"Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies"

Testimony by Gregory S. McNeal, JD/PhD
Associate Professor of Law and Public Policy
Pepperdine University

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Oversight and Management Efficiency
March 18, 2015

PEPPERDINE UNIVERSITY
School of Law

INTRODUCTION

The emergence of unmanned aerial vehicles in domestic skies raises understandable concerns that may require employment of mitigation technologies. However, before any funds are expended on such technologies, the Department of Homeland Security should engage in a comprehensive risk assessment to identify the probability, magnitude of harm, benefits of security measures, and cost of those measures. This testimony outlines four key issues that Congress should remain cognizant of when drafting legislation and/or overseeing the activities of the Department of Homeland Security.

RECOMMENDATIONS

1) CONGRESS SHOULD ENSURE THAT AGENCIES ARE DISTINGUISHING BETWEEN POSSIBLE THREATS AND PROBABLE THREATS; CONGRESS SHOULD ALSO ENSURE THAT AGENCIES ARE AVOIDING FEAR BASED APPEALS FOCUSED ON WORST-CASE SCENARIOS:

Drones are an exciting topic that captures the interest of journalists and the public. The popular attention associated with drones has the benefit of raising awareness about their potential uses, however it also raises the possibility that emotions and sensationalism will drive the crafting of public policy.

For example, after a recreational drone crashed on the White House lawn, "security experts" appeared on CNN to discuss the possibility that a drone might be equipped with explosives or weapons of mass destruction. This is a highly unlikely scenario. While consumer drones are readily available, lightweight explosives and weapons of mass destruction are not. Even if terrorists were able to procure explosives or WMD, using a consumer drone to conduct an attack would be one of the least effective means of carrying out an attack. Nevertheless, the Secret Service and other agencies seem to be planning for "possible" worst-case scenarios. Such an approach shifts the policy debate away from probability and creates demands for substantial governmental responses even when the risk does not warrant the response.[1]

Congress must ensure that agencies do not fall victim to the sensationalism that drives worst-case scenario based planning. Such an approach to risk management can justify enormous expenditures, no matter how unlikely the prospects are that the dire event will take place. As security analyst Bruce Schneier has written, focusing on the worst possible outcome "substitutes imagination for thinking, speculation for risk analysis, and fear for reason."[2] It substitutes ill informed possibilistic thinking over careful, well reasoned, probabilistic thinking, forcing us to focus on what we don't know, and what we can imagine, rather than what we do know. "By speculating about what can possibly go wrong, and then acting as if that is likely to happen, worst-case thinking focuses only on the extreme but improbable risks and does a poor job at assessing outcomes."[3]

Congress should ensure that agencies are as concerned with the probability of harm as they are of the possibility of a worst-case scenario. This requires paying attention to the "spectrum of threats, not simply the worst one imaginable, in order to properly understand and coherently deal with the risks to people, institutions, and the economy." While public attention to the issue of drones may create a sense of urgency amongst members of the public and some agency officials, this

---

[1] Sunstein, Cass R. 2003. Terrorism and Probability Neglect. *Journal of Risk and Uncertainty* (26)(2-3) March-May: 121-136.

[2] Schneier, Bruce. 2003. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* New York: Copernicus.

[3] *Id.*

"does not relieve those in charge of the requirement, even the duty, to make decisions about the expenditures of vast quantities of public monies in a responsible manner" that is disconnected from emotions and focused on probabilities.[4]

2) CONGRESS SHOULD ENSURE THAT AGENCIES ARE ASSESSING RISK BY CALCULATING BOTH THE PROBABILITY OF A SUCCESSFUL ATTACK AND THE MAGNITUDE OF LOSSES THAT MIGHT BE SUSTAINED IN A SUCCESSFUL ATTACK:

Congress should ensure that every agency action related to an alleged homeland security risk from drones is preceded by a risk assessment. Assessing risks is the first managerial step in decision making about potential threats, and it is one that is readily subject to Congressional oversight. Forcing agencies to conduct a risk assessment is the first step toward ensuring that agencies efficiently and effectively use taxpayer funds and control costs. A risk assessment is also the first step toward ensuring that agencies make hard choices with limited resources --- every possible threat cannot be guarded against, therefore agencies must focus on the riskiest threats.

