

NATIONAL CRITICAL
INTELLIGENCE ESTIMATE:
UNMANNED AIRCRAFT SYSTEMS
IN THE UNITED STATES

Team Draco Volans



John Boesen

Randy Mai

Vincent Salerno (TL)

For Approval: Professor Emeritus, Randall K. Nichols

Agenda

- ❑ EXECUTIVE SUMMARY
- ❑ sUAS MARKET & SAFETY
 - ❑ Facts
 - ❑ Issues
 - ❑ Indicators
 - ❑ Judgments
 - ❑ Recommendations
- ❑ UNMANNED UNDERWATER VEHICLES

Agenda

- FEDERAL AIR ADMINISTRATION RULES & PROPOSALS ON UAS
 - Facts
 - Issues
 - Indicators
 - Judgments
 - Recommendations

Agenda

- ❑ CYBER-TERRORISM / COUNTER CYBER-TERRORISM IMPLICATIONS OF UAS
 - ❑ Facts
 - ❑ Cyber Security Architecture (CSA)
 - ❑ Issues
 - ❑ Indicators
 - ❑ Judgments
 - ❑ Recommendations
- ❑ Glossary
- ❑ References

Executive Summary

- ❑ National Critical Intelligence Estimate (NCIE) was developed for Unmanned Aircraft Systems (UAS) in the United States
- ❑ This NCIE is separated into three categories:
 - ❑ sUAS Market and Safety
 - ❑ Federal Air Administration Rules and Proposals on UAS
 - ❑ Cyber-Terrorism / Counter Cyber-Terrorism Implications of UAS
- ❑ Each category has three issues and broken down by: Facts, Indicators, Judgments, and Recommendations with Cyber-Terrorism / Counter Cyber-Terrorism Implications of UAS including Cyber Security Architecture

Executive Summary

Issues

- ❑ Issues: sUAS Market and Safety
 - ❑ America is facing a distribution of sUAV into its NAS, how will the FAA contend with sUAV carrying components and materials safely without invading privacy in areas they have never operated in before? Will FAA's efforts be harmonized internationally?
 - ❑ What are the Safety issues created by sUAV and will increased sales compound this issue and how?
 - ❑ Considering increased numbers of sUAV how is the best way to integrate them into the national air effectively and safely?

Executive Summary

Issues

- Issues: Federal Air Administration Rules and Proposals on UAS
 - What rules and regulations can the FAA enact to ensure the safety and privacy of Americans from amateur or malevolent use of UAS?
 - Is registration of UAS impossible for the FAA?
 - What are the most effective technologies the FAA can implement to incorporate UAS into the NAS?

Executive Summary

Issues

- ❑ Issues: Terrorism/ Counter-Terrorism Implications of UAS
 - ❑ What are the risks to U.S. national security from open source information on its UAS performance?
 - ❑ While increasing surveillance via UAS, how will the U.S. safeguard American citizen Rights to Privacy?
 - ❑ What best practices can assist the FAA in creating (dynamic and/or scalable) public policy that incorporates UAS training, safety assessment, regulation, and countermeasures for preventing collisions?

Executive Summary

- ❑ Those nine issues were addressed for UAS to be safely integrated into the NAS without:
 - ❑ Reducing capacity
 - ❑ Decreasing safety
 - ❑ Negatively impacting current operators
 - ❑ Increasing the risk to NAS users or persons and property on the ground
- ❑ Recommendations for safe integration of UAS into NAS
- ❑ Conclusion:
 - ❑ Technology outstrips the legal regulations for UAS in the U.S.
 - ❑ Long range solutions require a multi-disciplinary approach

Executive Summary

Recommendations: sUAS Market and Safety

Accident Database – Expanded on FAA’s current Accident Database but a separate one for UAS only.

Beacon Enabled – Navigation lights

Capability and Payload – must have detailed guidelines as to the capability of the drone and its payload. Can it fly above 400ft? Is it capable of FPV (First Person View), Speed et al? Does it carry hazardous material? Is it autonomous? Does it have a camera?

Preflight check list – FAA approved checklist for amateur users of UAS

Regulated Drone Highways – Intercommunication of the drones to avoid collision. Need to develop a great centralized air traffic control system. This would assist the drone on determining the locations and distance of other flying gadgets.

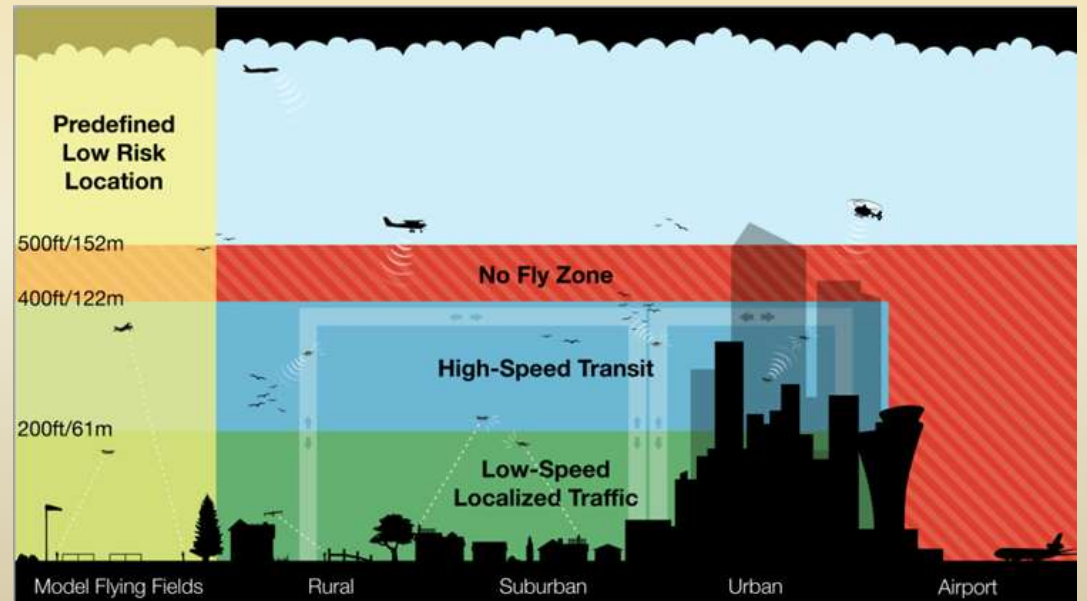
Sense and Avoid – Stage 1 Morphological Filtering, 2 Classify points of interest, 3 Non-Max Suppression (Eliminates multiple detection), 4 Tracking

Tracking system – Radar(Scattering/Reflection EMS, MIMO Multi Input Multi Output), Transponder(Comm.), Electro Optical(Video), Acoustic (Sound), GPS(Position), Radio(Comm. Link), Thermal(Temp), Linked Detection (Comm.)

Executive Summary

Recommendations: sUAS Market and Safety –Smart Skies Project

- Regulated Drone Highways for commercial package delivery
- Capability and Payload should determine Regulation requirement
- Beacon enabled by photocell
- Registered drones broadcast ID
- Pre-flight checklist added to box by manufacture and FAA rules and regs.
- FAA registration for commercial drones
- Sense & Avoid, Low Cost Radar, Mobile Radar
- Geofencing
- Training
- Optical –Electro Vision Systems



Executive Summary

Recommendations: Federal Air Administration Rules and Proposals on UAS

Certificates – Use of experimental certificates and exemptions to temporary regulations will not give FAA power to regulate the UAS market. Certifications for private citizens, companies and institutions need to be clearly defined for use of UAS.

Geofencing – Technology: Systems using GPS and mapping systems that set virtual boundaries around actual places, impose geographical limits on their movement and prevent UAS from going into undesignated airspace needed for all UAS military, private or commercial.

Insurance – Blanket Liability, Third Party/Product/War/Privacy and Trespass Liability. Use of liability coverage necessary, some companies already advertising for coverage on many types of sUAS with full coverage on damage to the sUAS.

Registration – Total registration of all UAS is not possible it needs to be voluntary with no fees or fines or else there will be no way to enforce registration with such widespread growth of the UAS market.

Sense and Avoid – Technology: Detect and Avoid and communication systems.

Tracking system – Technology: Using air traffic control systems and location broadcasting systems UAS need to be accounted for and be visible to all other aircraft manned or unmanned.

Training – Eight hours of voluntary training to certify UAS pilots for all sUAS, can be online videos or simulations run by commercial and / or FAA entities or classes hosted by FAA certified instructors.

Executive Summary

Recommendations: Cyber-Terrorism / Counter Cyber-Terrorism Implications of UAS

ASIC Chips – Improves performance and moves away from open source. Cryptographic Swap Type-1 ASIC chips used by NSA for encryption.

Automated Electro-Optical – mid-air collision avoidance system to provide UAS with sense and avoid (SAA) capability.

Automated static obstacle avoidance – system to support safe operation of unmanned rotorcraft at low altitudes and in unknown environments.

Cybersecurity – as computing of crafts increase due to sense and avoid, GPS, communications. Security and hardware must be hardened to exist in environments with increasing threats.

Global Automated Separation Management System – to manage complex air traffic scenarios involving manned and unmanned aircraft.

Mobile ground-based air traffic surveillance system – to provide UAS operators with information about local air traffic environment.

Sense and Avoid – SAA for UAS must have top priority in Critical Infrastructure public policy including comprehensive rules to enable and support ‘file and fly’ and implementation of public policy before a manned aircraft collides with a UAS in the NAS.

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

- ❑ **FAA must treat UAS as one of many Critical Infrastructures in the U.S.**
- ❑ **Add robust cybersecurity regulations, policy, and guidance**
 - ❑ **Strengthen security related certification criteria**
 - ❑ **Standardize and harmonize between domestic and international regulatory authorities**
- ❑ **The FAA must have an official public policy for UAS in the NAS, so it's prepared to mitigate the risk of a UAS collision with a piloted aircraft, whether by attack or accident**

Cyber Terrorism / Counter Terrorism Implications - Recommendations

U.S. must classify formerly open source information on its UAS performance.

- ❑ The U.S. must safeguard privacy and constitutional freedoms while increasing surveillance via UAS, to protect critical infrastructures.
- ❑ The FAA must create a dynamic and scalable UAS public policy that incorporates UAS training as a top priority, and include safety assessment, regulation, and countermeasures for preventing collisions.

