

TRACKING SPIES IN THE SKIES



FBI CESSNA N496WW. PHOTO BY CHRIS KENNEDY

ABOUT THE TALK

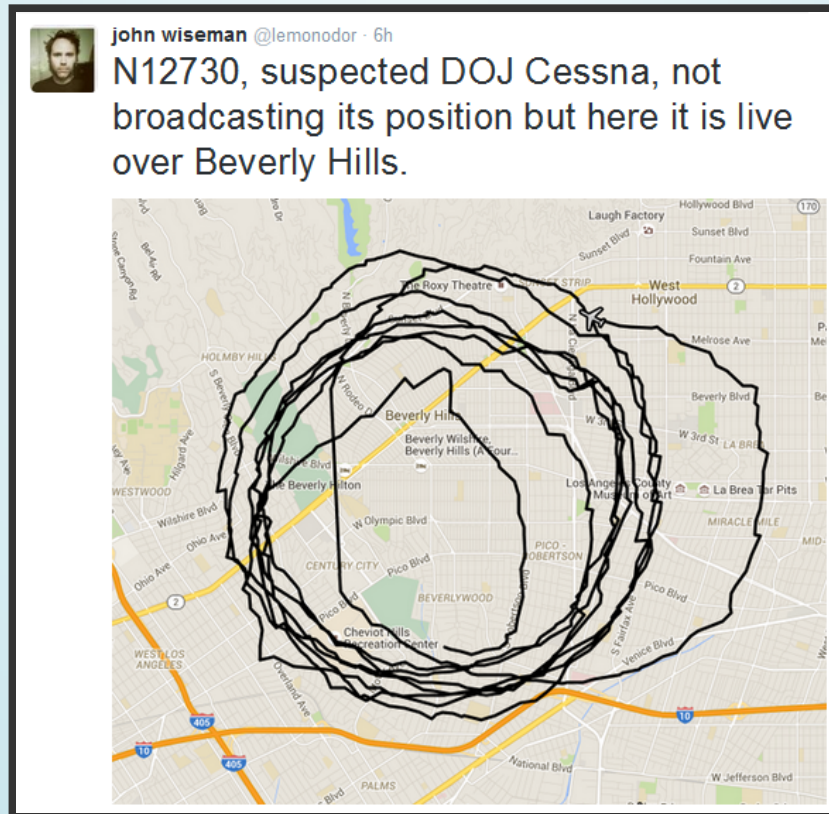
LAW ENFORCEMENT AND AERIAL SURVEILLANCE

- History of aerial surveillance (Sam Richards) [@minneapolisam](#)
- 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

