TRACKING SPIES IN THE SKIES

FBI CESSNA N496WW. PHOTO BY CHRIS KENNEDY
ABOUT THE TALK

LAW ENFORCEMENT AND AERIAL SURVEILLANCE

- History of aerial surveillance (Sam Richards) @minneapolism
- Technology on spy planes (Jerod MacDonald-Evoy) @jerodmacevoy
- Detecting surveillance aircraft (Jason Hernandez) @jason_nstar
HISTORY OF THE SKY SPIES

- Odd flight patterns noticed, *WSJ*, Baltimore
- r/conspiracy (John Wiesman - ADSB Detection)
- Citizen journalists (*Sam Richards*) #FBISkySpies and 100 Tail-numbers, links to FlightRadar24 tracks

![Map showing flight patterns over Beverly Hills](image)
SKY SPIES 101

- Sam's story goes viral, a week later AP breaks it into the mainstream
- Sen. Franken calls for investigation (nothing happens)
- FBI Planes hidden behind front companies (FVX Research, et. al)
WHAT WE KNOW

Wide Area Airborne Surveillance (WAAS)

- As new capabilities are developed, warfighters innovate to meet mission needs
- New and developing payloads create opportunities and challenges

FMV - 30 fps
Gorgon Stare - 2 fps

Gorgon Stare + ARGUS

MQ-1
Observe single target
Single ROVER / OSRVT

MQ-9
4x4 km coverage area
12 independent ROVER queries growing to 30

MQ-9
10x10 km coverage area
As many as 30 ROVER queries and potentially 65 clips to the Tactical Operations Center

