

## The Poor Man's Air Force Unattributed Mid-Range Drone Attacks

### PIPS White Paper: *Executive Summary*

Margaret Miller, Research Fellow  
Colin Cochran, Research Intern  
Clara Waterman, Senior Research Intern

On January 5, 2018, thirteen homemade drones loaded with explosives attacked two Russian military bases in Syria. Estimates indicate that attackers may have launched these GPS-guided Unmanned Aerial Vehicles (UAVs) from as far as 100 kilometers away, complicating attack attribution. While Moscow suspects that United States and Israel enabled the attack, the responsible actors remain unidentified.

Military and commercial technological advances are making mid-range unmanned aerial vehicles (M-UAVs) increasingly inexpensive and accessible. M-UAV proliferation enables resource-poor states and non-state actors to target civilian population centers with lethal airpower that is difficult to attribute. The United States faces difficulties countering asymmetric threats and engaging with adversaries at below-war levels of conflict. Attributing and responding to anonymous or proxy M-UAV attacks will exacerbate this gray-zone challenge. Uncertain attribution will contribute to U.S. policy paralysis, allow deliberate misattribution of attacks for propaganda purposes, and enable spoilers in peace processes and repression.

#### *The New Threat from M-UAVs*

M-UAVs are becoming more advanced, more available, and more dangerous. These drones are spreading to new actors because of their appeal as reconnaissance and counter-value weapons and decreasing costs. A lower threshold to accessing M-UAVs democratizes access to deadly airpower by blurring the line between great powers and other actors. The inherent qualities of M-UAVs coupled with their wider proliferation makes attribution of attacks potentially difficult.

- *Features of M-UAVs.* Mid-range UAVs are fixed-wing or hybrid vehicles of military, commercial, or homemade production that carry a payload beyond line of sight, but less than 200 km. M-UAVs are preferred options for actors seeking a low-cost alternative to military-grade UAVs with better performance than hobby drones. These vehicles can be manufactured or equipped with explosives, and commercial development is increasing their range. Sophisticated navigation technologies are enabling alternatives to radio and GPS control so that even low-end M-UAVs cannot be disabled by radio or GPS jammers.

- *Proliferation of M-UAVs.* M-UAVs will increasingly spread as commercial technological development drives down costs. Small states and non-state actors will prefer M-UAVs for attacks that need to be launched from a longer range to avoid defenses. M-UAV proliferation is driven by cost and availability, on the supply side, and their military utility, on the demand side. M-UAVs will continue to spread as these weapons become more inexpensive and useful. We have already seen suggestive evidence of states and non-state actors acquiring M-UAVs, accompanied by a growing inter-state M-UAV trade.
- *M-UAVs, coercive airpower, and attribution.* Improving M-UAV technology lowers the cost threshold for deadly airpower and expands the number of actors, both state and non-state, that can credibly threaten civilians. Further, increased proliferation creates an operating environment in which M-UAV attacks may be difficult to attribute. Uncertain attribution may, for example, make it unclear if states are supporting proxy organizations.

### *U.S. Gray-Zone Vulnerability*

The United States faces difficulties in the gray zone, an operating environment in which hostile actors employ asymmetric means, such as information operations, legal ambiguity, and proxy groups, to achieve revisionist political goals. Actors in the gray zone operate below the threshold of conventional warfare to erode the status quo and minimize the risk of retaliation.

Gray-zone strategies use emerging technologies, the threat of escalation, and ambiguity to reduce the possibility of U.S. retaliation. Technological development facilitates new strategies by lowering cost barriers to weaponry and improving the capabilities of cheap options. The United States has not effectively responded to gray-zone operations even when attribution was almost certain, because of the steep geopolitical costs of overreaction and accidental escalation. Gray-zone strategies exploit U.S. decision-making priorities, including reputational costs.

### *Dangers of M-UAVs in Gray Zones*

M-UAVs will contribute to U.S. vulnerability in the gray-zone by providing an inexpensive strategy to new actors below the threshold of conventional war. M-UAVs create three problems: fundamental uncertainty in attribution, potential for deliberate misattribution, and plausible deniability for spoilers and repression.

- *Uncertain attribution complicates U.S. policymaking.* Ambiguous or incorrect attribution will make it more difficult for the United States and its allies to respond to M-UAV attacks. Depending on the degree of certainty, the United States may be unable to determine the identities of responsible actors, suspect attribution, or incorrectly attribute attacks. Like other gray-zone threats, M-UAV attacks will blend weaponized ambiguity, below-war conflict, and a mix of state and non-state actors to overwhelm decision makers with uncertainty. Counter-acting pressures in U.S. decision-making will result in policy

paralysis, and the United States will expend valuable time and resources determining who is responsible for an M-UAV attack against civilians.

- *Deliberate misattribution for propaganda purposes.* Attributing an M-UAV attack is inherently difficult, and foreign groups have incentives to misattribute attacks. States and non-state groups will exploit misattribution for information operations in the gray zone through social media and other publications. Regimes will most likely shift blame for attacks to adversaries to motivate domestic constituencies to support a foreign policy objective or to generate international support for their cause through alliances or in international forums. Misattribution of M-UAV attacks risks implicating the United States in civilian deaths, which could erode public support in vulnerable regions.
- *Plausible deniability enables spoilers and repression.* As more groups use M-UAVs without attribution, preventing attacks will be increasingly complicated. Actors in the gray zone will use ambiguity to reduce political will to issue threats of retaliation. Actors may use M-UAVs to spoil peace processes or to implicate a third party for violence in a conflict. Hostile regimes may be more willing to use deadly M-UAVs to punish or repress civilians knowing that both attribution and an international response are unlikely.

Unattributed M-UAV attacks will strain U.S. policy and decision-making, similar to past gray-zone operations. M-UAV attribution problems force U.S. policymakers to choose between retaliating with imperfect information and inaction. In the past, weaponized ambiguity has challenged the United States because of U.S. reliance on public support for military action and concerns about escalating conflicts with peer adversaries. Uncertain attribution of M-UAV attacks will require adjusting U.S. strategy for a more complex operating environment.

### *Conclusion*

Military and commercial production will continue to decrease costs and improve the offensive capabilities of M-UAVs. More actors will gain access to mid-range airpower, which may be used against civilian targets without clear attribution. Uncertain attribution will complicate U.S. decision-making and lead to policy paralysis. Additionally, actors in the gray zone may intentionally misattribute M-UAV attacks for propaganda purposes and implicate the United States in civilian deaths. Further, attribution problems allow plausible deniability for M-UAVs used as spoilers and domestic repression.

There are two main implications of the threat discussed in this paper. First, counter-drone technology for area defense will become more important than point defense. Second, U.S. leaders and the U.S. public may need to become comfortable with uncertain attribution.

Adversaries have exploited U.S. vulnerability in the gray zone before, and it is unclear that this danger can be eliminated. This paper points to the need to mitigate the threat of M-UAV attribution problems and include this issue in future research and funding.