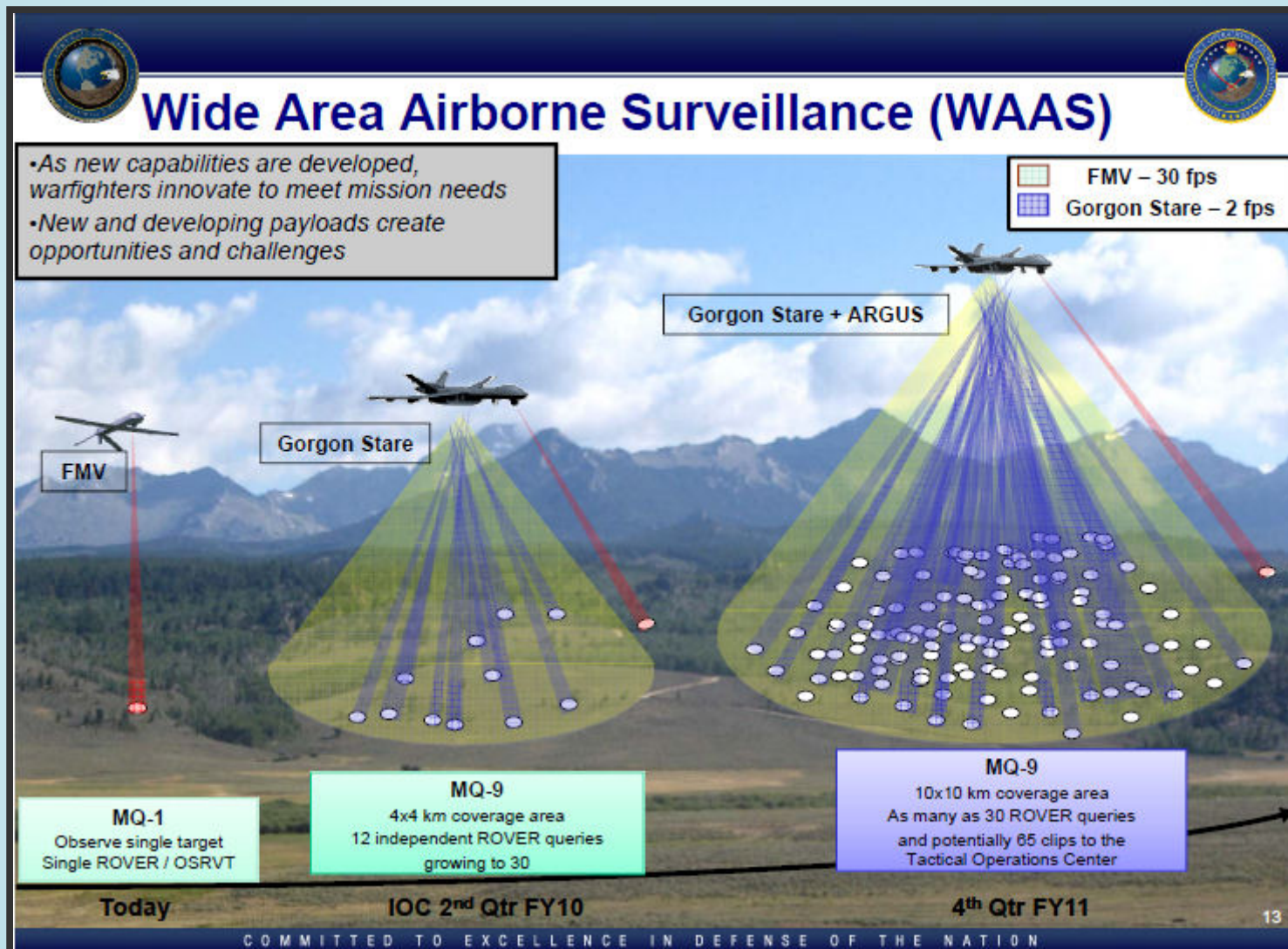


SKY SPIES 101

- 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



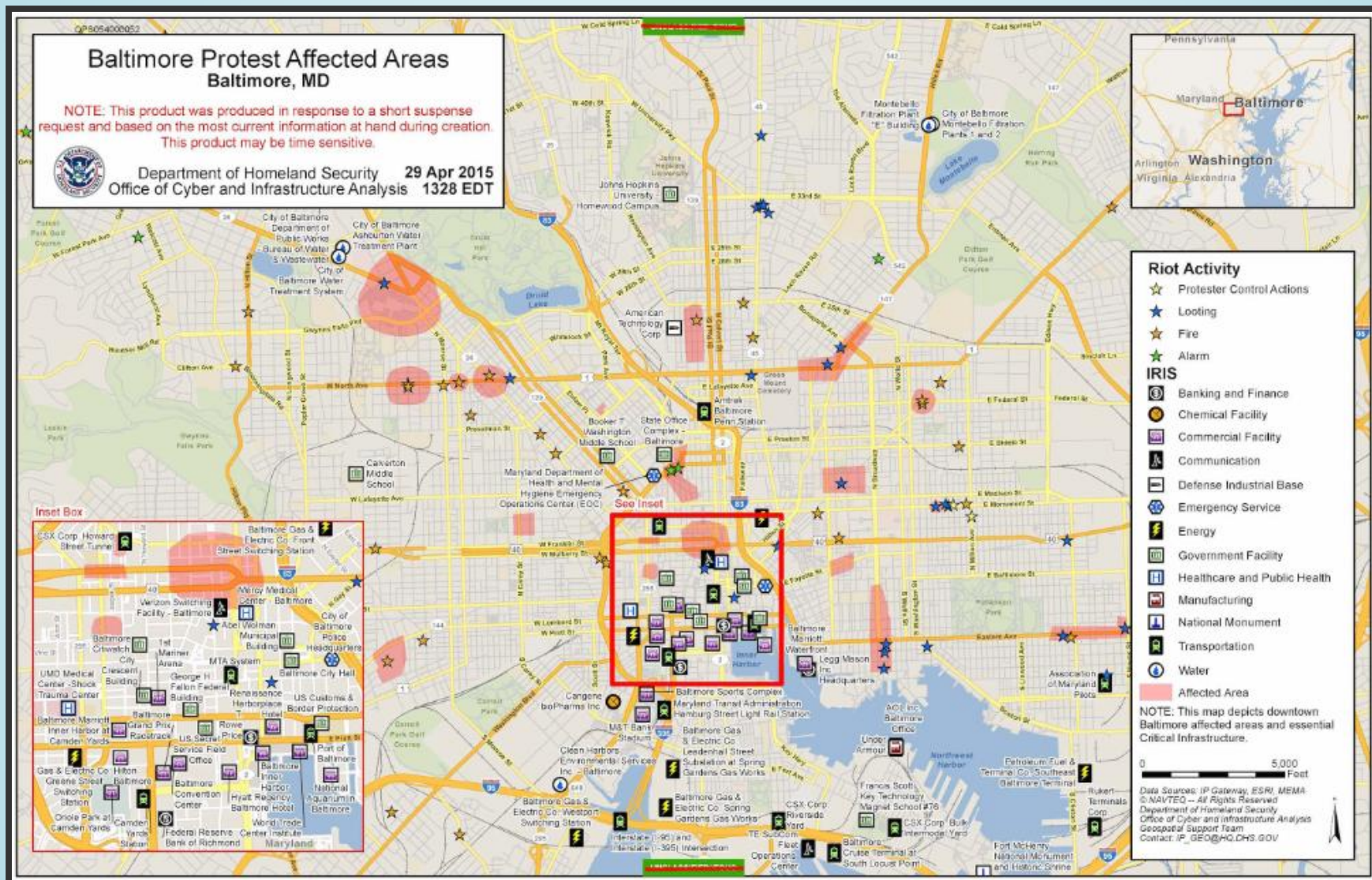
FAA FOIA DATA

A1248																	N89KW
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O		
2202	N89KW	271164	20130915317922	15-Sep-13	GVQ	20130915	18:18:00	I19	20130915	20:41:38	General Aviation	SR22					
2203	N701PM	353068	20130922841562	22-Sep-13	T94	20130922	14:02:42	GKY	20130922	15:16:00	General Aviation	SR22					
2204	N701PM	385677	20130922841566	22-Sep-13	GKY	20130922	20:46:06	5C1	20130922	21:57:49	General Aviation	SR22					
2205	N6168H	281131	20130927323321	27-Sep-13	MSL	20130927	15:28:00	MNV	20130927	16:37:00	General Aviation	PA32					
2206	N6168H	284780	20130927323322	27-Sep-13	MNV	20130927	18:49:00	MSL	20130927	19:56:56	General Av						
2207	N6168H	239354	20131003787450	3-Oct-13	MSL	20131003	15:32:00	APF	20131003	19:37:47	General Av						
2208	N89KW	24893	20131006028050	6-Oct-13	I19	20131006	23:23:00	I19	20131007	1:03:40	General Av						
2209	N310MH	65973	20131007073864	7-Oct-13	APF	20131007	13:36:00	MYEH	20131007	15:14:52	General Av						
2210	N6168H	32305	20131007039763	7-Oct-13	APF	20131007	11:15:00	MSL	20131007	15:19:48	General Av						