Today
IOC 2nd Qtr FY10
4th Qtr FY11

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION
### FAA FOIA DATA

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
<th>N</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>2202</td>
<td>N89KW</td>
<td>271164</td>
<td>20130915</td>
<td>GVQ</td>
<td>20130915</td>
<td>18.18</td>
<td>I19</td>
<td>20130915</td>
<td>20.4138</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2203</td>
<td>N701PM</td>
<td>353068</td>
<td>20130922</td>
<td>T54</td>
<td>20130922</td>
<td>14.02</td>
<td>K31</td>
<td>20130922</td>
<td>15.16</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2204</td>
<td>N701PM</td>
<td>356677</td>
<td>20130922</td>
<td>GKY</td>
<td>20130922</td>
<td>20.46</td>
<td>I51</td>
<td>20130922</td>
<td>21.57</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2205</td>
<td>N6168H</td>
<td>281131</td>
<td>20130927</td>
<td>MSL</td>
<td>20130927</td>
<td>15.28</td>
<td>M31</td>
<td>20130927</td>
<td>16.59</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2206</td>
<td>N6168H</td>
<td>264730</td>
<td>20130927</td>
<td>MNV</td>
<td>20130927</td>
<td>18.49</td>
<td>M31</td>
<td>20130927</td>
<td>19.56</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2207</td>
<td>N6168H</td>
<td>239364</td>
<td>20131003</td>
<td>MSL</td>
<td>20131003</td>
<td>15.32</td>
<td>I19</td>
<td>20131003</td>
<td>19.37</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2208</td>
<td>N89KW</td>
<td>24893</td>
<td>20131006</td>
<td>I19</td>
<td>20131006</td>
<td>23.23</td>
<td>I19</td>
<td>20131007</td>
<td>1.03</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2209</td>
<td>N310MH</td>
<td>65973</td>
<td>20131007</td>
<td>APF</td>
<td>20131007</td>
<td>13.36</td>
<td>M31</td>
<td>20131007</td>
<td>15.14</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2210</td>
<td>N6168H</td>
<td>32305</td>
<td>20131007</td>
<td>APF</td>
<td>20131007</td>
<td>11.16</td>
<td>M31</td>
<td>20131007</td>
<td>15.19</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2211</td>
<td>N89KW</td>
<td>87110</td>
<td>20131008</td>
<td>EYE</td>
<td>20131008</td>
<td>0.11</td>
<td>I19</td>
<td>20131008</td>
<td>1.10</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2212</td>
<td>N310MH</td>
<td>223645</td>
<td>20131009</td>
<td>APF</td>
<td>20131009</td>
<td>11.47</td>
<td>J71</td>
<td>20131009</td>
<td>14.34</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2213</td>
<td>N310MH</td>
<td>320287</td>
<td>20131010</td>
<td>APF</td>
<td>20131010</td>
<td>16.03</td>
<td>I19</td>
<td>20131010</td>
<td>18.26</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2214</td>
<td>N8749F</td>
<td>413536</td>
<td>20131011</td>
<td>EYE</td>
<td>20131011</td>
<td>15.09</td>
<td>H31</td>
<td>20131011</td>
<td>15.46</td>
<td>General Aviation</td>
<td>PA22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2215</td>
<td>N89KW</td>
<td>68228</td>
<td>20131019</td>
<td>I19</td>
<td>20131019</td>
<td>23.56</td>
<td>I19</td>
<td>20131020</td>
<td>1.15</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2216</td>
<td>N89KW</td>
<td>121387</td>
<td>20131021</td>
<td>PCW</td>
<td>20131021</td>
<td>0.19</td>
<td>I19</td>
<td>20131022</td>
<td>1.22</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2217</td>
<td>N89KW</td>
<td>202905</td>
<td>20131022</td>
<td>EYE</td>
<td>20131022</td>
<td>0.21</td>
<td>I19</td>
<td>20131022</td>
<td>1.19</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2218</td>
<td>N89KW</td>
<td>289720</td>
<td>20131023</td>
<td>PCW</td>
<td>20131023</td>
<td>0.27</td>
<td>I19</td>
<td>20131023</td>
<td>1.31</td>
<td>General Aviation</td>
<td>SR22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2219</td>
<td>N310MH</td>
<td>459199</td>
<td>20131024</td>
<td>APF</td>
<td>20131024</td>
<td>16.34</td>
<td>D31</td>
<td>20131024</td>
<td>17.56</td>
<td>General Aviation</td>
<td>C310</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2220</td>
<td>N310MH</td>
<td>482345</td>
<td>20131024</td>
<td>APF</td>
<td>20131024</td>
<td>20.17</td>
<td>I19</td>
<td>20131024</td>
<td>21.26</td>
<td>General Aviation</td>
<td>C310</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2221</td>
<td>N6168H</td>
<td>459093</td>
<td>20131024</td>
<td>MSL</td>
<td>20131024</td>
<td>19.45</td>
<td>D31</td>
<td>20131024</td>
<td>21.29</td>
<td>General Aviation</td>
<td>PA32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2222</td>
<td>N6168H</td>
<td>459094</td>
<td>20131024</td>
<td>DTS</td>
<td>20131024</td>
<td>21.46</td>
<td>I19</td>
<td>20131024</td>
<td>23.54</td>
<td>General Aviation</td>
<td>PA32</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GEOSPATIAL ANALYSIS

Baltimore Protest Affected Areas
Baltimore, MD

NOTE: This product was produced in response to a short suspense request and based on the most current information at hand during creation. This product may be time sensitive.

Department of Homeland Security
Office of Cyber and Infrastructure Analysis
29 Apr 2015 1328 EDT

Riot Activity
- Protester Control Actions
- Looters
- Fire
- Alarm

IRIS
- Banking and Finance
- Chemical Facility
- Commercial Facility
- Communication
- Defense Industrial Base
- Emergency Service
- Energy
- Government Facility
- Healthcare and Public Health
- Manufacturing
- National Monument
- Transportation
- Water

NOTE: This map depicts downtown Baltimore affected areas and essential Critical Infrastructure.

