect, identify, track and engage. Limitations in detecting SUAS, coupled with their potential capability as a weapons system, render meaningful reaction difficult. For example, in early 2015, the White House experienced a SUAS incursion when a radar system, designed to detect flying objects like planes, missiles and large drones, failed to detect a SUAS that crashed into a tree on the South Lawn.\textsuperscript{19} Similarly, a manned gyrocopter was able to land, undetected until visible to the naked eye, on the lawn of the U.S. Capitol building.\textsuperscript{20} These incidents highlight the difficulty of detecting the threat that these smaller aircraft systems pose.

Once detected, positive identification of SUAS is complicated by the fact some UAS can be mistaken for smaller manned aircraft, such as a gyrocopter.\textsuperscript{21} To increase the probably of positive identification, SUAS technical knowledge must be acquired in advance. The foundation of this solution depends upon acquiring the necessary knowledge and understanding of SUAS technology, and is not a simple task. With estimated annual global revenue predicted to reach one billion, keeping track of individual operators as well as manufacturers of unmanned vehicles and their components is a daunting task.\textsuperscript{22} The limited regulation of model aircraft adds to the complexity of usefully cataloging SUAS.

Detection, identification and tracking must not only be accurate, it must also be timely to permit deliberate action. Thus, it is necessary to focus on technological solutions that enable positive identification of the SUAS threat, increase available reaction time, and minimize uncertainty in response decisions. Any such system must be able to discriminate on multiple levels. A fusion of multi-spectral sensors, including electro-optical, infrared, and acoustical, could provide a centralized air picture informed by pre-existing threat identification data. Ideally, this would provide confident airborne positions of SUAS while enabling autonomous positive identification of the vehicle and its payload.\textsuperscript{23}

Even when accurate and timely detection, identification and tracking of a SUAS threat occur, the nature of the response is, in itself, a
complex issue. For any response option, particularly from a military perspective, five discrete issues need to be addressed: responsibility, command and control (C2), capability, authorities and guidance.24

Responsibility and C2, essentially who is in charge of the response effort, are inter-related. Both will depend on the situation: where the threat arises, the nature of the threat, and the type of target. For example, in the example of the gryocopter on the Capitol lawn, the National Park Police had primary jurisdiction. However, the Federal Bureau of Investigations had significant interest in investigating and prosecuting the offender, as did local law enforcement in the District of Columbia. More often than not, any threat response will become a collaborative interagency effort, with elements of dispersed or distributed responsibility.25

The capability required to neutralize a SUAS threat will depend on the effect a responder seeks. Any response other than watching the threat, especially in a domestic setting, will be incredibly difficult. “Killing the robot,” with traditional kinetic response options such as with bullets or bombs, in the homeland, are not feasible for a number of reasons. The resiliency of the aircraft, with on-board autopilot, could compensate for damage inflicted to its aerodynamic capability. Damage to the SUAS, combined with its autopilot, could lead to an uncontrolled flight situation, with unpredictable consequences. For example, the SUAS could crash into a civilian area and cause significant collateral damage.26 Thus, simply shooting the SUAS down is not a simple task or optimal engagement choice.

There are a host of potential non-kinetic response options: directed energy, laser, reactive and proactive signals jamming, geofencing or navigational denial, electronic spoofing or cyber highjacking or cyber attack of the SUAS. As with kinetic options, non-kinetic response options also evoke collateral consequences that must be taken into account.27 For example, could an electronic attack to neutralize a SUAS sufficiently discriminate between the threatening aircraft and nearby “friendly” electronic devices?

Each non-kinetic option also evokes unique authorities (permissions) and guidance concerns. To illustrate, any solution involving the use of radio frequencies could implicate Federal Communications Commission (FCC) processes and approvals.28 However, as will be discussed below, the regulatory, legal and policy landscape has not kept pace with technology, especially with regard to the SUAS threat.