Cyber Terrorism / Counter Terrorism Implications - Recommendations

- ❑ SAA for UAS must have top priority in Critical Infrastructure public policy
 - ❑ Include comprehensive rules to enable and support ‘file and fly’
 - ❑ Implement public policy before a manned aircraft collides with a UAS in the NAS
- ❑ FAA must follow best practices of the Smart Skies Project
 - ❑ Must include ways and means for training UAS operators to
 - ❑ Avoid midair collisions
 - ❑ Demonstrate proficiency in collision avoidance
 - ❑ Must require all UAS to have active detection technology installed
 - ❑ Must require orientation of UAS operators to local GBSAA installations

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- Automated Electro-Optical (EO) mid-air collision avoidance system to provide UAS with SAA capability
- Automated static obstacle avoidance (SOA) system to support safe operation of unmanned rotorcraft at low altitudes and in unknown environments
- Mobile ground-based air traffic surveillance system (MATS) to provide UAS operators with information about local air traffic environment
- Global Automated Separation Management System (ASMS) to manage complex air traffic scenarios involving manned and unmanned aircraft

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Automated Electro-Optical (EO) System
 - ❑ Detect and Avoid System (DAS) a.k.a. Sense and Avoid (SAA)
 - ❑ DAS solution particularly suited to small fixed-wing UAS
 - ❑ DAS required to make use of existing cost-effective sensing and processing capabilities already on-board a typical UAS
 - ❑ Aware of size, weight, power, and cost-constraints of sUAS platforms
- ❑ Provides sUAS with suitable detect and avoid capability, a decision aid to pilots, and improves the safety of manned and unmanned aviation operations

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Automated static obstacle avoidance (SOA) system to support safe operation of unmanned rotorcraft at low altitudes and in unknown environments
 - ❑ Be suitable for use in unknown outdoor environments
 - ❑ Use sensors appropriate for weight, cost, and power consumption of mini unmanned helicopters
 - ❑ Enable inspection of remote pieces of infrastructure Beyond the Visual Light Of Sight (BYLOS) of the aircraft controller
 - ❑ Be robust through intermittent communications
 - ❑ Capable of avoiding common obstacles including trees and structures and capture imagery of inspection target
- ❑ Uses lightweight COTS sensors, simple perception methods, and reactive behaviors to achieve autonomous obstacle avoidance

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Mobile ground-based air traffic surveillance (MATS) system to provide UAS operators with information about local air traffic environment
 - ❑ Use low-cost and portable primary surveillance radar (PSR) that supports UAS operations at any location
 - ❑ Supplemented with other surveillance systems
 - ❑ Automatic Dependent Surveillance – Broadcast (ADS-B) to enhance the airspace picture provided to the UAS pilot, who uses MATS sensor information to keep the UAS well clear of other aircraft
 - ❑ Ability to sense and avoid satisfies a key requirement for flying UAS in the NAS
- ❑ Can assist UAS operations and provide information about local airspace users to UAS pilots to keep UAS clear of other aircraft

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Global Automated Separation Management System (ASMS) to manage complex air traffic scenarios involving manned and unmanned aircraft
 - ❑ Provides air traffic separation services for complex Air Traffic Management (ATM) scenarios
 - ❑ Involving a mix of manned and unmanned aircraft from any country
 - ❑ Improve the efficiency and flexibility of ATM for future airspace environments
 - ❑ Scenarios involve large numbers and diverse mix of cooperative and uncooperative airspace users
- ❑ Remotely located computing, commercial data links, and aircraft-based flight management systems provide separation services for complex ATM scenarios, reduce the workload of air traffic controllers, improve efficient use of airspace, and maintain and improve current safety levels



NATIONAL CRITICAL
INTELLIGENCE ESTIMATE:
SUAV MARKET AND SAFETY

Market and Safety - Facts

UAV!#*@! Call the
FAA!!



UAVS CAN BE HAZARDOUS TO LOW-FLYING PILOTS

Don't Bet the Farm by Putting UAV Operations Above Pilot Safety.

Small UAVs can be virtually invisible—and potentially lethal—to agricultural pilots, emergency medical helicopters, law enforcement and other low-flying aircraft operating in the same airspace. Birds smaller than many UAVs have collided with aircraft, blowing through cockpit windows, disabling engines and killing pilots in the process.

Here's what you can do as a safe and responsible UAV operator:

- Get certified and well-trained in operating a UAV
- Equip UAVs with strobe lights and tracking technology, like an ADS-B Out system
- Follow the law—always give the right-of-way to the manned aircraft
- Coordinate with local aircraft operators about your UAV operations
- Carry sufficient UAV liability insurance

A UAV collision could have far-reaching consequences. An ag pilot's fatal collision with an unmarked meteorological tower resulted in millions of dollars in liability for the farmer, landowner and tower manufacturer. UAV operators could be similarly culpable for a midair collision.

Fly with care. Don't put your livelihood and pilots' lives at risk.



A message brought to you by your local aerial applicator and

Learn more at AgAviation.org/uavsafety | Knowbeforeyoufly.org | Thinkbeforeyoulaunch.com

Market and Safety - Facts

Tracking of accidents
1999-2011,
Military UAV

RQ004 UAV MISHAP HISTORY								
YEAR	CLASS A		CLASS B		DESTROY		HOURS	CUM HOURS
	#	RATE	#	RATE	A/C	RATE		
FY99	1	375.94	0	0	1	375.94	266	266
FY00	1	221.73	0	0	0	0.00	451	717
FY01	0	0.00	0	0.00	0	0.00	486	1203
FY02	2	127.71	0	0.00	2	127.71	1566	2769
FY03	0	0.00	0	0.00	0	0.00	779	3548
FY04	0	0.00	0	0.00	0	0.00	1375	4923
FY05	0	0.00	1	34.99	0	0.00	2858	7781
FY06	0	0.00	0	0.00	0	0.00	3568	11349
FY07	0	0.00	0	0.00	0	0.00	5972	17321
FY08	0	0.00	0	0.00	0	0.00	6634	23955
FY09	1	13.75	0	0.00	0	0.00	7274	31229
FY10	0	0.00	0	0.00	0	0.00	8322	39551
FY11	1	7.56	1	7.56	0	0.00	13232	52783
5 YR AVG	0.4	4.83	0.2	2.41	0.0	0.00	8286.8	
10 YR AVG	0.4	7.75	0.2	3.88	0.2	3.88	5158.0	
LIFETIME	6	11.37	2	3.79	3	5.68	52783	

UPDATED 28-DEC-11

Market and Safety - Facts

- Drone pilots have to follow flight rules and abide by air space classes for safety purposes:
 - Flight Rules
 - Visual Flight Rules (VFR)
 - Instrument Flight Rules (IFR)
 - Special VFR (SVFR)

Table 4.1 Summary of airspace classes and their basic characteristics

Airspace Class	Controlled					Non-controlled	
	A	B	C	D	E	F	G
IFR allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SVFR allowed	Yes	Yes	Yes	Yes	Yes	No	No
VFR allowed	No	Yes	Yes	Yes	Yes	Yes	Yes
Separation	For all aircraft	For all aircraft	IFR/IFR IFR/VFR	IFR/IFR	IFR/IFR	IFR/IFR if possible	None
Traffic information	–	–	VFR/VFR	IFR/VFR VFR/VFR	For all aircraft if possible	For all aircraft if possible and requested	For all aircraft if possible and requested
Clearance required	Yes	Yes	Yes	Yes	Only for IFR	No	No

Market and Safety - Facts

UAS Pilots Need to know

Always remember:

 <p>You are responsible for each flight</p>	<p>You are legally responsible for the safe conduct of each flight.</p> <p>Take time to understand the rules - failure to comply could lead to a criminal prosecution.</p>	 <p>Keep your distance</p>	<p>It is illegal to fly your unmanned aircraft over a congested area (streets, towns and cities).</p> <p>Also, stay well clear of airports and airfields.</p>
 <p>BEFORE each flight, check drone for damage</p>	<p>Before each flight check that your unmanned aircraft is not damaged, and that all components are working in accordance with the Supplier's User Manual.</p>	 <p>Keep your distance 50 metres</p>	<p>Don't fly your unmanned aircraft within 50m of a person, vehicle, building or structure, or overhead groups of people at any height.</p>
 <p>Drone is in sight at all times</p>	<p>You must keep the unmanned aircraft within your sight at all times.</p>	 <p>Consider rights of privacy</p>	<p>Think about what you do with any images you obtain as you may breach privacy laws. Details are available from the Information Commissioner's Office.</p>
 <p>YOU are responsible for avoiding collisions</p>	<p>You are responsible for avoiding collisions with other people or objects - including aircraft.</p> <p>Do not fly your unmanned aircraft in any way that could endanger people or property.</p>	 <p>Permission to use drones for paid work</p>	<p>If you intend to use an unmanned aircraft for any kind of commercial activity, you must get a 'Permission' from the Civil Aviation Authority, or you could face prosecution. For more details, visit www.caa.co.uk/uas</p>

Market and Safety - Facts



I FLY SAFE

All drones are aircraft—even the ones at the toy store.
So when I fly a drone I am a pilot.
Before I fly I always go through my pre-flight check list.
I regularly check the safety guidelines at [faa.gov/uas](https://www.faa.gov/uas)

FLY SMART, FLY SAFE, AND HAVE FUN!

