Quantifying the COTS Drone Threat Landscape

Kevin Finisterre
March, 2017
Quantifying the COTS Drone Threat Landscape

Recently there has been no shortage of public commentary about drones as a potential threat vector. Unfortunately, there have been very few Threat Modeling conversations about the perceived threats that drones represent. Historically, much of the data about the actual impact of malicious drones and RC aircraft has been classified. However, social media is increasingly providing data in news articles and blogs. In many cases, data has been disseminated via forums, Twitter feeds, Telegram channels, or other public sources. Increasingly, government and military agencies are also declassifying and, like social media, are sharing data with the general public.

As examples of drone threats present themselves it is increasingly important to have tools that classify and categorize the specific types of threats. A common set of Threat Modeling tools is necessary to allow interested parties to be on the same page regarding the threat potential. A set of recognized methodologies is necessary in the Counter Unmanned Aerial System (CUAS) community to help frame threat potential for those who are attempting to track developments in the counter drone market.

A recent paper titled “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology”, produced by the Combating Terrorism Center, in West Point, highlights “a typology to help the reader make sense of the incidents in which terrorists have used drones” (see link below). The paper details many of the notable instances on the public record since 2008. These incidents will soon represent a sizable portion of the last decade's drone and RC threats.

Figure 2: Typology of Terror UAS Use
Even with the typology described in Figure 2, the community still lacks a methodology to classify this type of threat on a per site (or environment) case-by-case basis. In some instances, the objective may not represent a level of threat that warrants a response. In other instances, however, a response may be warranted, although this is highly dependent on other variables in a larger threat model. David Kovar’s USENIX talk, “UAVs, IoT, and Cybersecurity”, mentioned the larger scale of modeling drone threats against the specifics of a mission, or operational goal. A number of variables are used when calculating risk on a per location (or mission) basis, as highlighted in the following flowchart:

https://www.usenix.org/conference/lisa16/conference-program/presentation/kovar

![UAV Risk Assessment Model](image.jpg)

At the Digitalbond S4x17 conference, Kevin Finisterre presented a drone-specific modification of Microsoft’s DREAD model: the Department 13 DREAM Threat Model. The DREAM model can be used to complement the UAV Risk Assessment Model presented by David Kovar. Specifically, the DREAM model can be used as either of the two “Estimator” blocks in Kovar’s model. Other aspects of Kovar’s model, such as the “Threat Analysis” and the “Occurrence Probability” calculations, are also inherently present in the DREAM model. Essentially, Kovar’s model feeds the DREAM model’s output to the “Risk Assessor” block.

https://prezi.com/tufgpte8vxqt/drone/?utm_campaign=share&webgl=0&utm_medium=copy#
The DREAM Threat Model uses a simplistic and subjective methodology to classify a drone’s potential risk. Essentially, DREAM is the Microsoft DREAD model (minus the D model, and adding a subjective Mitigation value). Each RC model or drone is graded for the following categories:

**Damage Potential:** What type of negative impact does the drone have on its environment, such as payload ability, battery life, stability, GPS assistance, way-pointing, and capability.

**Reproducibility:** How easy is it to create a drone or RC craft that is capable of such a threat? Consider the level of effort it would take to obtain, or build, such a craft.

**Exploitability:** What skills and resources are needed to create a negative impact using this particular drone? Can it be done by a single individual, or will it require a team? Does it require any aerospace understanding and targeted skills (IED)?

**Affected area or persons:** How many individuals will be affected? What type of visually or physically sensitive area will be affected? Will it cause a minor annoyance, or injury and death? Will it affect only individuals or larger groups, or will it cause mass casualties?

**Mitigation value:** A subjective value will be assigned as an organization specific wild card. It will act as a modifier for specific threat management. It can include stake holder commentary, outside intelligence, or any other influencing mechanism for assigning values.
Category elements and weighting will differ, depending on the environment and the business logic used to interpret the value of assets vs. potential threats. It would be necessary to create a personalized exercise, with the appropriate peers, to determine a meaningful variation of the above weighted matrix. The matrices used should be specific to the environment. For example, a threat matrix for an airport would be very different from a threat matrix for a Forward Operating Base. In the DREAM model, the Mitigation value was provided specifically as a flexible override metric to help deal with the subjective nature of "threat".