IV. LEGAL AND POLICY CHALLENGES

After the quadcopter landed on the White House lawn earlier this year, CNN interviewed President Obama. His statements set the stage for the current state of the regulatory, legal and policy landscape with regards to UAS in the U.S.: (i) there is an absence of a regulatory structure for UAS; (ii) the UAS legal framework needs to get the good and minimize the bad; (iii) the regulatory structures are lagging behind the technology, especially with regards to the threat; and (iv) UAS need not be dangerous or violate personal privacy.29

Although there are not substantial regulatory and legal structures that specifically address UAS in the U.S., existing authorities do allow for the protection of government property. However, as applied specifically to the SUAS threat, these regimes are imperfect. While some of these rules and regulations “fit” when it comes to the SUAS threat, others require
some refinement. In this regard, the legal and policy discussion should focus on three areas:

(1) the Federal Aviation Administration (FAA) regulatory scheme;
(2) state and federal drone legislation; and
(3) specific agency authorities, either through Executive Order or legislative authority

A. FAA Regulatory Scheme

Despite the passage of the 2012 FAA Modernization and Reform Act, which was supposed to fast-track processes for assimilating UAS into the National Airspace System (NAS) by the end of 2015, FAA regulation has been slow-going. In February 2015, the FAA issued a Notice of Public Rule-Making, or NPRM, for SUAS, which has yet to be finalized and would apply only to small commercial UAS.

For the FAA to permit SUAS to operate in the NAS, the Secretary of Transportation must first find that such operations would not create a hazard to other NAS users or the public at large, and that they would not pose a threat to national security. In an attempt to alleviate those concerns, the NPRM proposes operational limitations, operator certification requirements, and aircraft requirements, such as Visual Line of Sight (VLOS) operations, visual observers, registration with a Transportation Security Agency (TSA) review for airman certificate applicants, and other similar requirements. The underlying assumption of the NPRM, then, is that users of the NAS and the public will be safe and that our national security will be protected because UAS operators will have both knowledge of the FAA rules and will comply with them.

However, as foreshadowed by prior SUAS incidents, as set forth above, the potential threats posed by SUASs are varied, real, and of immediate concern. The most substantial threats are threats from terrorist groups who have demonstrated that they are not interested in following the rules. Yet, in the lengthy NPRM, there are only a few sections that could potentially address UAS threats. Specifically, the NPRM would prohibit:

(1) SUAS operations in Class A airspace and require prior permission from air traffic control in Classes B, C or D airspace, or within lateral boundaries of the surface area of Class E airspace;
(2) SUAS operation in “prohibited and restricted” areas without permission from the using or controlling agency;
(3) the careless or reckless operation of a SUAS “so as to endanger the life or property of another;” and
(4) the pilot in charge from allowing any object to be dropped from the aircraft in flight if doing so would create a hazard to persons or property.

The regulatory ramification for violating any of these prohibitions consists mainly of civil penalties, sometimes as high as ten thousand dollars per violation. Ramifications might also include criminal penalties for anyone who knowingly and willfully violates either the Federal Aviation Act of 1958 or the Hazardous Materials Transportation Act and their implementing regulations. That said, the imposition of criminal or civil penalties presupposes that the perpetrator can be identified, caught and subsequently taken to court. As discussed at length above, the anonymity of the SUAS threat calls into question this regulatory assumption.

Regardless, the NPRM rules are not currently in effect; they continue to remain in the process of being considered. What is in
effect is an FAA Advisory Circular #91-57A and an accompanying policy statement, which together provide guidance for “model aircraft,” UAS used for “hobby or recreational purposes.” It only applies to non-commercial SUAS and requires conformity with “community-based” or nationwide set of safety guidelines, aircraft are limited to 55lbs, operators are to not interfere with or else will give way to manned aircraft, and notice must be given to Air Traffic Control if any use will be within five miles of that airport. Further, “[o]perators must stay out of restricted airspace areas, and obey any FAA Temporary Flight Restrictions (TFRs)” while restricting flights below 400ft. While this guidance is somewhat helpful, it does not address the primary threat, the bad actors who are not concerned with the rules.

This does not mean that the regulatory landscape remains a void for bad actors to proliferate. If the operator of a SUAS uses it to commit a crime such as murder, destruction of property, or an act of terrorism, these acts could be punished after-the-fact, under various existing FAA regulations as well as federal and state laws.

However, the more pressing question is what can the government do to prevent these incidents and protect itself before a SUAS threat is manifested? The answer is not apparent in the FAA rules. Because of the FAA regulatory lag, over the last few years, the states have jumped into the fray and attempted to legislate how UAS will be used. Whereas the FAA’s focus has been on safety, the focus of the state and federal UAS bills has been on privacy and due process.

B. State and Federal Drone Legislation

Because the FAA’s progress has been slow with regards to domestic use of UAS, the vast majority of states have attempted to fill this void. In the past three years, state legislators have proposed a combined total of 296 UAS bills. Almost half of the states entertained multiple bills simultaneously. Twenty-five states have passed such legislation. Federal UAS legislation has also been introduced, which largely tracks state initiatives in scope and purpose.