2211	N89KW	87110	20131008126384	8-Oct-13	EYE	20131008	0:11:00	I19	20131008	1:10:28	General Av						
2212	N310MH	223646	20131009201185	9-Oct-13	APF	20131009	11:47:14	JZI	20131009	14:34:00	General Av						
2213	N310MH	332087	20131010347001	10-Oct-13	JZI	20131010	16:03:00	APF	20131010	18:26:31	General Av						
2214	N8749F	413536	20131011417177	11-Oct-13		20131011	15:09:40	HNB	20131011	15:45:04	General Av						
2215	N89KW	68228	20131019024446	19-Oct-13	I19	20131019	23:56:00	I19	20131020	1:15:00	General Av						
2216	N89KW	121387	20131021162775	21-Oct-13	PCW	20131021	0:19:57	I19	20131021	1:22:37	General Av						
2217	N89KW	202905	20131022247472	22-Oct-13	EYE	20131022	0:21:00	I19	20131022	1:19:00	General Av						
2218	N89KW	289720	20131023329460	23-Oct-13	PCW	20131023	0:27:00	I19	20131023	1:31:40	General Aviation	SR22					
2219	N310MH	461999	20131024469100	24-Oct-13	APF	20131024	16:34:55	DAB	20131024	17:56:19	General Aviation	C310					
2220	N310MH	482343	20131024469108	24-Oct-13	DAB	20131024	20:17:03	APF	20131024	21:25:55	General Aviation	C310					
2221	N6168H	452803	20131024487443	24-Oct-13	MSL	20131024	19:45:00	DTS	20131024	21:23:38	General Aviation	PA32					
2222	N6168H	452621	20131024487444	24-Oct-13	DTS	20131024	21:45:00	MSI	20131024	23:54:13	General Aviation	PA32					