Data Source: IP Gaines, ES&H WRMA

© 2015 All Rights Reserved
Department of Homeland Security
Office of Cyber and Infrastructure Analysis
Geospatial Support Team
Contact: IP_GEO@DHS.GOV
SURVEILLANCE INDUSTRIAL COMPLEX

Market Segments

- **US DoD**
  - International Defense
  - $10B

- **US Federal and International Security Organizations**
  - 10 US / 50 International
  - SBP, Sec Service, OGA, Coast Guard, National Guard, CIA

- **Federal / States Law Enforcement**
  - 10 US / 50 State / 100 International
  - FBI, DEA, SBI, SP, AG
  - Target price $5-$10M

- **Large Cities Law Enforcement**
  - 20 US / 400 International
  - LA, NY, Chicago, Phoenix, DC, ...
  - Target price $5-$7M

- **Medium Cities Law Enforcement**
  - 200 US / 2000 International
  - St Louis, Dayton, Indianapolis, Cincinnati, ...
  - Target price $1-$3M

- **Event / Location Security/ Private Security**
  - NASCAR, NFL, Parades, Events Amusement parks, Airports, Critical Infrastructure
  - Short term Operations some fixed site surveillance

- **$10B**
- **$50B**
- **$28B**
TYPES OF AIRCRAFT

- Small fixed wing (Cessnas)
- Large dual engine (Beechcraft)
- Military style (Pilatus)
- Helicopters
- Drones (Small and Large)
EQUIPMENT

- Wescam by L3 Communications
- Infrared cameras - **FLIR SAFIRE** and other models
- Cell site simulators (a.k.a. Stingrays, IMSI catchers, etc.)
- "LETC" Devices [Law Enforcement Technical Collection]
EXAMPLES OF USE

- FBI Aerial Surveillance of Freddie Grey protests
- FBI Aerial Surveillance of Arizona I-10 shooter suspect's apartment
- Phoenix PD used Pilatus to follow U-Haul thief
HIDDEN IN *PLANE SIGHT*

- FBI, CBP, DEA and DOJ use of front companies
- $10 FAA records request reveals equipment
- The Delaware problem
PHOENIX PD PLANE

FOOTAGE OBTAINED VIA PUBLIC RECORDS REQUEST FROM PHOENIX PD
VIDEO AT ARCHIVE.ORG
VIDEO AT YOUTUBE.COM
TRACKING THE SKY SPIES

- How do we more generally detect surveillance aircraft and activity?
- Registrations can be changed and obscured
- Many surveillance technologies are commercially available
- How much surveillance is happening in other parts of the world?

- Technical and operational requirements dictate flight patterns
- Surveillance flights look very different from most other traffic

SCREEN-CAPTURE BY BRIAN ABELSON. CONTENT FROM FLIGHTRADAR24.COM
TRACKING AIRCRAFT

• Tracking aircraft - radar is not practical for hobbyists

• Aircraft transponders transmit a beacon signal with a unique identifier (ICAO address)

• Protocol: *Automatic Dependent Surveillance-Broadcast (ADS-B)*

• Positions can be calculated with **multilateration**
  - Compare time difference of messages arriving at multiple receivers

• Requires 4+ receivers for accurate calculation

• Aggregator networks collect feeds from ADS-B receivers and calculate aircraft positions

• Some aircraft also transmit additional information: (latitude / longitude), call sign, altitude, etc.
  - Currently not required for all aircraft, and may not be accurate
GATHERING ADS-B DATA AT SCALE

• Active community of radio / aviation / hacking enthusiasts collect ADS-B data
• Requires a Raspberry Pi 1B+, an RTL-SDR radio, antenna, and internet connection (< $100)
• Multiple aggregators collect ADS-B data and calculate positions
  ▪ FlightRadar24.com, FlightAware.com, adsbexchange.com
• FAA regulations require an increasing number of aircraft to transmit ADS-B
  ▪ Part of the "NextGen" program
• Similar regulations in .EU, .IN, .AU, elsewhere
LIMITATIONS TO DATA