 Federal Aviation Administration

[knowbeforeyoufly.org](https://www.knowbeforeyoufly.org) | [faa.gov/uas](https://www.faa.gov/uas)

PRE-FLIGHT CHECKLIST

- ▶ I fly below 400 feet
- ▶ I always fly within visual line of sight
- ▶ I'm aware of FAA airspace requirements: [faa.gov/go/uastfr](https://www.faa.gov/go/uastfr)
- ▶ I never fly over groups of people
- ▶ I never fly over stadiums and sports events
- ▶ I never fly within 5 miles of an airport without first contacting air traffic control and airport authorities
- ▶ I never fly near emergency response efforts such as fires
- ▶ I never fly near other aircraft
- ▶ I never fly under the influence

Market and Safety - Facts

A Map of Where All the Drones Live in the United States



Military Only

Market and Safety - Facts

- ❑ Example of flight paths of Remotely Piloted Aircraft – Military
- ❑ After 2015 projected 400,000 sUAV to be sold in U.S.
- ❑ No way to predict their flight paths



Market and Safety - Facts

- Additional Commercial uses
 - Recreational Photography
 - Mapping
 - Real Estate
 - Cinematography
 - Public safety (other than police)
 - Expanded Agriculture uses
 - Oil, gas, and mineral exploration

Market and Safety - Facts

- ❑ Consumer drone industry growing @ 15 – 20% annually
- ❑ U.S. largest consumer market in the world
- ❑ The market place braces for the effects of ruling to be realized
- ❑ Lower prices on higher end hardware and software create ease of access for larger amounts of people to gain access to drone products

Market and Safety - Facts

- ❑ Other drivers in private and commercial drone markets:
 - ❑ More advanced technology
 - ❑ Explosion in advancements of portable professional photography and videography
 - ❑ Number of drone companies launched
 - ❑ Remote sensing
 - ❑ Aerial surveillance

Market and Safety - Facts

- ❑ Increased capabilities
- ❑ Inspecting
- ❑ Evaluation / Management
- ❑ Delivery / Laborious Tasks
- ❑ Autonomy - AI

Market and Safety - Facts

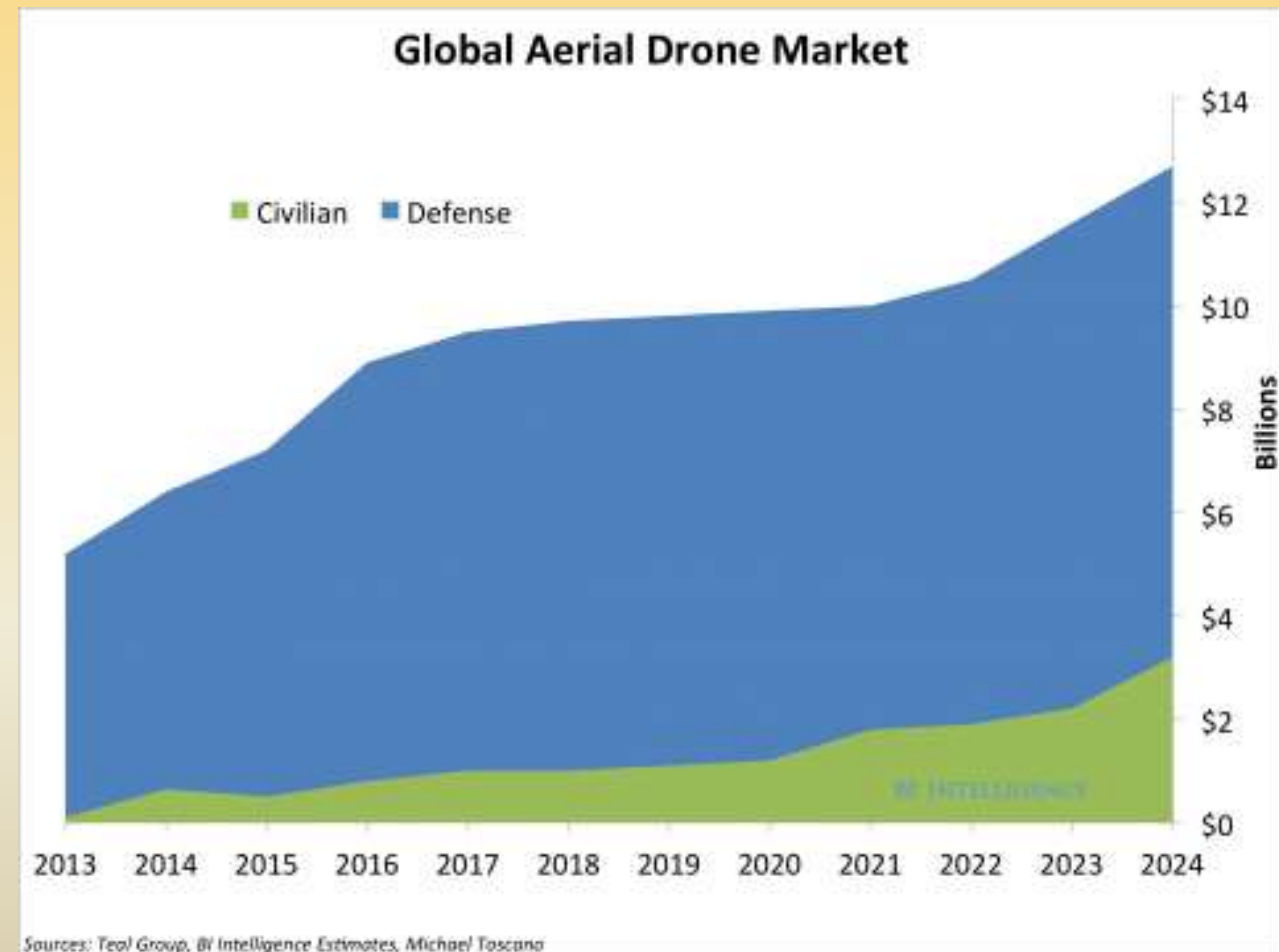
- ❑ Increase in regulation
- ❑ Lowering of price
- ❑ Increase in technology i.e. self training software
- ❑ Increase of uses
- ❑ Increase in insurance purchases
- ❑ Increase of accidents / incidents

Market and Safety - Facts

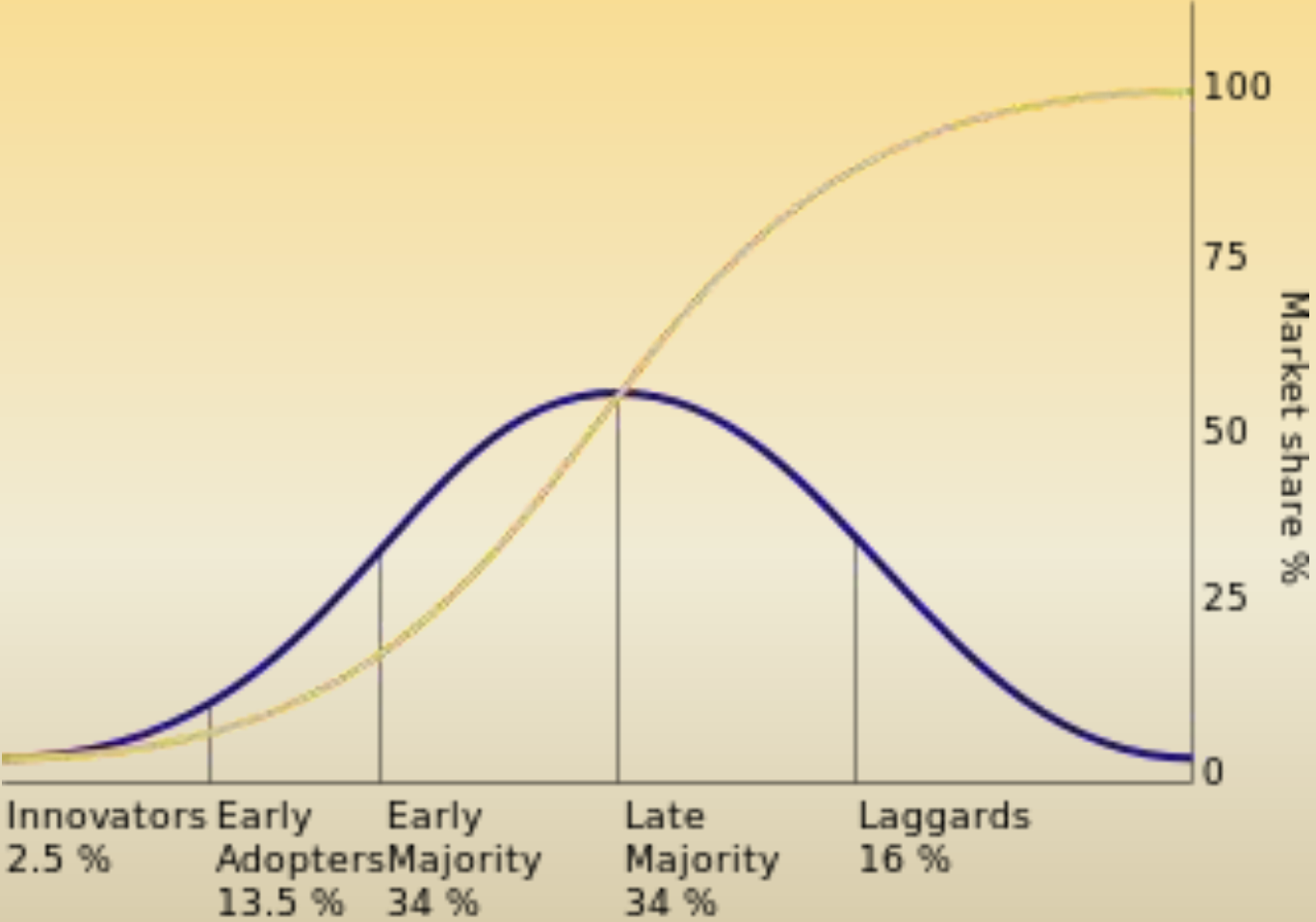
- ❑ Drones revolutionary technology
 - ❑ Not confined to past paradigms
 - ❑ Gravity
 - ❑ 3D space
 - ❑ Terrain
 - ❑ Dangers
 - ❑ Eliminate burdensome, dangerous, repetitive tasks, and in some cases impossible
- ❑ Black Swan Event

Market and Safety - Facts

- ❑ Military will be the highest in dollar volume
- ❑ sUAV don't cost millions
- ❑ Military and Civilian are increasing