The generalized goal of almost all of these proposals is to “protect citizens’ privacy” or free them from “unwarranted” surveillance. Although each state takes a different path to doing so, generalized trends can be gleaned. Across all three years, most of these bills apply to local law enforcement agencies and prohibit them from using UAS to gather information or evidence, with various exceptions. Many also contain procedural hurdles, operational constraints, detailed reporting and oversight regimes, and significant ramifications for violations. Of all the legislation introduced to date, other than criminalizing violations of regulatory procedures such as those that address privacy or prohibitions on weaponized drones, very few have attempted to address the potential danger that privately operated UAS pose to critical infrastructure.

C. Specific Agency Authorities

Various government agencies have unique authorities that allow them to take certain actions. While the SUAS threat to critical infrastructure could impact any number of government agencies, the SUAS problem from the perspective of a military commander charged with protecting a U.S. installation is one of the many examples across the interagency that highlights the legal and policy
shortfalls in responding to this unique challenge.

As discussed in Section III above, one potential response option is to “kill” the SUAS, to shoot it. However, a kinetic kill is, in most circumstances, not legally viable. Under the current paradigm, the FAA considers UAS to be aircraft and a federal statute prohibits interfering with or shooting down aircraft. 18 U.S.C. § 32, Destruction of Aircraft or Aircraft Facilities, states, in relevant part:

(a) Whoever willfully—
(1) sets fire to, damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States or any civil aircraft used, operated, or employed in interstate, overseas, or foreign air commerce; shall be fined under this title or imprisoned not more than twenty years or both.

Even if “killing” the SUAS was a viable option, the mechanics of actually doing so in the U.S. is difficult and impractical for a number of reasons.

The first reason emanates from the self-defense paradigm applicable in the U.S., which has its basis in Human Rights Law (HRL), and more directly, in U.S. domestic law. HRL applies in peacetime. In the U.S., HRL is embodied in domestic criminal law. In this legal paradigm, the starting point is liberty, as embodied in the Fourth Amendment to the U.S. Constitution, which guarantees “The right of the people to be secure in their persons … against unreasonable searches and seizures.”44 For this reason, Americans are only deprived of their freedom of movement, such as by arrest, based upon probable cause. The United States Supreme Court also established the Constitution’s Fourth Amendment standard of “objective reasonableness” as the appropriate standard for assessing the use of force in the context of making an arrest or other seizure of a person in a case called Graham v. Connor.45 Thus, personnel involved in law enforcement and security duties utilize use-of-force options ranging from simple displays of authority, to the application of various levels of force, to include the use of deadly force only when objectively reasonable to do so.

In the military, use of force domestically is codified in the unclassified STANDING RULES FOR THE USE OF FORCE (or SRUF). The SRUF applies to routine military department functions, including anti-terrorism and force protection. Because its basis is rooted in HRL and the Constitution, the overall posture of the SRUF is generally restrictive in nature.

That said, under the SRUF, “unit commanders always retain the inherent right and obligation to exercise unit self-defense.” However, they can do so only “in response to a hostile act or demonstrated hostile intent,” essentially, an imminent threat.46

Individuals with the capability to inflict death or serious bodily harm and who demonstrate the intent to do so may be considered an imminent threat. The imminent threat analysis is based on all facts and circumstances and does not necessarily mean “immediate” or “instantaneous.”47 What does this mean in the context of a hovering or inbound SUAS? Thus, for SUAS response, the first problem encountered is determining “hostile intent.”
Assuming there is a viable technical solution to assist in rapidly identifying friend versus foe, under the SRUF, and consistent with HRL, use of force is a last resort, must be the minimum necessary, and should be reasonable in intensity, duration, and magnitude. If these requirements are met and the commander opts to take the shot, the second practical problem becomes one of collateral damage. Will this trigger uncontrolled flight? If so, where does the damaged SUAS land? Not knowing specifics as to the SUAS’ payload when taking the shot, further complicates this scenario as shooting it down could release chemical or biological agents.

Change the facts slightly to where the SUAS is flying over the base, perhaps not posing an obvious threat, but filming. Depending on the security classification of the particular area, taking imagery without permission may be unlawful, but not as federal trespass, as currently written. This is yet another case where the law failed to keep pace with the technology. The federal statute, 18 U.S.C. § 1382, is ground-centric. It is titled, “Entering military … property,” and provides, in relevant part, “Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation… Shall be fined under this title or imprisoned not more than six months, or both.” FAA regulations control activity in airspace; yet there are currently gaps there with regards to SUAS threats.