• Major commercial flight tracking sites augment their data with FAA radar data
• FAA data comes with restrictions that tracking sites do not publish positions of aircraft on the FAA's block list
• Bulk access to data is limited or expensive
• ADS-B Exchange is an exception
• Does not use FAA data, does not censor flights
• Provides free access to live & historical data
  ▪ Donation info on their site
PICKING SURVEILLANCE FLIGHTS OUT OF THE DATA

- There are over 80,000 flights a day (~10 gb / day)
- At any given time 8,000~13,000 aircraft are in the air
- Most of these are not surveillance flights
- How do we pick out the surveillance flights?
SURVEILLANCE FLIGHTS VS. OTHERS

- Most non-surveillance traffic goes from point A to B as quickly and directly as possible
- Minimizes flying over populated areas and crossing in to airports' controlled airspace

A MAP OF CONTROLLED AIRSPACE AROUND PHOENIX SKY HARBOR AIRPORT, FROM OPENAIP
TECHNICAL / OPERATIONAL CONSTRAINTS OF SURVEILLANCE FLIGHTS

- Altitude "sweet spot"
- Cell site simulators - range of ~2 miles
- Surveillance flights typically take off and land at the same airport
- Cover densely populated metro areas
- Aircraft capabilities - airspeed, power output, weight capability
SURVEILLANCE SCORE METHODOLOGY

- Calculate headings of each aircraft and increase the score each time it changes > 90 degrees
- Conditional based on altitude
  - Sweet spot is appx. 6,000 - 12,000 ft
- Future refinements:
  - Consider proximity to airports and controlled airspace
  - Score based on aircraft model
  - Increase score if on FAA block list
  - Additional geometric calulations to filter out survey activity
  - Compare flights to interesting geography -- borders, events, etc.
PATTERN BASED DETECTION

- Surveillance flights make a large number of turns
- Most flights with 30+ turns "look" like surveillance flights

SCREEN-CAPTURE BY GLOBAL REVOLUTION TV. CONTENT FROM FLIGHTRADAR24.COM
IMPLEMENTATION / ARCHITECTURE

- ADS-B Exchange
  - World's largest co-op of unfiltered flight data
  - Real-time aircraft position data

- Virtual Radar Server
  - Plot aircraft positions on a map

- RabbitMQ
  - Task queue

- Flight snippet converter

- Future: historical flight data

- Flight analysis thread 1
- Flight analysis thread 2
- Flight analysis thread n

- redis
  - In-memory geo-cache
  - Suspicious flight snapshot

- mongoDB
  - Landed / out of range flights
  - Persistent storage
  - Future: retrospective analysis

- Web map
WHAT YOU CAN DO TO TRACK SPY PLANES

- Set up an ADS-B receiver for < $100 and feed data to adsbexchange.com
- Donate to adsbexchange.com
- Use, fork, and improve our application
QUESTIONS + MORE INFO:

- https://www.nstarpost.com
- github.com/nstarpost
- twitter.com/nstarpost

For interesting links and a copy of the presentation, see https://www.nstarpost.com/defcon-25/
NOTES, LINKS, AND ERRATA:

- Airworthiness records in the US are available at [https://aircraft.faa.gov/e.gov/ND/](https://aircraft.faa.gov/e.gov/ND/)
- A recent copy of the FAA's block list is available on Muckrock, thanks to a request from Tony Webster
- The discussion of ADS-B skipped over mentioning Mode-S transmissions
  - Mode-S is a simpler protocol that does not include location data, but transmissions are locatable with multilateration
- The slide "Phoenix PD Plane" was edited to add video links, and various other links were added for reference
- The aircraft shown in the "Example" slide was speculated to be conducting speed patrols, but we believe it to be unlikely based on further research
- Machine learning is another avenue for improvement
- "LETC" was spelled out