Market and Safety - Facts

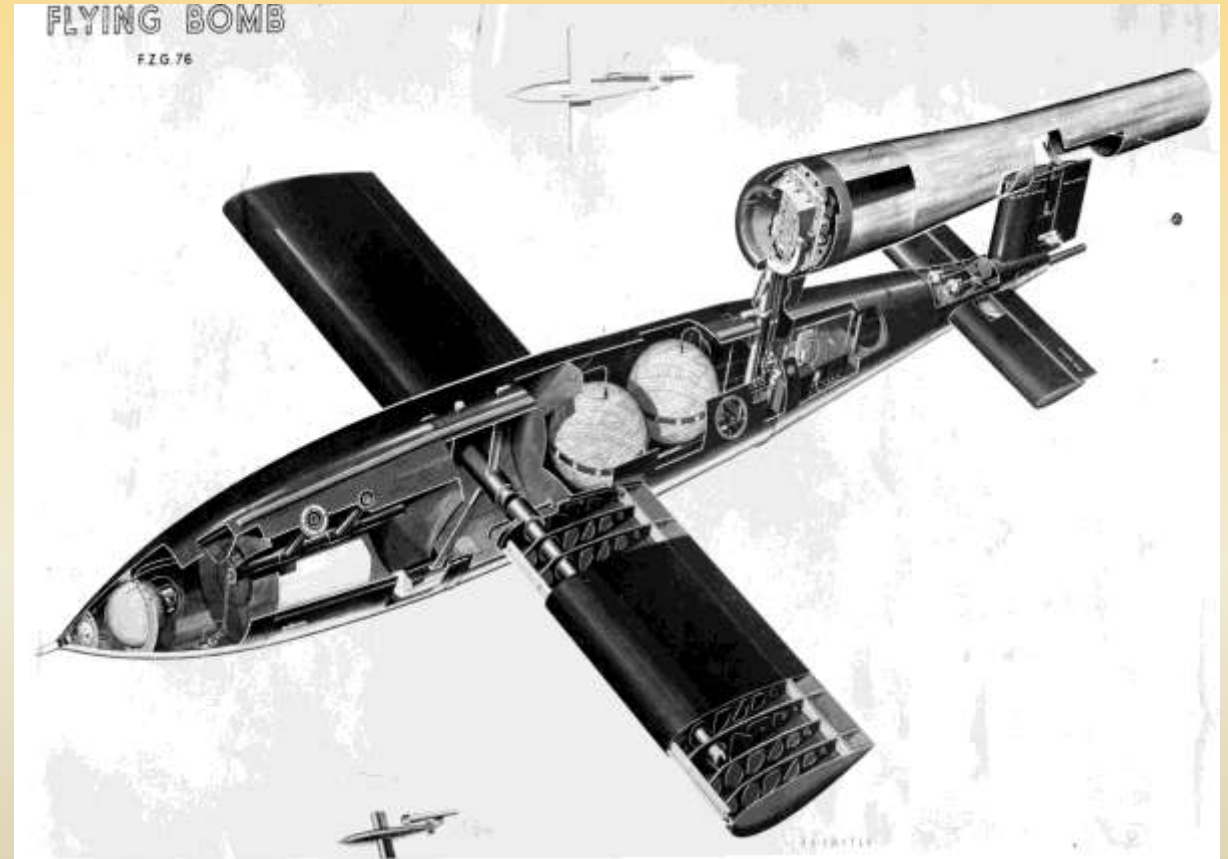


Market and Safety - Facts

- Market life cycle of sUAV
 - Innovators
 - Early Adopters
 - Early Majority
 - Late Majority
 - Laggards

Market and Safety - Facts

- ❑ On June 13th 1944, the Germans launched the first attack of V-1 rockets on England
- ❑ First use of Drone Technology



Market and Safety - Facts



Radio controlled model airplane,
Crusader, 1960

Early Adopters



Northrop / Radio-plane Basic
Training Target (BTT) 1940's-50's

Market and Safety - Facts

Beginning of Early Majority 1970-80



Market and Safety - Facts

- ❑ At early stage of adoption curve
- ❑ FAA moving forward with ruling
- ❑ Technology Advances
- ❑ New uses
- ❑ Infrastructure i.e. Geo-fencing / no fly zones
- ❑ Drone hiring

Market and Safety - Facts

- ❑ Drone crash sites - Locations are approximate
 - ❑ 47 military crashes
 - ❑ 23 civilian
- ❑ Close calls
 - ❑ 15 risky encounters between a rogue drone and other aircraft near an airport.
 - ❑ 110 places plan to host drones by 2017

Market and Safety - Facts

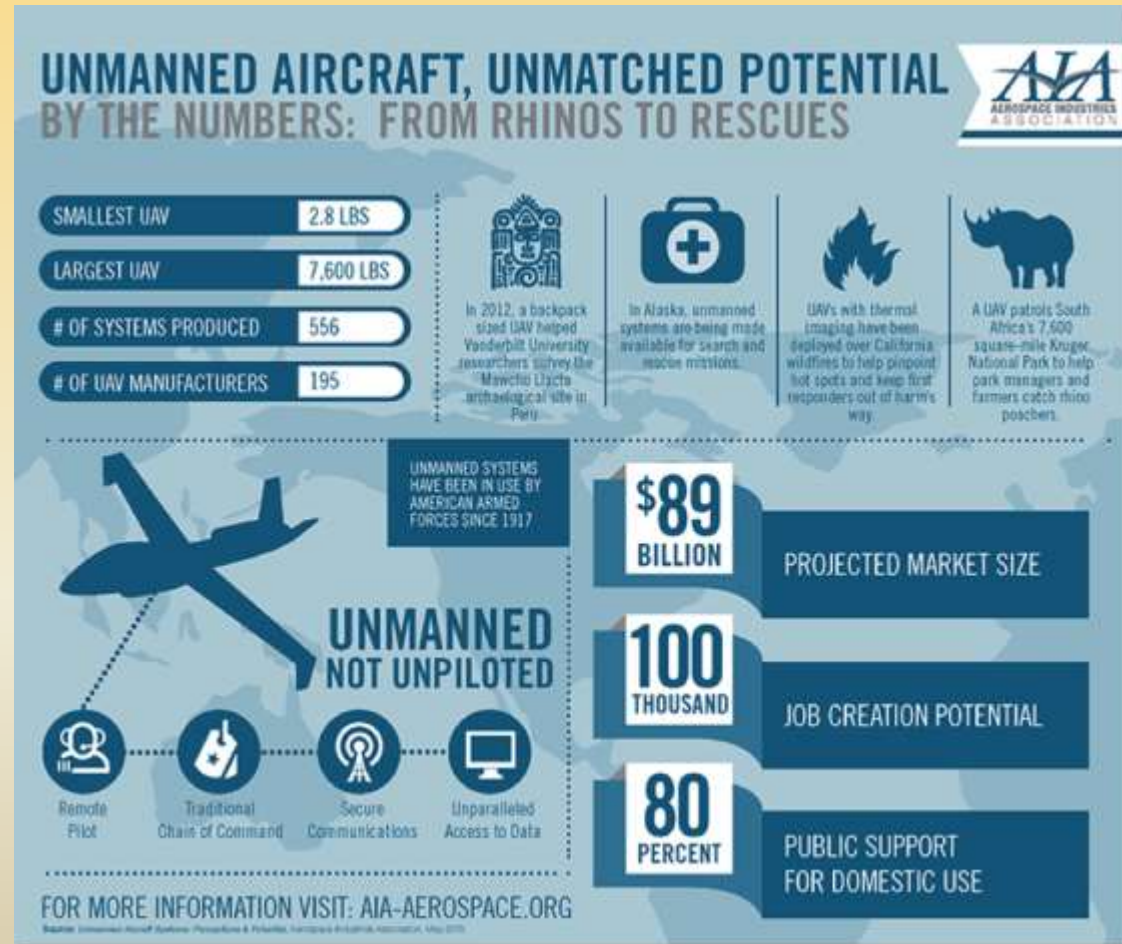
- ‘The World's Most Popular Drone Is a Magnet for Reckless Pilots’ by *JASON KOEBLE*



Market and Safety - Facts

- ❑ Reasons for accidents increase
 - ❑ Popularity of DJI
 - ❑ Affordability
 - ❑ Can fly within minutes
 - ❑ Beginner pilot coupled with advanced drone

Market and Safety - Facts



Market and Safety - Facts

- ❑ sUAS is an emerging sector of aerospace industry with great market demand
- ❑ sUAS market includes: UAVs, blimps and zeppelins
- ❑ Approximately 70% of global growth and market share is in the U.S.
- ❑ sUAVs are the most predominant segment of the sUAS market

Market and Safety - Facts

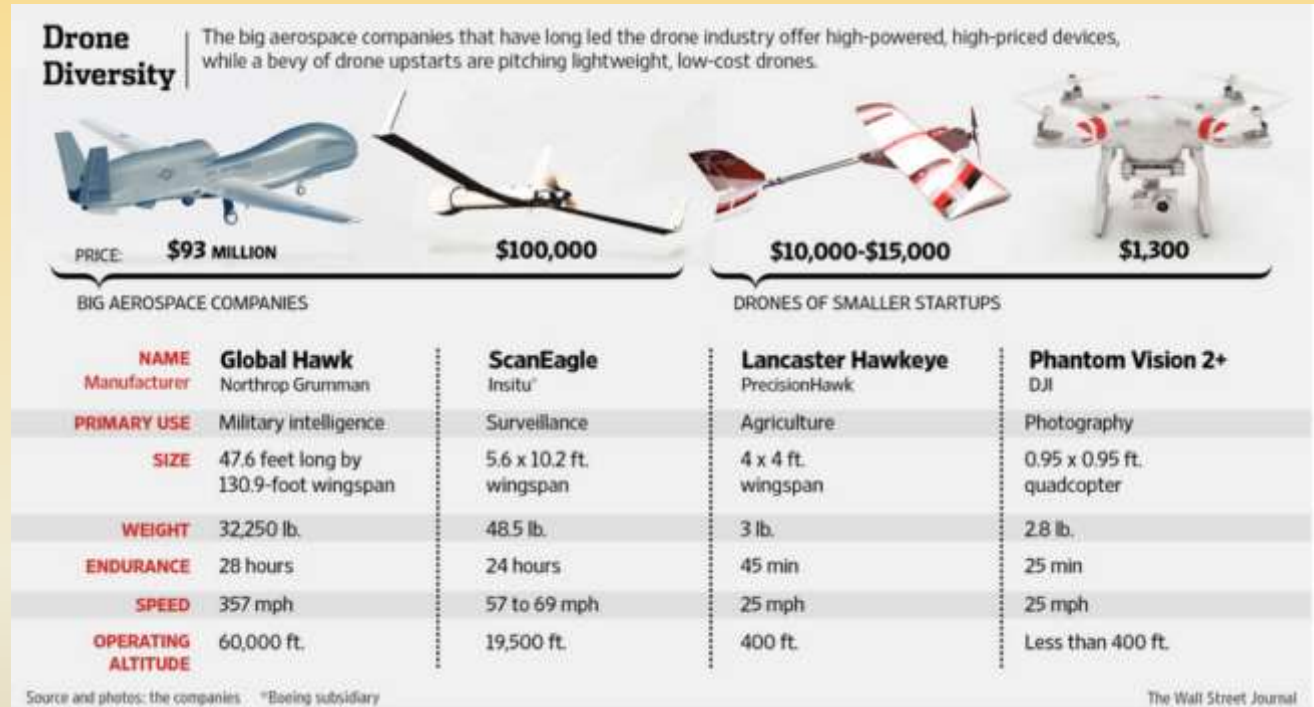
- ❑ UAV expenditures reached more than U.S. \$3 billion and more than 12% in 2010
- ❑ Half of expenditures on UAVs are dedicated to Research and Development
- ❑ 100,000 jobs creation potential
- ❑ 80% public support for domestic use