Some other government agencies have interesting enforcement provisions that might be worth emulating. For example, the Department of Energy (DOE) has some helpful provisions in the Atomic Energy Act, including restrictions on aircraft landing at DOE sites, found at 10 Code of Federal Regulations (CFR) § 862. It applies to all persons or aircraft entering or otherwise within or above areas within the boundaries of lands or waters subject to the jurisdiction, administration, or in the custody of the DOE at sites designated by DOE. It specifically includes unmanned aircraft in its scope. This regulation prohibits the operation or use of aircraft on lands or waters of DOE-designated sites as well as violations of FAA regulations regarding minimum altitudes and prohibited flight maneuvers over a designated site. Anyone willfully engaging in those and other activities outlined in the regulation may be subject to criminal penalties.

The DOE also has contracted protective force personnel who, under 10 CFR § 1047, have limited arrest authorization to protect nuclear weapons, special nuclear material, classified matter, nuclear facilities, and related property. They can arrest without a warrant in certain circumstances, including for photographing DOE installations. This could be a useful tool to protect against airborne surveillance of sensitive sites or equipment, which other government agencies, including the Department of Defense, might consider.

Likewise, the Navy and U.S. Coast Guard (USCG) have interesting “Protective Zone” authorities that should be considered to protect stationary and mobile assets against SUAS threats. 33 CFR § 165.2010 establishes geographic parameters around U.S. naval vessels in the navigable waters of the United States, called naval vessel protection zones, and permits enforcement action within them. Under the regulation, a naval vessel protection zone is a regulated area of water surrounding large U.S. naval vessels that provides for their
safety and security. Generally speaking, this statute permits the USCG or, if the USCG is not present or immediately available, the senior naval officer in command, to enforce a minimum 100 yard perimeter around a large U.S. naval vessel at all times in the navigable waters of the United States. It applies whether the large U.S. naval vessel is underway, anchored, moored, or generally within a floating dry-dock. This same kind of protective zone could be employed for other assets as well. These are just a few examples of potential solutions to bring SUAS policy and law up to par with technological advances.

V. CONCLUSION

While the current legal and policy landscape was not created with the SUAS threat in mind, it is still flexible enough to address it. At the same time, it could use some refinement. In the short-term, educating SUAS operators on current regulations is a wise approach. If good intentioned operators follow the rules, the bad actors will be more readily apparent to everyone else.

Relying on the good graces in individuals might be a good interim measure, but any long-term solution to the SUAS threat will require scientists, engineers, lawyers and policy makers to collaborate to both solve the technical problems and create the regulatory and statutory framework to implement it. This will require a three-pronged approach of working within the existing FAA regulatory framework; leveraging state and federal legislation; and seeking additional specific agency authorities. Doing this will require a cross-disciplinary collaboration, whole-of-government effort, and public-private partnerships. All of us are better than any of one of us.

To be sure, the SUAS threat is real and there will be no one-size-fits-all answer. Any solution to this problem must take into account the complex legal and operational environment and the uniqueness of agency needs, while utilizing the technical capabilities to detect, identify, track and respond to threats. As the SUAS threat advances, so too must the laws and policies that enable response.

APPENDIX A - REFERENCES

9. Lichfield, supra note 3.
10. Leonnig and Rupar, supra note 2.
**FPSRussia, YouTube.com,** *Prototype Quadrotor With Machine Gun!*, (Apr. 23, 2012), https://www.youtube.com/watch?v=SNPMJk2fgJU.


**Schmidt and Shear,** supra note 1.


**Roggero,** supra note 14.

**Briggs II,** supra note 19.

**Roggero,** supra note 14.

**Id.**

**Roggero,** supra note 14.

**Id.**

**Roggero,** supra note 14.

**Id.**

**Roggero,** supra note 14.

**Id.**

**Roggero,** supra note 14.

**Id.**

**Id.**


**Federal Aviation Administration, Notice of Proposed Rulemaking,** Dept. of Transportation, Feb. 15, 2015. As of the time of this publication, the NPRM is not final.

**Id.**

**Id.**

**4 CFR §13.23** Criminal penalties. (Section 110(b) of the Hazardous Materials Transportation Act (49 U.S.C. 1809(b)).


**Id.**


**Zoldi ET AL.,** supra note 37.

**U.S. Const. amend. IV**


**Chairman of the Joint Chiefs of Staff Instr. 3121.01B, Standing Rules for the Use of Force (SRUF) for U.S. Forces,** (June 13, 2005).


**Id.**

**10 CFR 862.4(b), citing 42 U.S.C. 2273 and 2278(a) (trespass), sections 223 and 229.**