CONDUCTING A THREAT ASSESSMENT OF YOUR REFINERY’S AIRSPACE

THE “MUST KNOWS” TO COVER YOUR ASSETS
GOAL

• Let’s rethink the way we evaluate the threat that drones present?
  • Risk Assessment
  • Crisis Management
THE THREAT
HOW MANY DRONES ARE YOU IN YOUR AIRSPACE TODAY?
Physical & IT Security Strategies Have a Gaping Hole

- Every enterprise and every individual protected by a traditional fence now requires an aerial equivalent.
HOW HAVE DRONES CREATED THIS GAP: LOW BARRIER TO ENTRY

Drones:
• Inexpensive
• Carry heavy payloads
• Flown by anyone

Payloads:
• Photo, video cameras
• Network sniffers
• IoT hacking devices
• Sensitive microphones
• And worse

Recent trends of the proliferation of drones create a distinct security challenge
3 CHALLENGES SECURITY ORGANIZATIONS MUST OVERCOME

• Threat Variance
• No Design Standards
• Variable Infrastructure
CHALLENGE 1: THREAT VARIANCE
THREAT: WEAPONIZED DRONE

Payload
• Explosives
• Chemicals
• Guns, flamethrowers, weapons
• Electromagnetic pulse (EMP)

Threat
• Injury, loss of life

Examples
• ISIS (~50 attacks per day)
• Water contamination (prank)
• Radioactive waste (prank)
**THREAT: SURVEILLANCE DRONE**

- Threat: Surveillance Drone

**Payload**
- High resolution camera

**Threat**
- Privacy
- Corporate Espionage
- Intelligence gathering for physical attack
- Vulnerability Reconnaissance

**Examples**
- Paparazzi
- “No photo” facilities
- Peering through windows
THREAT: HACKING DRONE

Payload
- Sniffing device
- Spoofing device
- Raspberry Pi

Threat
- Hacking, data extraction

Examples
- Data center snooping
- WiFi spoofing
- Internet-of-Things hacking
CHALLENGE 2: NO DESIGN STANDARDS
EXAMPLE: DJI PRODUCT LINE (5 YEAR TIMELINE)

There is no regulated frequency or way that drones communicate to a controller.
CHALLENGE 3: VARIABLE INFRASTRUCTURE
EVERY SITE IS VULNERABLE TO DRONE ATTACKS

- Datacenters
- Corporations
- Private Residences
- Prisons
- Stadiums
- Events
CONDUCTING A THREAT ASSESSMENT
WEATHER

• What times of day is threat most prominent
  • What weather effects do they use to their advantage/how are you negatively impacted by the weather
  • Sunrise/sunset/etc.
  • If someone is flying at night, does this increase the likelihood that they are a belligerent player

• What type of weather would lead to an accident?
  • Recreational Droner flying within airspace range but at a neutral location gets drone caught in wind gust that pushes it to facility

Weather can give you indicators into human behavior to help you evaluate threat
Baiji, Iraq
Tuesday
Partly Cloudy

88 °F | °C
Precipitation: 0%
Humidity: 19%
Wind: 13 mph

Temperature | Precipitation | Wind

1 AM | 4 AM | 7 AM | 10 AM | 1 PM | 4 PM | 7 PM | 10 PM
Fri | Sat | Sun | Mon | Tue | Wed | Thu | Fri
74° 53° | 79° 55° | 82° 56° | 85° 60° | 88° 63° | 82° 60° | 85° 61° | 85° 62°
AREA OF OPERATIONS

- Boundary/borders
  - Only designated refinery area?
  - How far out can you look to mitigate threat?
    - Radius; what distance will be most beneficial
  - How far out can you influence threats?
    - Send police to investigate areas
- Terrain analysis
  - Parks-Free Game for drone pilots, expected that they fly from there
  - Beaches-Higher likelihood that this is a recreational user
  - Abandoned building
- Complete layout of refinery
- Key Terrain
  - Assets whose physical integrity could put whole facility at risk
- Overall understanding of the area
AREA OF OPERATIONS
NAIS AND PATTERN OF LIFE

• What specifically do we know about the threat and how can we implement this in our surveillance techniques?

• NAIs: Where are the most important mitigation points?
  • Risky terrain, areas of potential pipe leak, wherever you would have your inspectors look

• PATTERN OF LIFE: What are behaviors outside of norm that would be an indicator of a belligerent?
  • Person flies from beach on a sunny day close to your facility due to proximity of beach
  • Person flies from an abandoned building to surveil your site on a continuous basis
THREAT ASSESSMENT
COURSES OF ACTION (COAS)

• What do we *expect/anticipate* will happen?
  • Typically we are analyzing the threat, so the courses of action will be what we expect to see the threat doing

• Most likely/Most dangerous; want to know the overall potential of the threat in order to combat it
  • Prioritize!
CRITERIA FOR COAS

• Suitability
  • A threat COA must have the potential for accomplishing the threat’s likely objective or desired end state

• Feasibility
  • Consider the time, space, and resources required to execute the COA.