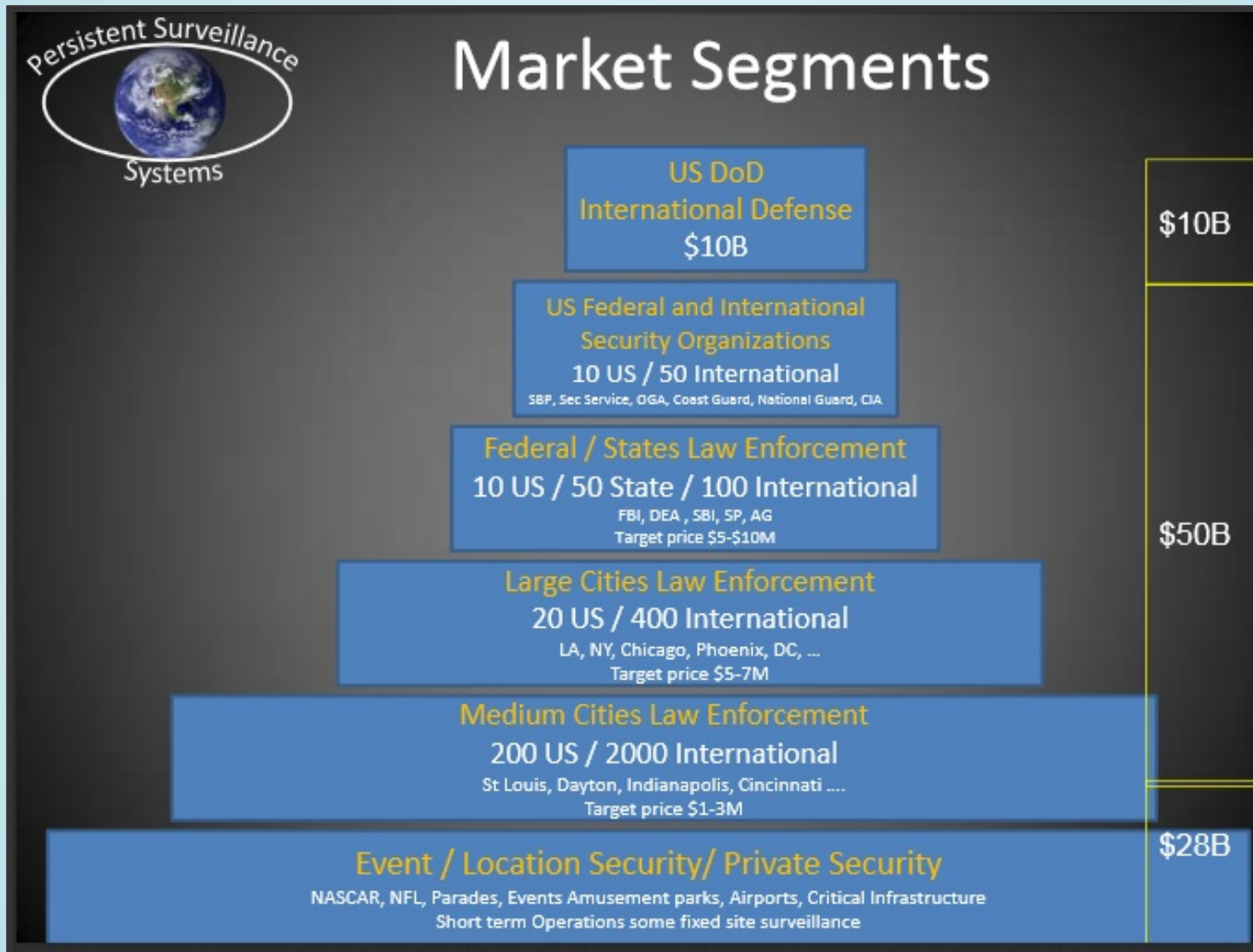
www.pss-1.com



GEOSPATIAL ANALYSIS



SURVEILLANCE INDUSTRIAL COMPLEX



TYPES OF AIRCRAFT

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



PHOENIX PD PILATUS PC-12. PHOTO BY CHRIS KENNEDY

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

2.0 GENERAL INFORMATION

2.1 DESCRIPTION

This installation provides locates an MX-15HDi EO/IR Sensor in the lower fuselage pressure box previously installed by STC SA1811CE and installs two (2) LETC Antenna Arrays on the lower fuselage skin.

Installation of the LETC Arrays required the relocation of several existing antennas, all current antenna locations are defined in D/N 01890002 Antenna Arrangement.