Market and Safety - Facts

- ❑ sUAV manufacturers remain fairly concentrated in the U.S., Israel, India, China
- ❑ Increased awareness and mission capabilities of sUAVs driving innovations and new applications
- ❑ There will be significant growth in UAVs driven by low cost and its capability in undertaking high threat tasks
- ❑ U.S. Air Force contemplates “All – UAV/UAS Future”

Market and Safety - Facts

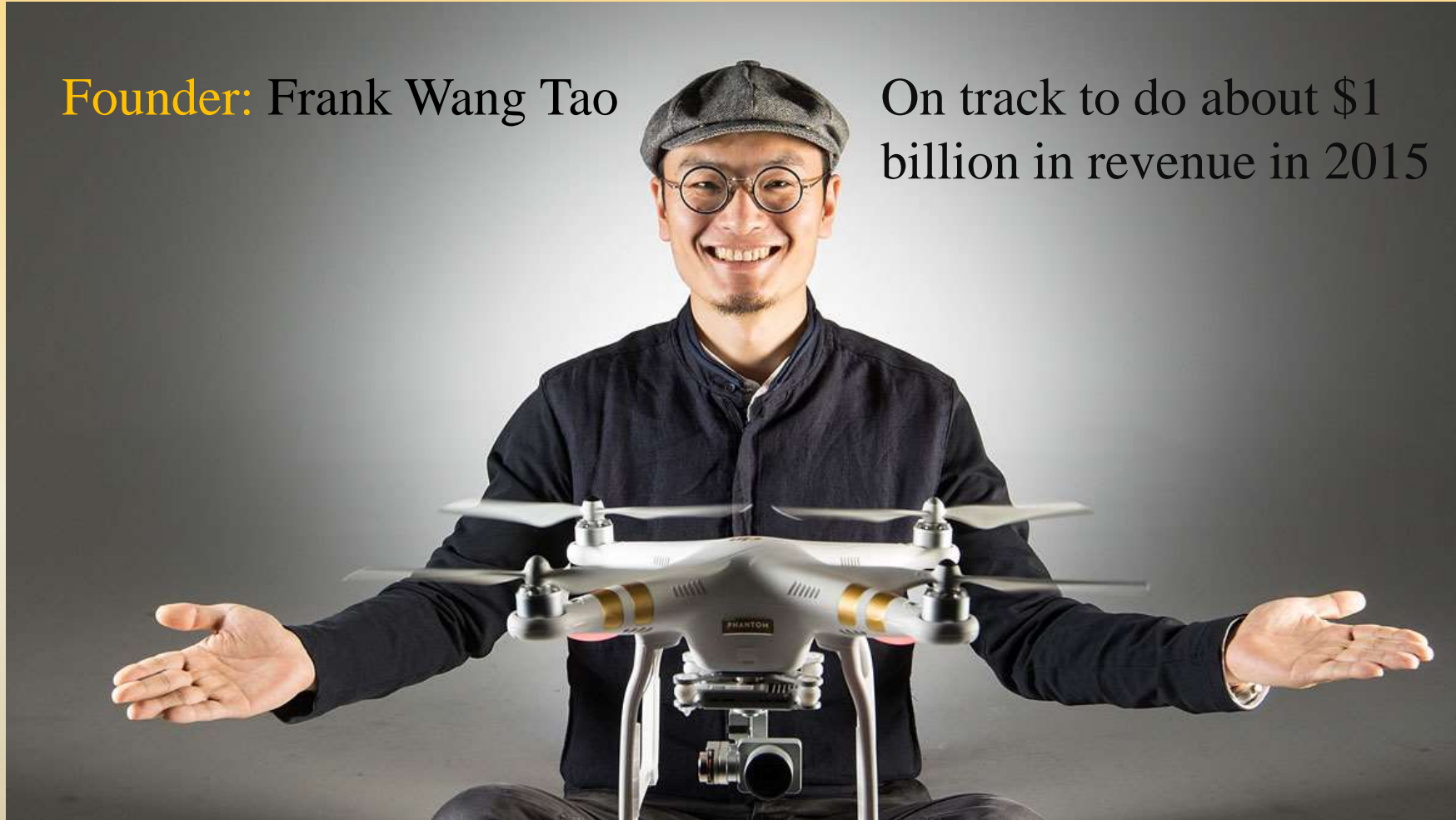
- Military
 - Combat
 - Surveillance / Observation
 - Rescue
 - Other
- Civilian
 - Recreation
 - Commercial
 - Law enforcement
 - Other



Market and Safety - Facts

Founder: Frank Wang Tao

On track to do about \$1 billion in revenue in 2015

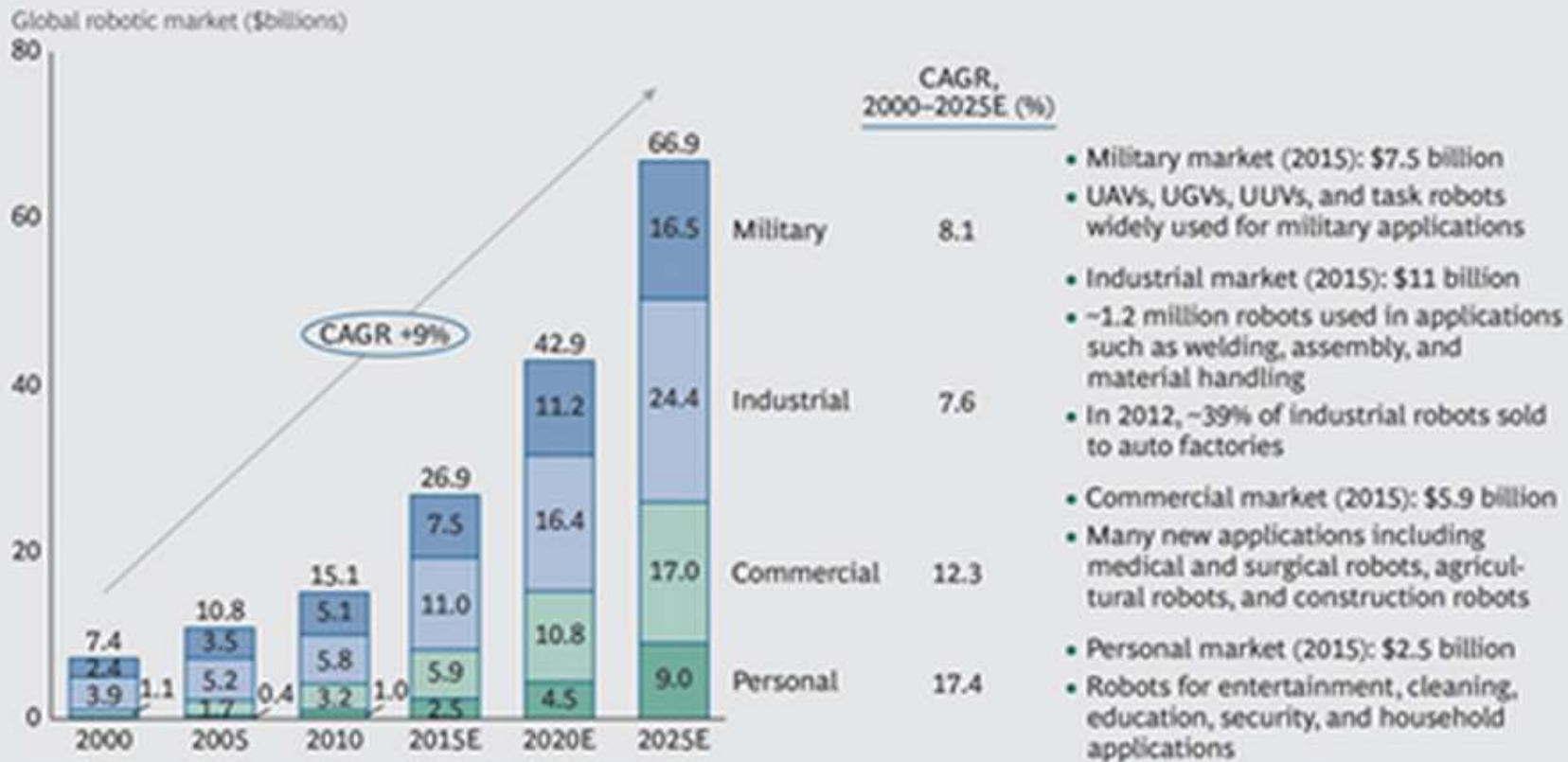


Market and Safety - Facts

- ❑ Frank Wang Tao
 - ❑ Chinese national
 - ❑ World's first drone billionaire
 - ❑ Sold 400,000 units last year
 - ❑ On track to do twice that in 2015
 - ❑ DJI is 70% of world market for sUAV
 - ❑ Therefore: Just over 571,500 were sold in 2014

Market and Safety - Facts

EXHIBIT 1 | Worldwide Spending on Robotics Is Expected to Reach \$67 Billion by 2025



Sources: International Federation of Robotics, Japan Robot Association; Japan Ministry of Economy, Trade & Industry; euRobotics; company filings; BCG analysis.

Note: UAV = unmanned aerial vehicle; UGV = unmanned ground vehicle; UUV = unmanned underwater vehicle. Estimates do not include the cost of engineering, maintenance, training, or peripherals.