• Acceptability
  • Risk involved for threat
  • How it affects our mission

• Historical activity*
<table>
<thead>
<tr>
<th>Flight time</th>
<th>Spark</th>
<th>Phantom 3 Std</th>
<th>Phantom 4 Adv</th>
<th>Phantom 4 Pro</th>
<th>Mavic</th>
<th>Inspire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Speed</td>
<td>31 mph (50 km/h)</td>
<td>34 mph (54 km/h)</td>
<td>45 mph (72 km/h)</td>
<td>45 mph (72 km/h)</td>
<td>40 mph (65 km/h)</td>
<td>58 mph (94 km/h)</td>
</tr>
<tr>
<td>Range</td>
<td>1.2 miles (2 km)</td>
<td>0.6 miles (1 km)</td>
<td>4.3 miles (7 km)</td>
<td>4.3 miles (7 km)</td>
<td>4.3 miles (7 km)</td>
<td>4.3 miles (7 km)</td>
</tr>
<tr>
<td>Camera</td>
<td>12-MP stills 1080p video</td>
<td>12-MP stills 2048 x 1536p video</td>
<td>20-MP stills 4K 60fps video</td>
<td>20-MP stills 4K 60fps video</td>
<td>12-MP stills 4K video</td>
<td>20-MP stills 4K/5K video</td>
</tr>
<tr>
<td>Size</td>
<td>5.6 x 5.6 x 2.1 in (143 x 143 x 53.3 cm)</td>
<td>13.8 in diagonal (350 mm)</td>
<td>13.8 in diagonal (350 mm)</td>
<td>13.8 in diagonal (350 mm)</td>
<td>13.2 in diagonal (350 mm)</td>
<td>15.8 x 10.6 x 10.7 in (442.7 x 31.7 x 27.0 cm)</td>
</tr>
<tr>
<td>Takeoff weight</td>
<td>11.6 oz (330 g)</td>
<td>9.6 lb (4.3 kg)</td>
<td>3 lb (1.4 kg)</td>
<td>3 lb (1.4 kg)</td>
<td>1.6 lb (0.73 kg)</td>
<td>8.8 lb (4 kg)</td>
</tr>
<tr>
<td>Other features</td>
<td>Follow me, Return home, Obstacle avoidance, FPV</td>
<td>Follow me, Return home</td>
<td>Follow me, Return home, Obstacle avoidance</td>
<td>Follow me, Return home, Obstacle avoidance, 360° Obstacle avoidance</td>
<td>Follow me, Return home, Obstacle avoidance</td>
<td>Obstacle avoidance, Spotlight Pro/Broadcast, Cinematic mode</td>
</tr>
<tr>
<td></td>
<td>(US$399 with camera gimbal)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EXAMPLE: BAIJI OIL REFINERY
MOST DANGEROUS COURSE OF ACTION
MOST LIKELY COURSE OF ACTION

1. Deploy
2. Surveil
3. Disrupt
4. NA
CRITERIA CONTINUED

• How does the AO (refinery) encourage/discourage the threat?
• Situate threat on map (we know this as a “SITEMP;” visual representation of what may occur
• **Match COAs with UAV Matrix and NAIs**
  • This is the overall BLUF: how implementing UAV operations into the refinery business can successfully mitigate risks of A, B, and C in order to create a safer work environment, etc.
Deploy
Patrol
Defend
Surveil
Disrupt
HAVE A PLAN!

**DELIBERATE RISK ASSESSMENT WORKSHEET**

<table>
<thead>
<tr>
<th>1. MISSION/TASK DESCRIPTION</th>
<th>2. DATE (DD/MM/YYYY)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refinery Operations</td>
<td>3/30/2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. PREPARED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Name (Last, First, Middle Initial)</td>
</tr>
<tr>
<td>Ibrahim, Uzkar, H</td>
</tr>
<tr>
<td>b. Rank/Grade</td>
</tr>
<tr>
<td>CPT</td>
</tr>
<tr>
<td>c. Duty Title/Position</td>
</tr>
<tr>
<td>Security Manager</td>
</tr>
<tr>
<td>d. Unit</td>
</tr>
<tr>
<td>Baiji Oil Refinery</td>
</tr>
<tr>
<td>e. Work Email</td>
</tr>
<tr>
<td>f. Telephone (DSN/Commercial (Include Area Code))</td>
</tr>
<tr>
<td>g. IUC/GIN (as required)</td>
</tr>
<tr>
<td>h. Training Support/Lesson Plan or OPORD (as required)</td>
</tr>
<tr>
<td>i. Signature of Preparer</td>
</tr>
</tbody>
</table>

Five steps of Risk Management:
1. Identify the hazards
2. Assess the hazards
3. Develop controls & make decisions
4. Implement controls
5. Supervise and evaluate

<table>
<thead>
<tr>
<th>4. SUBTASK/SUBSTEP OF MISSION/TASK</th>
<th>5. HAZARD</th>
<th>6. INITIAL RISK LEVEL</th>
<th>7. CONTROL</th>
<th>8. HOW TO IMPLEMENT</th>
<th>WHO WILL IMPLEMENT</th>
<th>9. RESIDUAL RISK LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refinery Operations</td>
<td>Drone Surveillance</td>
<td>Moderate</td>
<td>Work with local law enforcement to go out to locations where drone deployment is outside of our expectations</td>
<td>Call Local Police Department</td>
<td>Security Manager</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>Drone Payload Delivery</td>
<td>High</td>
<td>Use Detect System, go through escalation plan. Once drone passes designated safe zone, employ emergency countermeasures</td>
<td>Employ Active Countermeasure</td>
<td>Security Manager</td>
<td>M</td>
</tr>
</tbody>
</table>

How:
- Call Local Police Department
- Security Manager
- Employ Active Countermeasure
- Security Manager