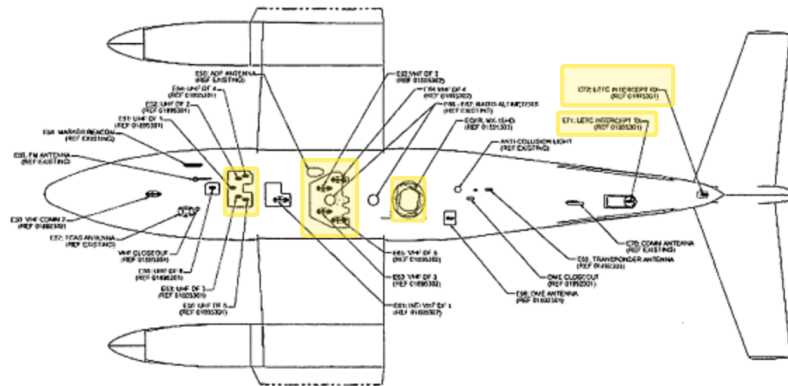
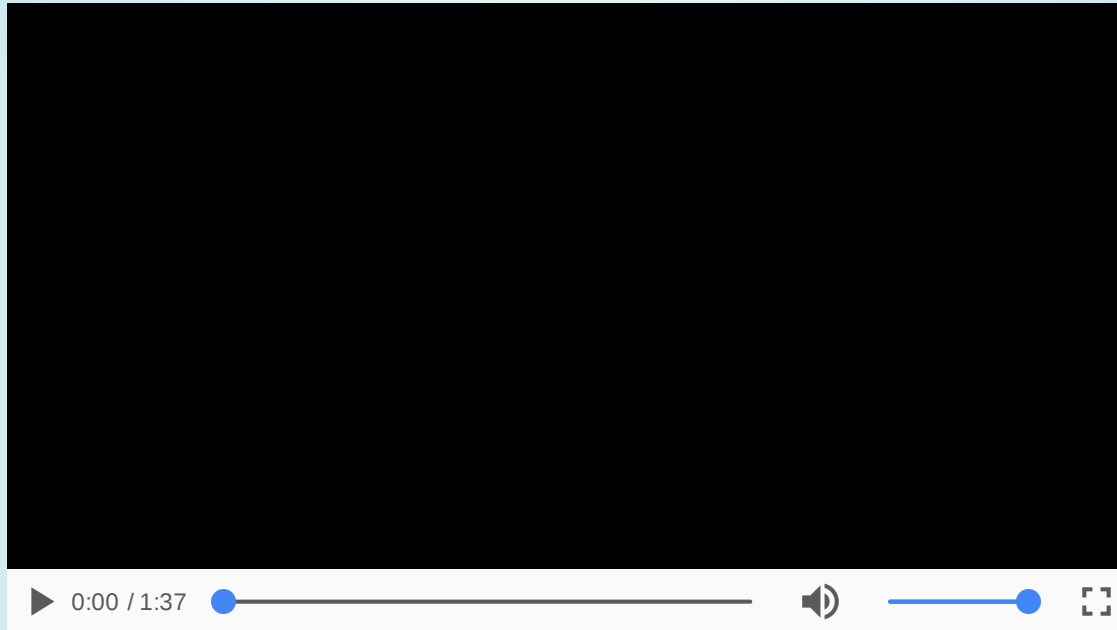


Figure 1: Lower Fuselage

2.2 LOCATION OF ACCESS PANELS

The VHF Comm Antenna is installed on the forward lower access panel, which is utilized for

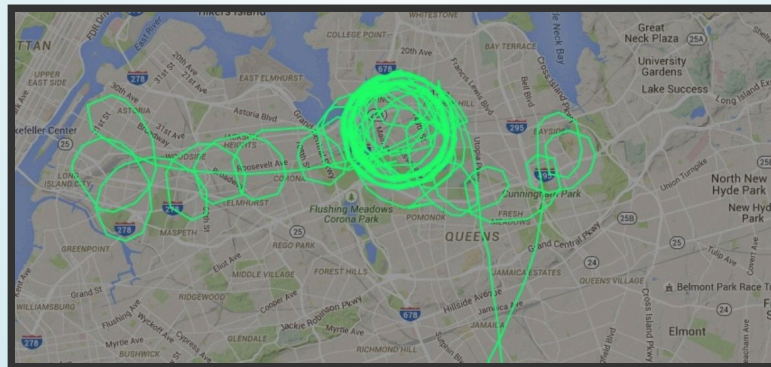
PHOENIX PD PLANE



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](https://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