Market and Safety - Facts



Market and Safety - Facts

- ❑ UAV spending across globe increased attention after terrorist attack on World Trade Center in 2001
- ❑ U.S. Department of Defense increased funding for UAV programs significantly after attack
- ❑ Increase in UAV budget during 2009 to 2011
- ❑ Growth during comes from USA and Europe

Market and Safety - Facts

- ❑ Spending for UAVs tends to come primarily from defense budgets
- ❑ U.S. share in 2008 in the UAV market is 60%
- ❑ U.S. share in total worldwide defense spending is about 48% in 2008
- ❑ U.S. in forefront of developing and deploying reconnaissance and strike UAVs

Market and Safety - Facts

- ❑ U.S. accounts for 73% of RDT&E spending & 59% of procurement
- ❑ France and Germany have set pace for UAV deployment in Europe
- ❑ In Mid-East region Israel was pioneer for many current tactical UAV efforts
- ❑ Israel major player in UAV sales to armed forces around the globe
- ❑ Asia-Pacific region has great potential in coming years

Market and Safety - Facts

- UAV expenditures are expected to increase over next 10 yrs. from present expenditure of approximately \$3.4 billion to \$7.3 billion

(\$Millions)	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
R&D	1,030.0	1,130.0	1,450.0	1,720.0	1,810.0	2,190.0	2,450.0	2,525.0	3,570.0	3,805.0	21,680.0
Production	1,408.2	1,356.4	1,447.5	2,024.4	3,131.9	3,344.3	3,889.9	4,066.3	3,472.2	3,791.7	27,932.8
O&M	340.0	385.0	475.0	405.0	435.0	445.0	500.0	580.0	660.0	740.0	4,965.0
Total	2,778.2	2,871.4	3,372.5	4,149.4	5,376.9	5,979.3	6,839.9	7,171.3	7,702.2	8,336.7	54,577.8

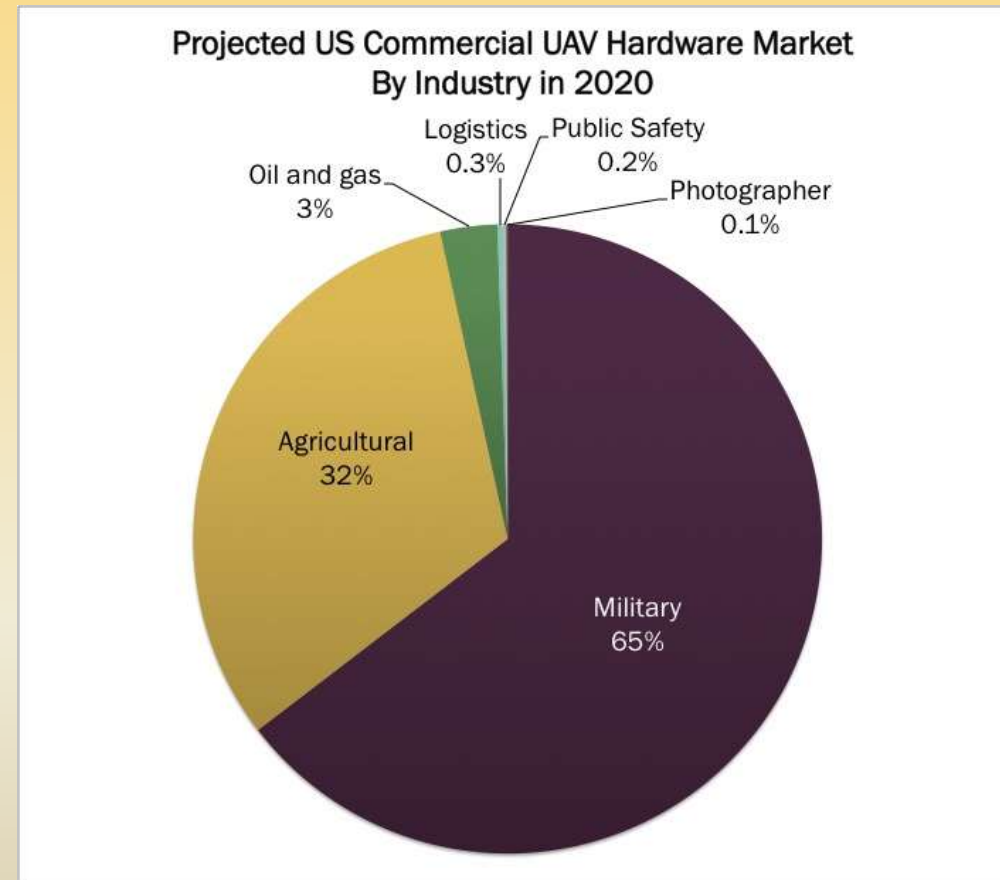
(R&D, \$Millions)	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
USA	850.0	900.0	1,200.0	1,400.0	1,300.0	1,600.0	1,800.0	1,800.0	2,800.0	3,000.0	16,650.0
Rest of World	180.0	230.0	250.0	320.0	510.0	590.0	650.0	725.0	770.0	805.0	5,030.0
Total	1,030.0	1,130.0	1,450.0	1,720.0	1,810.0	2,190.0	2,450.0	2,525.0	3,570.0	3,805.0	21,680.0

(Procurement, \$Millions)	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
USA	1,085.0	895.0	1,055.0	1,565.0	2,105.0	1,845.0	2,255.0	2,625.0	2,185.0	2,445.0	18,060.0
Rest of World	323.2	461.4	392.5	459.4	1,026.9	1,499.3	1,634.9	1,441.3	1,287.2	1,346.7	9,872.8
Total	1,408.2	1,356.4	1,447.5	2,024.4	3,131.9	3,344.3	3,889.9	4,066.3	3,472.2	3,791.7	27,932.8

(O&M, \$Millions)	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
USA	240.0	275.0	340.0	265.0	290.0	300.0	335.0	370.0	400.0	440.0	3,255.0
Rest of World	100.0	110.0	135.0	140.0	145.0	145.0	165.0	210.0	260.0	300.0	1,710.0
Total	340.0	385.0	475.0	405.0	435.0	445.0	500.0	580.0	660.0	740.0	4,965.0

Market and Safety - Facts

- By Industry
 - Military still the largest
 - Agriculture projected to be largest in commercial /private