"Risk is the expected consequences of a terrorist attack, and the accepted definition of risk as applied in the terrorism context, is *Risk = (probability of a successful attack) X (losses sustained in the successful attack).*"[5] *Probability of successful attack* in this context is the likelihood of a successful terrorist attack using a drone if the security measure were not in place. On the probability side of the equation, the benefits of drones are that they allow an adversary to control delivery of an attack from a distance, perhaps solving some operational problems (like risk of capture) that terrorists may face in planning and mounting an operation. However, they introduce complexity into the attackers operation that may decrease the likelihood of a successful attack. The clear advantages of drones are that they allow for: 1) attacks over perimeter defenses, 2) multiple simultaneous attacks without directly risking attacker personnel, 3) better surveillance capabilities. However, the probability of a successful attack may also go down when an attacker chooses to use a drone. In fact, one RAND/Defense Threat Reduction Agency study found:

> [UAVs] do not appear to have major advantages over other ways of carrying out operations against similar targets, although they cannot be dismissed outright as a potential threat. Where they did appear preferable, the choice for these systems was driven by the actions of the defense or inplace security measures—i.e., were alternative attack modes foreclosed by defenses or did concerns about a potentially compromised plan push the attacking group farther away from its desired targets? The price of these advantages was, however, greater complexity, technological uncertainty, and higher cost and risks associated with these platforms. Consequently, rather than being an attack mode likely to be widely embraced by such actors, UAVs ... appear to represent a "niche threat"—potentially making some contribution to the overall asymmetric and terrorist threat... UAVs do provide some advantages to an attacker, but in most cases there are simpler alternatives that provide similar, or even superior, capabilities.[6]

---

[4] Mueller, John and Stewart, Mark G. 2011. *Terror, Security, and Money.* New York: Oxford University Press.
[5] *Id.*
[6] Jackson, Brian A. *et.al.* 2008. *Evaluating Novel Threats To The Homeland*, RAND.

Losses sustained in the successful attack in this context include the fatalities and other damage (both direct and indirect) that will accrue as a result of a successful terrorist attack employing a drone.[7] This part of the calculation takes account of the value and vulnerability of people and infrastructure, as well as any psychological and political effects. Thus, agencies engaging in an analysis of risk must separate the probability that an attack will be successful if committed using a drone (the subject of the preceding paragraph) from the magnitude of harm that would flow from that particular attack if it were successful.

Thus the prior factor, *probability of successful attack*, would address the low likelihood that an attacker would be able to acquire explosives or WMD, and the decreased likelihood of success with explosives or WMD when using a drone versus alternative methods (like delivering from a manned aircraft, a vehicle, or carried by a person). Whereas the *losses sustained* factor assumes the scenario analyzed probabilistically is successful, and looks to what harms would then flow. In the context of drones, this will requiring gathering information about the payload capabilities of various systems (if assessing a threat from explosives), or the dispersal capability of various systems (if assessing a threat from WMD). What analysts will likely find is that the low payload capabilities of drones will reduce the direct losses sustained from an attack, however the propaganda value associated with a drone attack may increase the indirect costs (such as psychological, economic and political effects) associated with their use.

Taken together, the *probability of a successful attack* employing a drone multiplied by the *losses sustained in the successful attack* will tell agencies what the risk from drones is. From there agencies, guided by Congress, can determine whether the risk is acceptable. If the risk is unacceptable, then agencies should adopt mitigation, risk reduction, and security measures to reduce the risk to an acceptable level --- remaining cognizant of the fact that such measures have costs (the subject of the next section).

3) CONGRESS SHOULD ENSURE THAT BEFORE ANY FUNDS ARE SPENT ON SECURITY MEASURES, AGENCIES ENGAGE IN RISK ASSESSMENT AND A FORMAL COST-BENEFIT ANALYSIS USING BEST PRACTICES:

The employment of mitigation technology against risks cannot take place in a vacuum. Rather, it requires agencies to consider the degree to which a security measure is likely to deter, disrupt, or protect against a terrorist attack. Mitigation technologies are thus a benefit that can reduce risk (as calculated in the prior section).[8] To determine the benefit of a security measure, agencies should make the following calculation: *Benefit of a security measure = (probability of a successful attack) x (losses sustained in the successful attack) x (reduction in risk generated by the security measure).*[9]

The first two factors in this equation are identical to those calculated earlier, while the *reduction in risk* factor is a degree, or percentage factor. In the context of drones, reductions in risk may come from greater surveillance of areas near airports where drones might pose a risk to commercial aircraft, or it may be specific technologies designed to jam the communication links between drones and their operators. But all of the likely risk reduction security measures will have costs, and sometimes those costs may be significant. Thus, the costs will need to be compared to the *benefit of a security measure.* A hypothetical will help illustrate this analytical proces.

HYPOTHETICAL:

---

[7] Mueller, John and Stewart, Mark G. 2011. *Terror, Security, and Money.* New York: Oxford University Press.
[8] *Id.*
[9] *Id.*

FACTS: Assume that in a ten year span of time we believe there is a chance of one successful attack by an explosives laden drone against a federal facility (a 10% yearly chance). Suppose further that we believe an attack will result in one death (valued at $10 million, an admittedly high estimate), and significant psychological and economic damage (valued at $50 million, an admittedly high estimate). For this hypothetical the total losses from such an attack amount to $60 million.

RISK: The yearly *risk* from such an attack is thus the (*probability of a successful attack* .10) x (*losses sustained in a successful attack* $60 million) = $6 million.

BENEFIT OF SECURITY: Now assume that a security system can be installed that cuts the probability of a successful attack by 50%. Such a system might be a combination of cameras, sensors and jamming equipment that allows for detection of a drone and the jamming of the drone's control link.