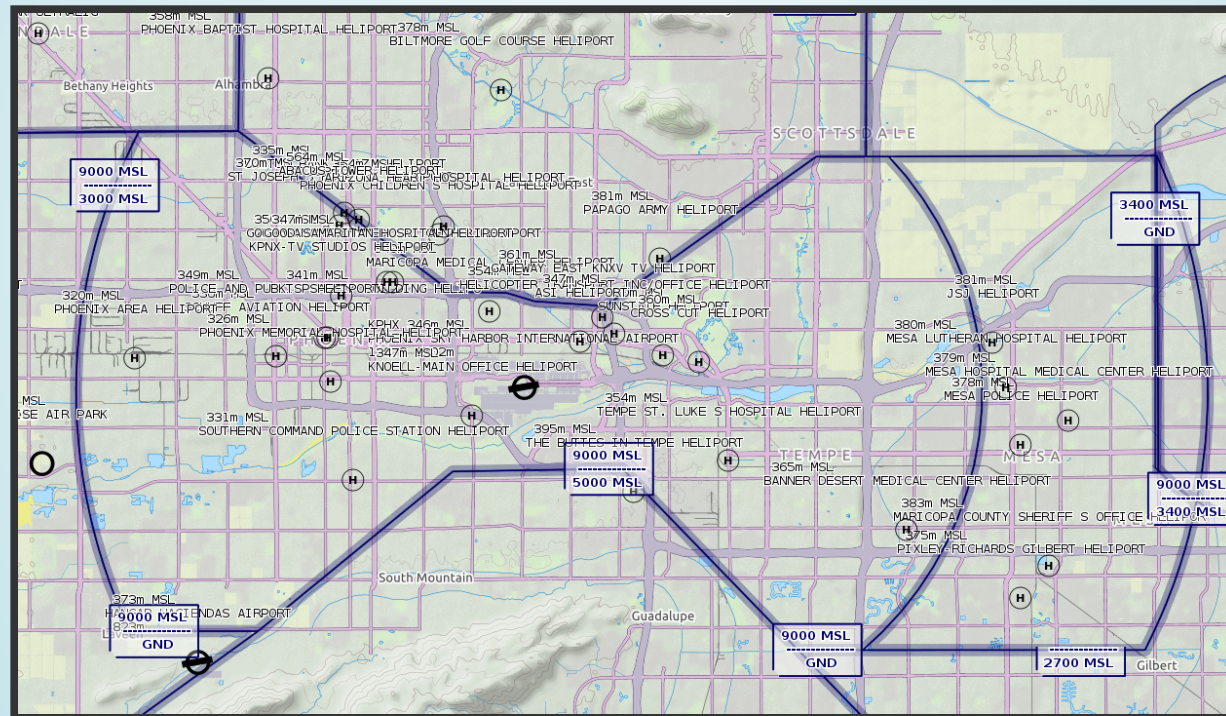
- Major commercial flight tracking sites augment their data with FAA radar data
- FAA data comes with restrictions that tracking sites do not publish positions of aircraft on the [FAA's block list](#)
- Bulk access to data is limited or expensive
- ADS-B Exchange is an exception
- Does not use FAA data, 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

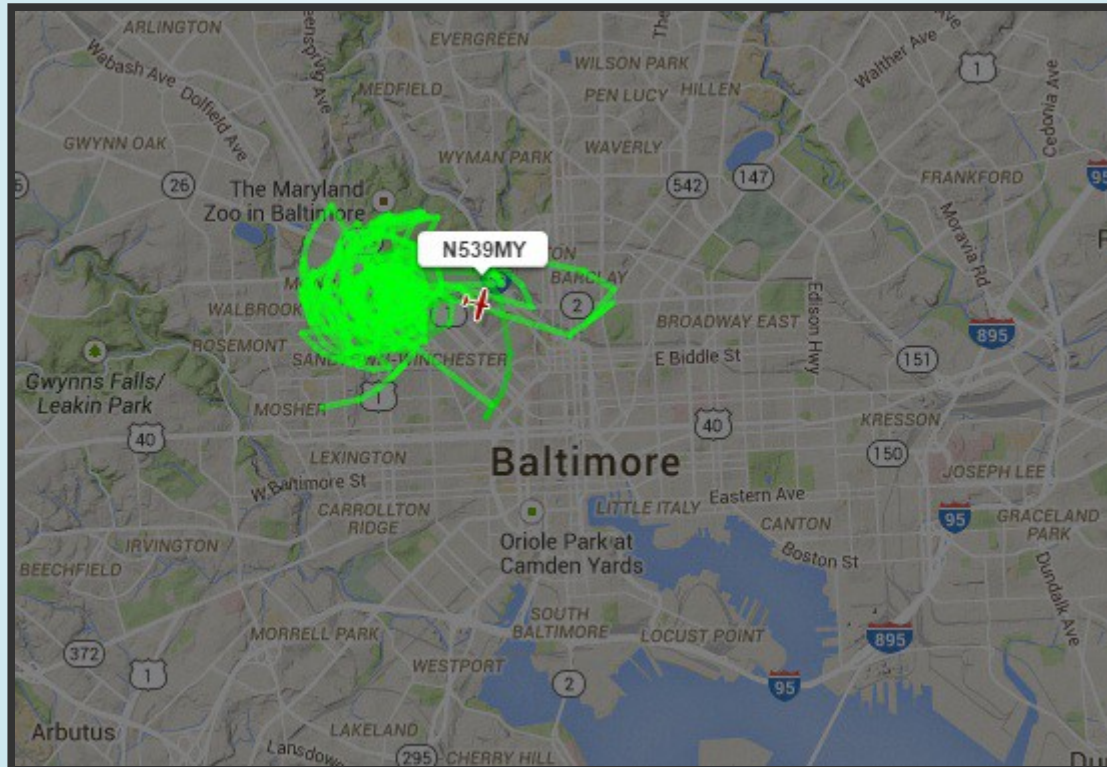
- Altitude "sweet spot"
- Cell site simulators - range of ~2 miles
- Surveillance flights typically take off and land at the same airport
- Cover densely populated metro areas
- Aircraft capabilities - airspeed, power output, weight capability