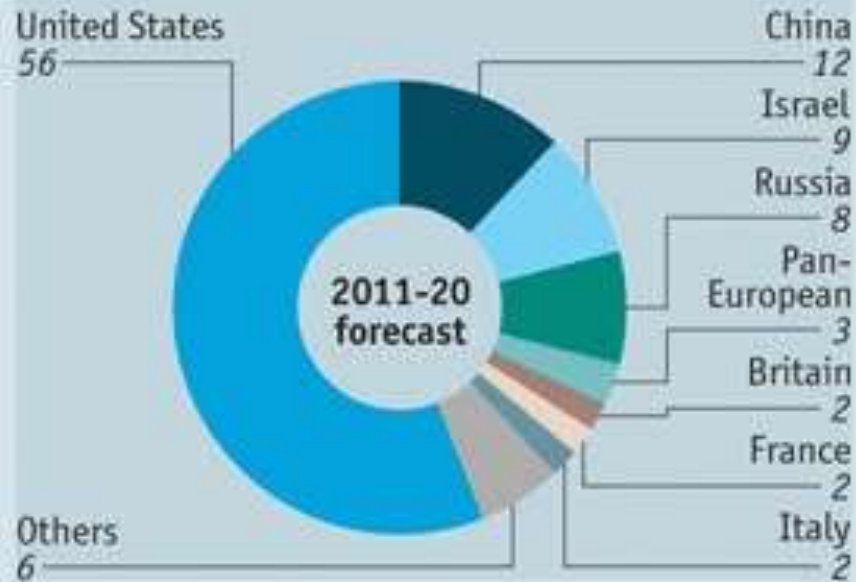


Market and Safety - Facts

Rise of the machines

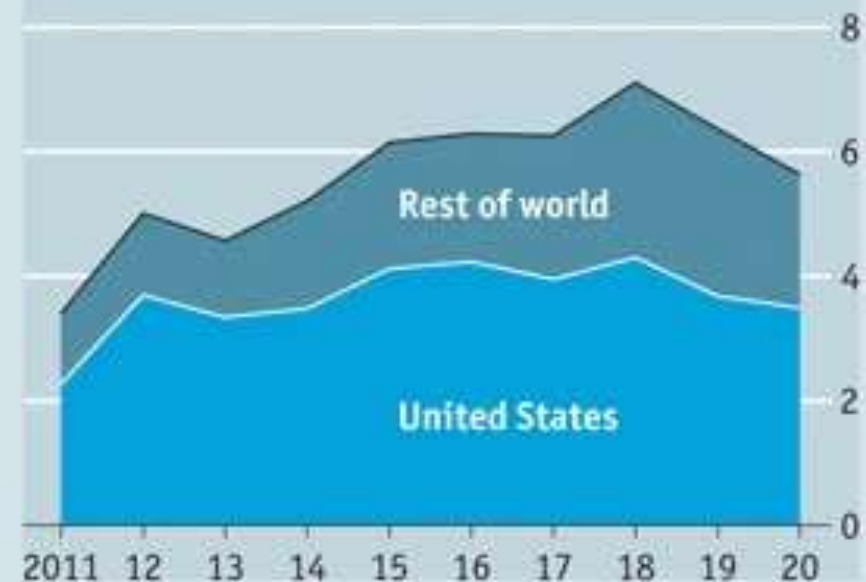
Unmanned aerial systems

R&D, by country, %



Sources: IHS Industry Research and Analysis; Teal group

Procurement forecasts, \$bn

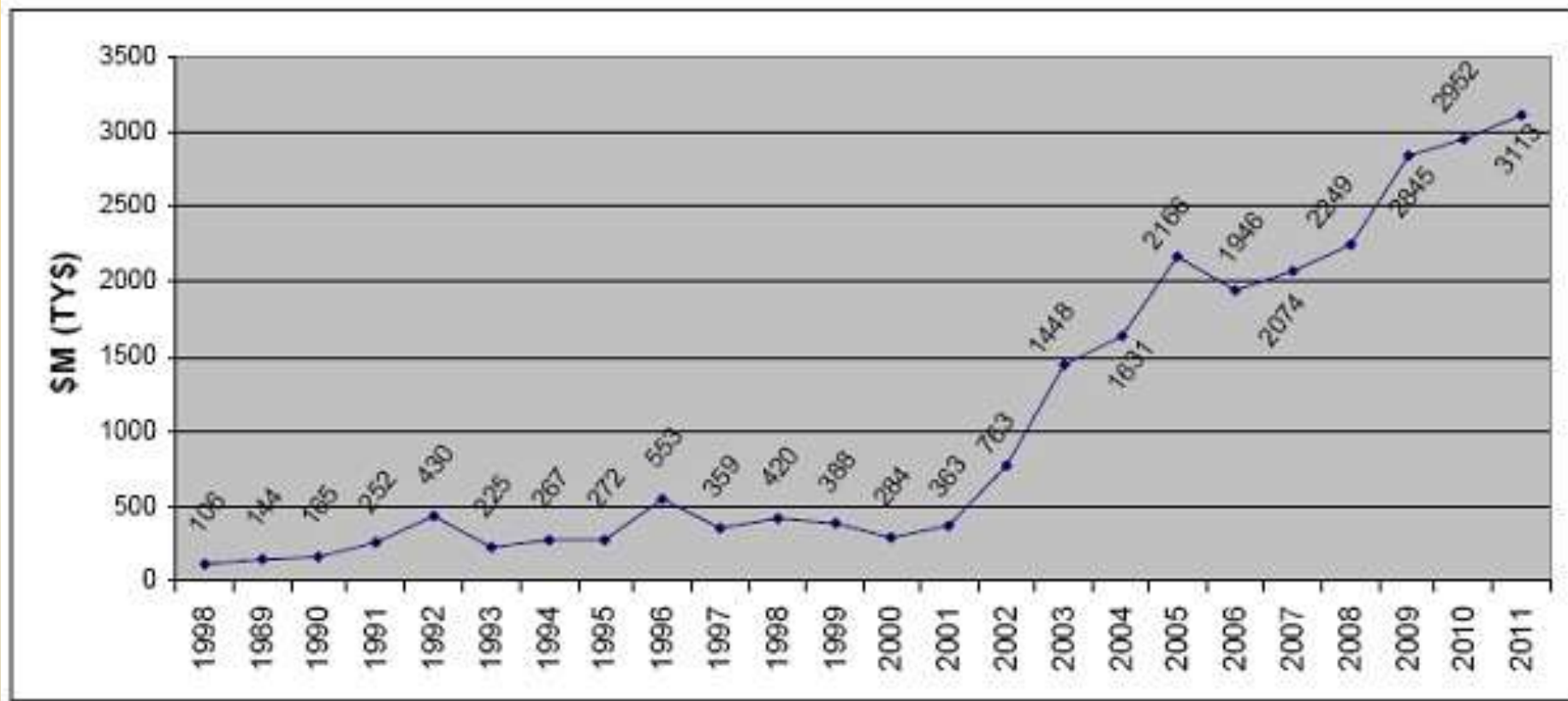


Market and Safety - Facts

Previous Graph:

- R&D % of major players in relationship to growing unmanned aerial systems market
- Procurement in terms of dollars in relationship to growing unmanned aerial systems market
- Rest of World represents all other countries
- UAS market predicted to grow through 2017
- Although dropped after 2017 sales will remain strong

Market and Safety - Facts

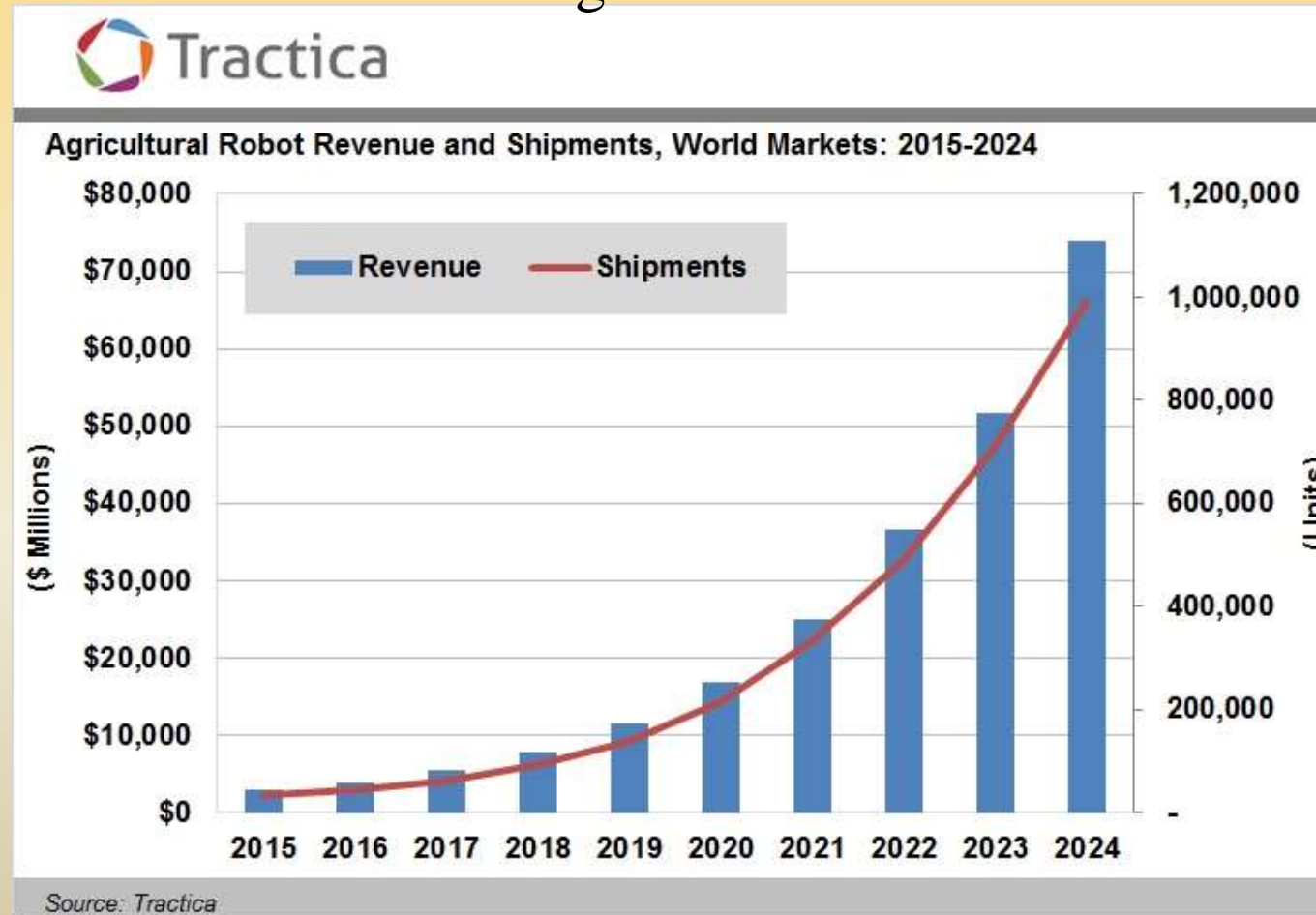


Market and Safety - Facts

- ❑ For above figure:
 - ❑ 1990 and 1999 - DoD invested greater than \$3 billion in UAS procurement, development, and operations
 - ❑ After September 11, 2001, record investments were made in UAS-related R&D projects
 - ❑ UAS inventory in U.S. anticipated to grow from 250 in 2005 to 675 by 2010 and 1400 by 2015
 - ❑ Excluding mini and micro UAVs