The yearly *benefit* of the security measure is the reduction in *risk* associated with its employment, which is thus the (*probability of a successful attack* .10) x (*losses sustained in a successful attack* $60 million) x (*reduction in risk generated by the security measure* .50) = $3 million.

IS THE COST OF SECURITY WORTH IT?: To determine whether the cost of such a security system is worth the expenditure of taxpayer dollars, we must compare the costs to the benefits. If the cost of cameras, sensors, and an interdiction system for drones in this hypothetical were less than $3 million, the benefits would outweigh the costs, and it would be a cost-effective security measure.

Importantly, this hypothetical calculation only takes account of the security measures being implemented at one federal facility. The reality is that implementing such measures across the federal government will require aggregating the costs across thousands of facilities. How to allocate those scarce resources will require prioritization, driven by risk assessments (as explained above), and will require the identification of a specific individual or office within the Department of Homeland Security responsible for coordinating interagency efforts to conduct risk assessments.

4) CONGRESS SHOULD ENSURE THAT SPECIFIC INDIVIDUALS AT THE DEPARTMENT OF HOMELAND SECURITY ARE RESPONSIBLE FOR CONDUCTING THESE ANALYSES AND REPORTING THEIR METHODOLOGY. CONGRESS MAY ALSO WANT TO PROVIDE FUNDS TO THE CENTERS OF EXCELLENCE FOR AN INDEPENDENT EVALUATION OF THREATS:

Given the complexity of the risk assessment picture associated with drones and their potential to pose a homeland security threat, Congress should direct that a specific individual or office within the Department of Homeland Security assume responsibility for generating threat assessments.

There is some precedent for this type of managerial approach. In 2004, the Department of Homeland Security initiated a $100 million program to evaluate whether civilian aircraft should be equipped with countermeasures to defeat the threat of man portable surface to air missiles. The program was directed by Congress as a means to evaluate whether Congress should require that some or all U.S. commercial airliners install such devices. At the time, the office within DHS was known as the Counter-MANPADS System Program Office. Congress could create a similar temporary office within DHS for the purpose of evaluating the threat posed by unmanned aircraft.

In the alternative, Congress could direct the Under Secretary, National Protection & Programs Directorate to lead and staff a similar effort within DHS and make the Under Secretary the lead federal official for interagency efforts.

Additionally, Congress may want to consider requesting the support of the Department of Homeland Security Centers of Excellence. These university based research centers can engage in terrorism risk analyses that will supplement the work of DHS. Such outside research may provide an independent check on the interests of government agencies that may adopt or promote drone countermeasures as a means to ensure the continued relevance of their office or to justify increased budgetary outlays.[10]

CONCLUSION

The emergence of unmanned aerial vehicles in domestic skies raises understandable concerns that may require employment of mitigation technologies. However, before any funds are expended on such technologies, the Department of Homeland Security should engage in a comprehensive risk assessment to identify the probability, magnitude of harm, benefits of security measures, and cost of those measures.

[10] For an example of such mismanagement, *see* GAO Report, *DOD Needs Strategic Outcome-Related Goals and Visibility over Its Counter-IED Efforts* available at: http://www.gao.gov/assets/590/588804.pdf

Dr. Gregory McNeal, is an Associate Professor of Law and Public Policy at Pepperdine University where his research focuses on security, technology, and crime. He has written extensively about drones and is a contributor to Forbes.

Dr. McNeal has aided state legislators in drafting legislation related to unmanned aircraft and advised executive branch agencies at the state and federal level on matters related to drones. He has testified before the House Judiciary Committee about drones and privacy and has testified before the House Foreign Relations Committee about counterterrorism. He serves as a voting member of the ASTM technical committee creating scientific standards to govern drones and their operation. He is currently an academic member of the Secret Service Electronic Crimes Task Force.

Previously, Dr. McNeal served as a consultant to the Chief Prosecutor of the Department of Defense Office of Military Commissions on matters related to the prosecution of suspected terrorists held in the detention facility in Guantanamo Bay, Cuba. He also co-directed a U.S. Department of Justice counterterrorism grant program. He has consulted with the Department of Defense on a range of issues, including helping to draft a manual aimed at reducing harm to civilians in conflict.

Dr. McNeal has presented at dozens of unmanned aircraft industry events and advised drone start-ups, sensor manufacturers, law enforcement, consulting firms, venture capital and private equity funds, and Fortune 500 companies about technical, legal, regulatory, and management issues related to drone technology.

He has authored over a dozen law review articles, and is a co-author of the casebook *Anti-Terrorism and Criminal Enforcement*, co-editor of the book *Saddam On Trial: Understanding and Debating the Iraqi High Tribunal*. He is the editor of a forthcoming book *Cybersecurity and Privacy*, author of the forthcoming book *Prosecuting Terrorism* (under contract with Oxford University Press), and is conducting research for books about civilian and military uses of drones.