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 calculations to filter out survey activity
 - Compare flights to interesting geography -- borders, events, etc.

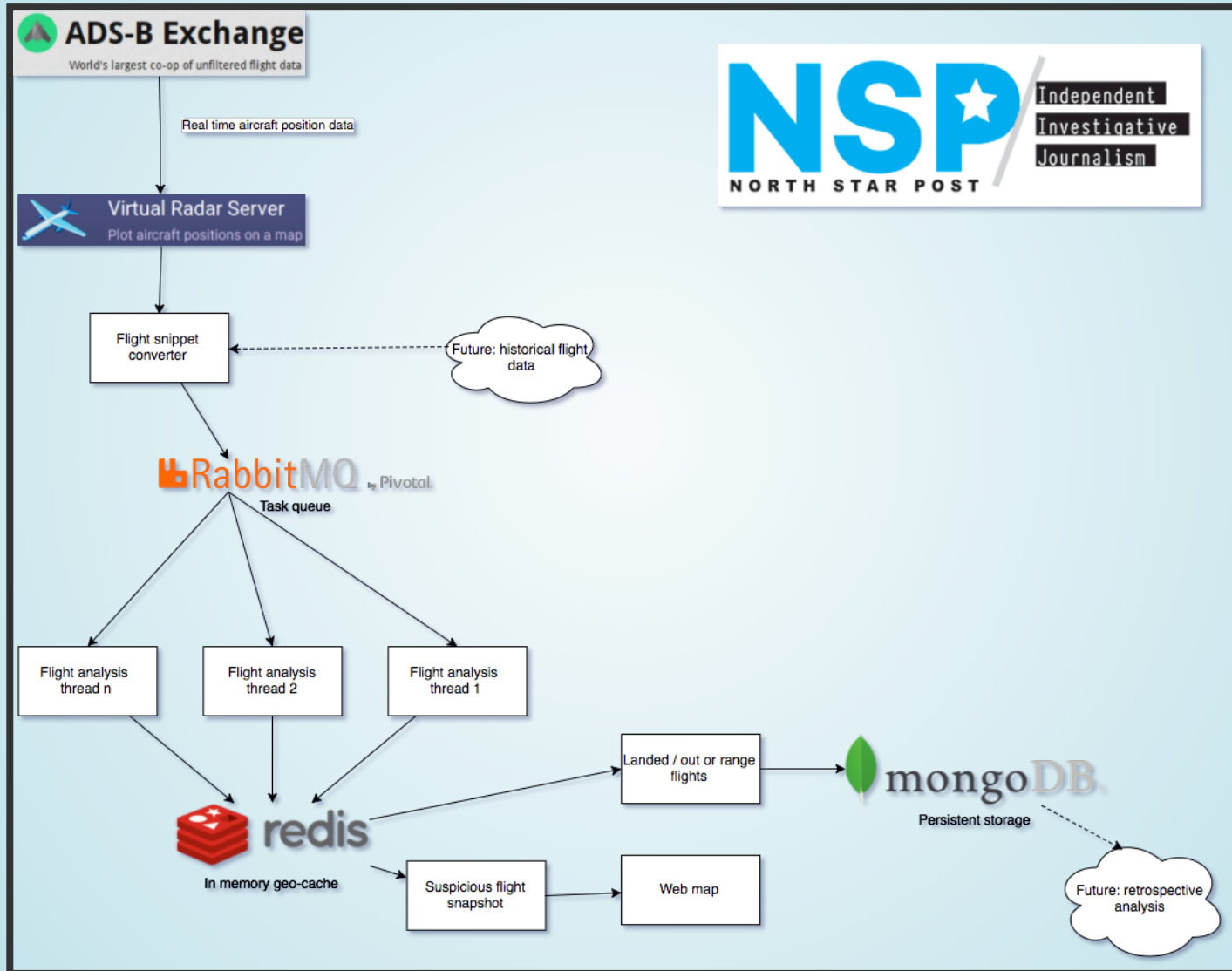
PATTERN BASED DETECTION

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