Part of Microsoft’s strategy after creating DREAD was to utilize a complementary model: STRIDE. STRIDE helps understand the relationship between threats and countermeasures. The model uses a goal-based approach which considers the attacker's goals. This approach allows an organization to start with a list of common threats that are grouped in parallel with specific location-specific attributes. Using this baseline, certain types of potential threats can be ranked and then ruled out because they do not apply to specific scenarios. Pre-selected threat categories that are coupled with predefined threat lists can be used to scrutinize specific aspects of vulnerability in the context of the facility or location being protected from threats by a variety of drone models and types.


At the S4x17 conference, Kevin Finisterre presented a complementary model (see below) that is represented by a modified Police Use of Force Ladder and a Use of Force Continuum. The model has pre-defined MESMER responses (mitigations) that match a pre-selected list of sample drone threats. In practice, this model performs in a similar manner as a Microsoft STRIDE implementation.
2017 has seen an increase in the threatening use of Commercial-off-the-Shelf (COTS) and DIY drone platforms. It is becoming hard to be a skeptic about drone threats as the extra data points collected about these threats adds validity to the general conversation. One of the more comprehensive reports on threat potential is another paper produced by the Combating Terrorism Center at West Point: “CTC Perspectives: The Islamic State’s Drone Documents: Management, Acquisitions, and DIY Tradecraft”. The paper presents highly detailed threat intelligence that was previously unavailable to the public. DIY aircraft include the Islamic State Skywalker X8 (pictured on the next page). The Skywalker X8 is purportedly using ArduPlane “APM” software. This is one of the most shocking representations of the potential “DIYDrone” threats. Many people in the communities turn a blind eye to the realities of what their weekend hobby, and OpenSource project, can theoretically enable. This reality is hard to ignore.

There is a growing amount of information about the COTS and DIY drones that are being used in the theater. In addition, there is more information being made available regarding the lethal payloads that are used by potential drone attackers. A recent article by Nick Waters (@N_Waters89), who is an ex-British Army officer and an open source analyst (with help from fellow OSINT Twitter users @vpkivimaki & @AbraxasSpa) detailed some of the in-theater threats from a munition standpoint in relation to payload options. Keep in mind this is some of the most accurate and current data that is publicly available, and that it was sourced over Twitter.

https://www.bellingcat.com/uncategorized/2017/02/10/death-drone-bombs-caliphate/
In the short amount of time it took for this document to be edited, a document was published by the Middle East Media Research Institute which presents 10 years of drone intel. The intel spans early experiments by Hezbollah and Al-qaeda up to current IS-based drones. The document provides alarming imagery that depicts the goals of those who wish to use drones maliciously. The document’s explicit imagery, presented below, is important enough to be included in this document.


Poster distributed by the pro-ISIS Sawa’eg media group on February 1, 2017, showing an ISIS drone targeting the Statue of Liberty. Text reads: “New Islamic State Nightmare” (Telegram.me/Sawaeg)
Additional examples of new in-theater occurrences were also shared on public media as this document was being edited. This narrative continues to validate itself day-by-day.

Publicly available information about known munitions, combining payloads, and damage estimates allows assumptions to be made about the ability of terrorists to weaponize specific drones. Such information allows implied attrition to be derived, based on what has already been seen in-theater. In addition, available munitions can be examined, including a range of target weights (with characteristics such as shape and activation techniques) that can be used in weighting threat models such as DREAM.
At this point, a bit of brainstorming is required. Individual analysts need to bring their own concept of “killer drones” to the table for further discussion. To facilitate this request, I am asking that anyone reading this document take a moment to fill out the online form provided below. Please submit 1 or 2 examples of drones that you are *aware* of which could theoretically be considered a threat. Please research the drone’s flight characteristics (such as range or agility), payload capabilities (how much weight, or sensor capability), and its level of autonomy (can it fly by itself? via GPS? via vision system?).

In addition, please note whether the drone’s platform has been used “In Theater” (on a battle field, or by a terrorist actor). Any additional commentary about why you feel the drone poses a threat (or does NOT pose a threat) is welcome. Any type of drone, from Block 5 military drones to children’s hand-held toy drones, are valid for submission. Submissions will be discussed in a future blog post that details the inner-workings of the Department 13 DREAM Threat Model that utilizes the submissions.

D13 Drone Entry Form: https://goo.gl/forms/h9WubHJwYsazlS7D2