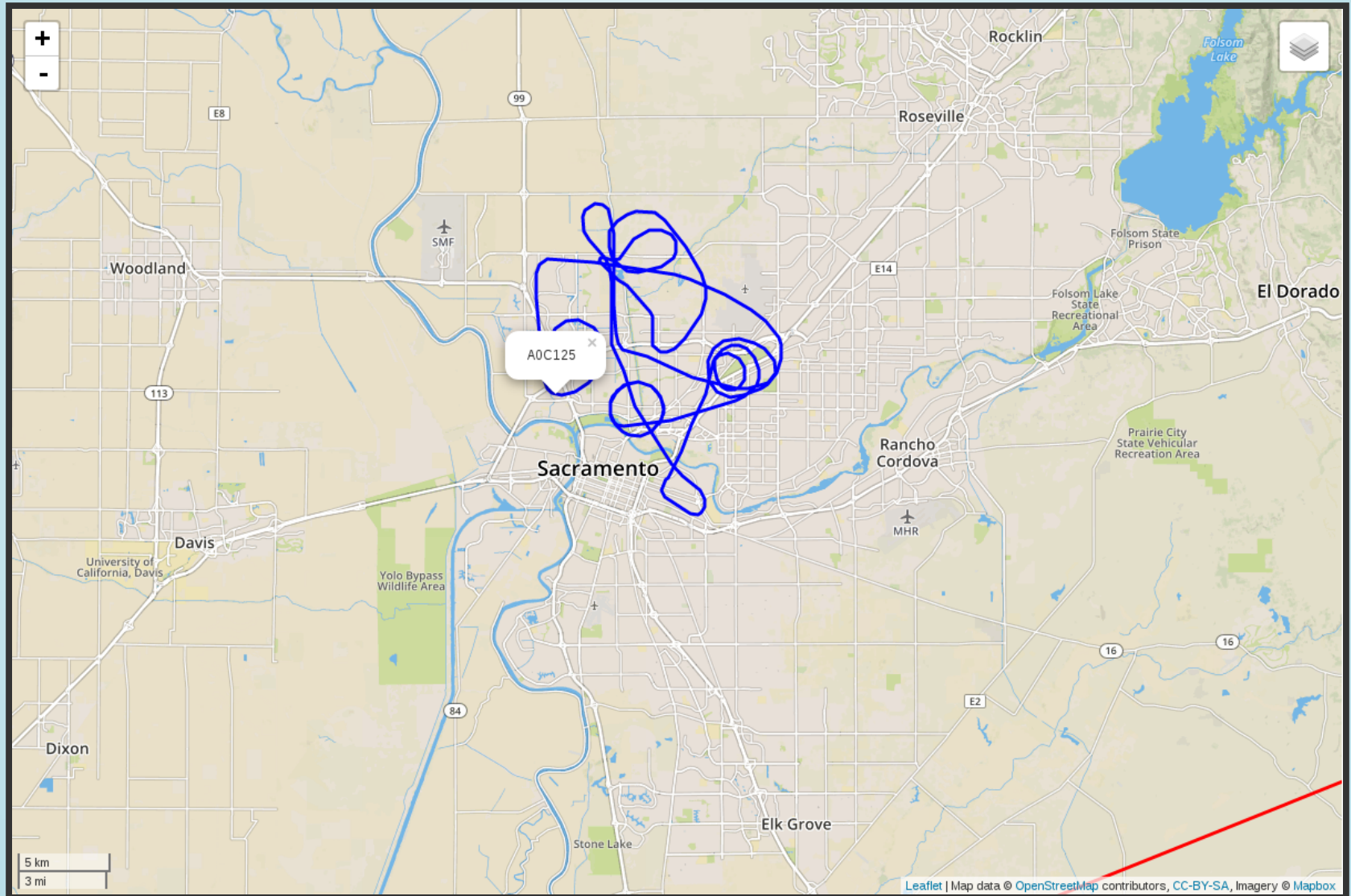


SCREEN-CAPTURE BY GLOBAL REVOLUTION TV. CONTENT FROM FLIGHTRADAR24.COM

IMPLEMENTATION / ARCHITECTURE



EXAMPLE



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/>
- 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