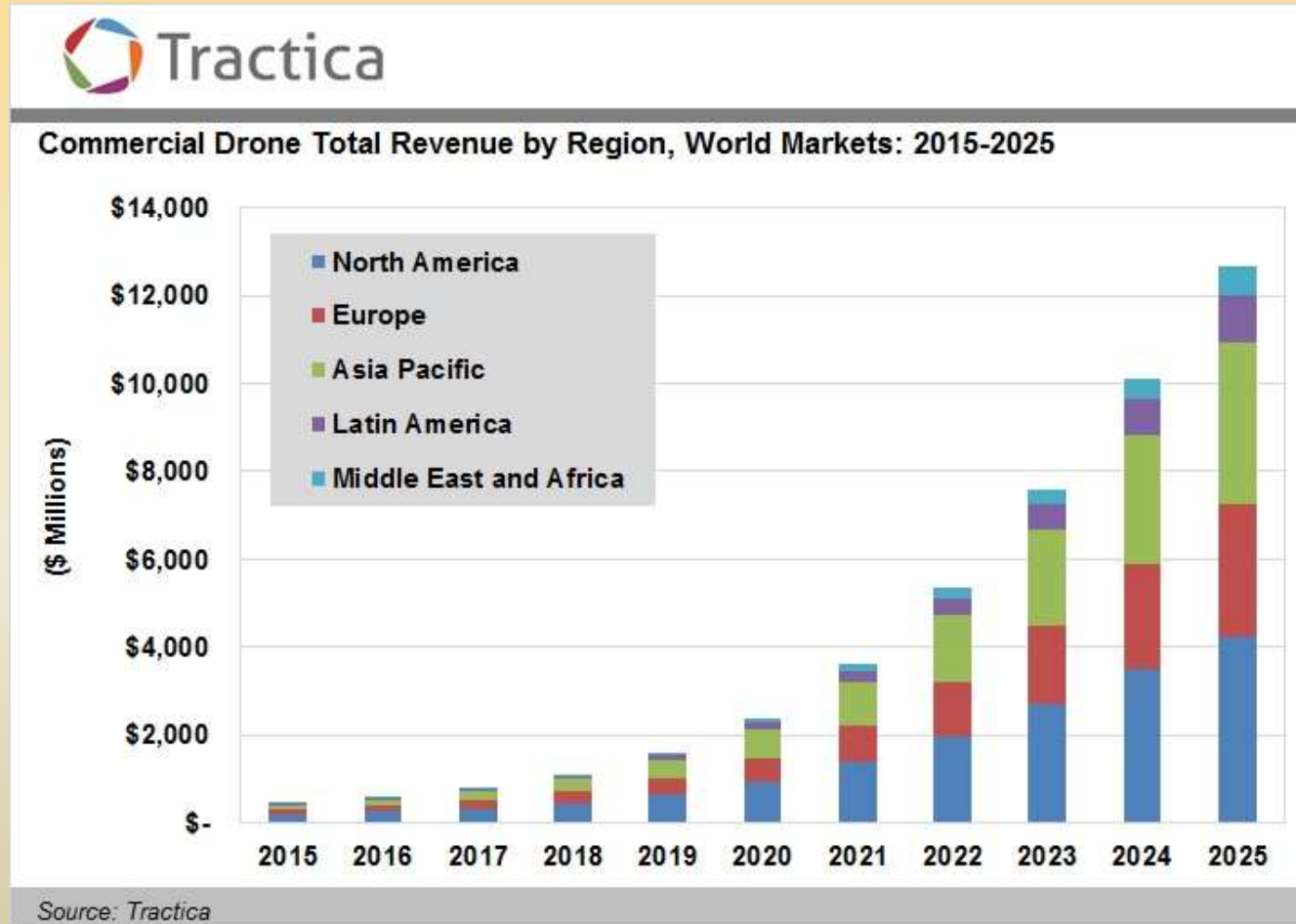
Market and Safety - Facts

Agricultural



Market and Safety - Facts

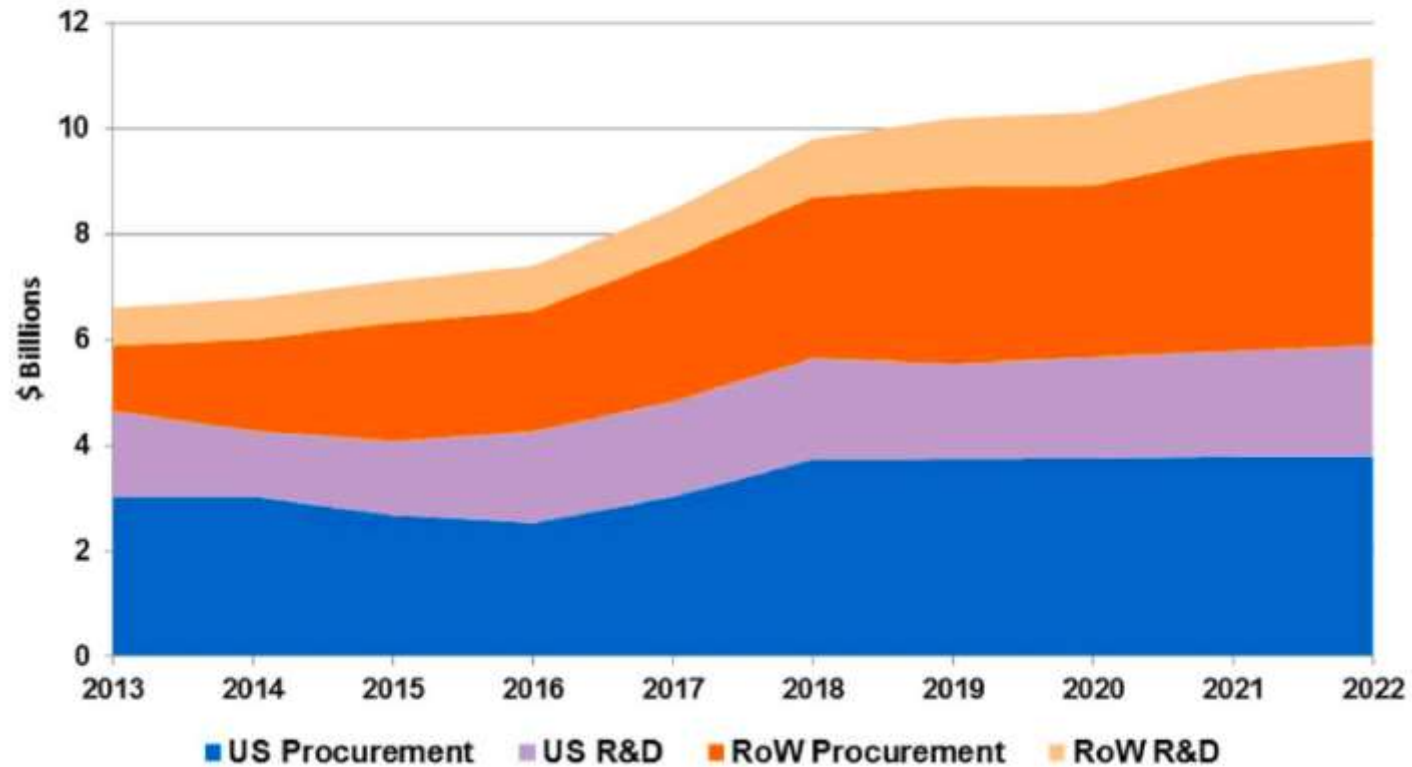
Commercial



Market and Safety - Facts

World UAV Budget Forecast

R&D and Procurement



RoW=Rest of World; speculative UCAV procurement not included

Market and Safety - Facts

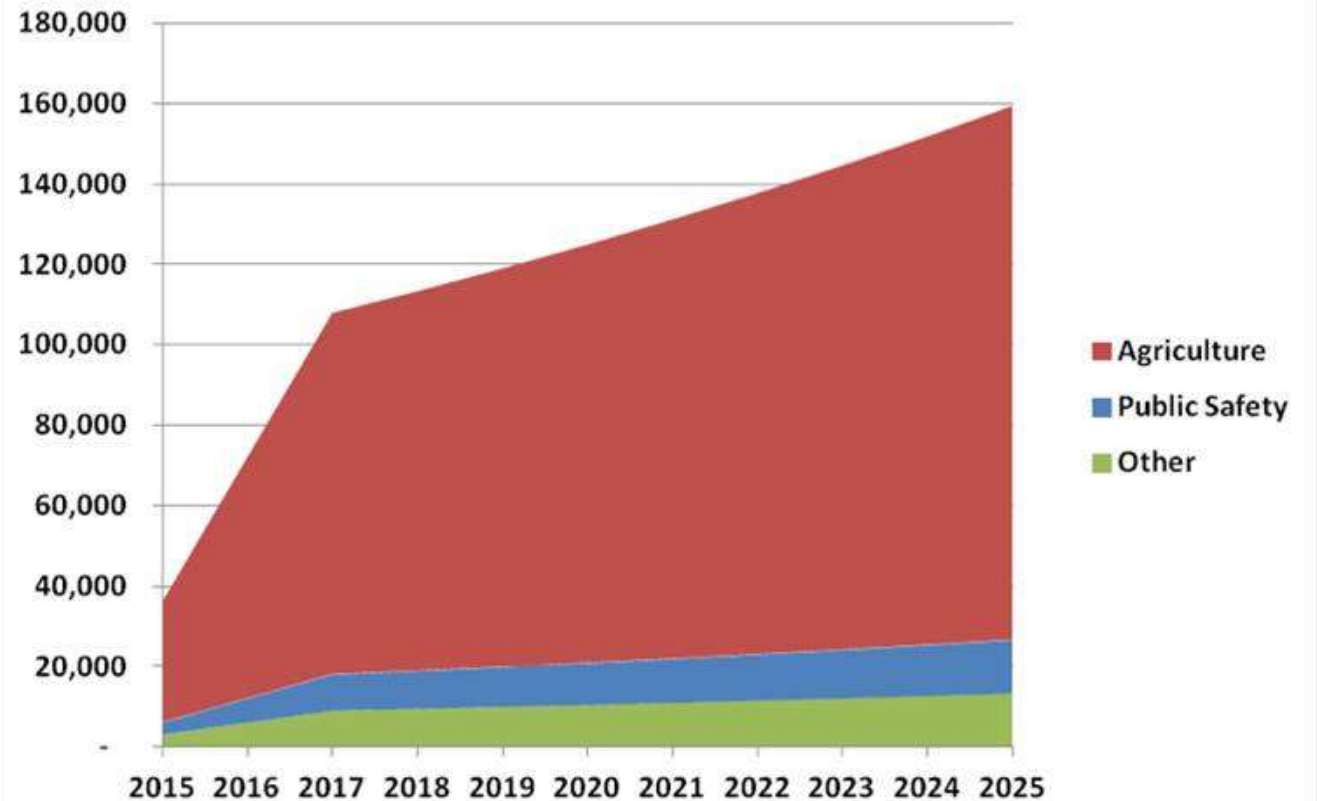
- ❑ UAVs most dynamic growth sector of aerospace industry
- ❑ Worldwide UAV market will double over next decade
- ❑ \$6.6 billion in research, development, test and evaluation (RDT&E)
- ❑ Procurement expenditures in 2103 about \$11.4 billion in 2022

Market and Safety - Facts

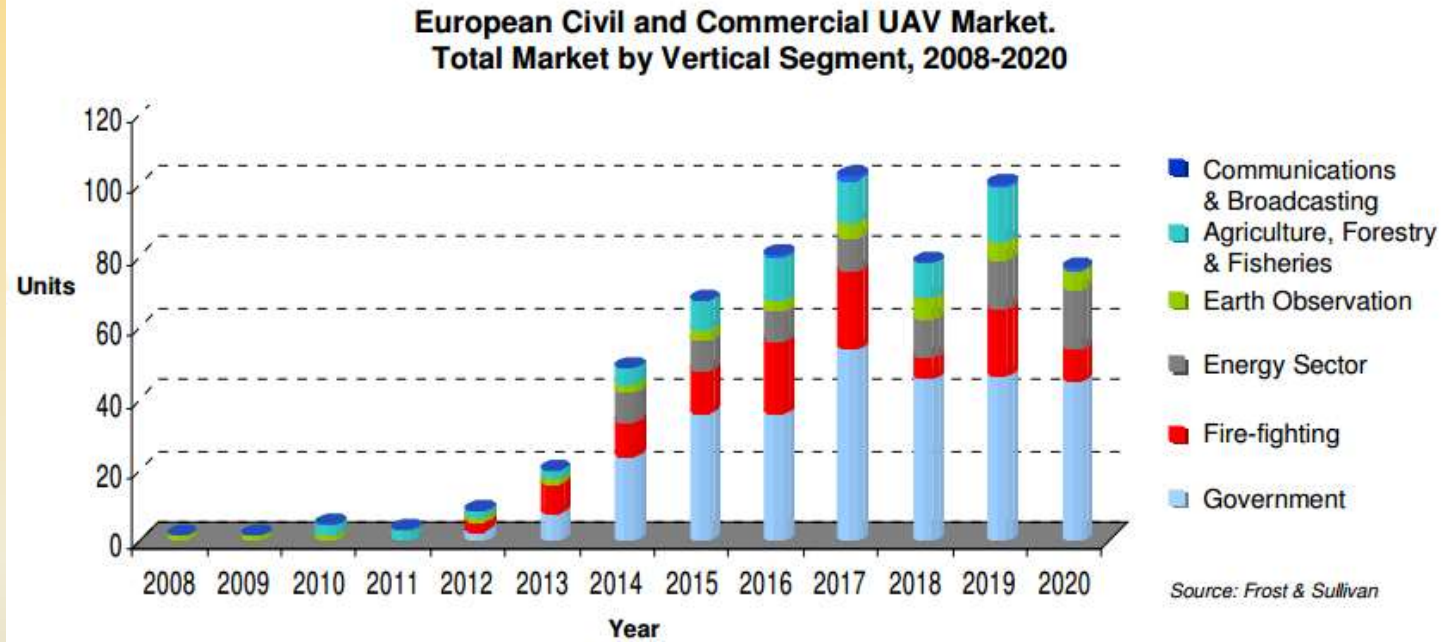
Projected Increase in UAS Sales:



Figure 2: Annual UAS Sales for Agriculture, Public Safety, and Other Markets

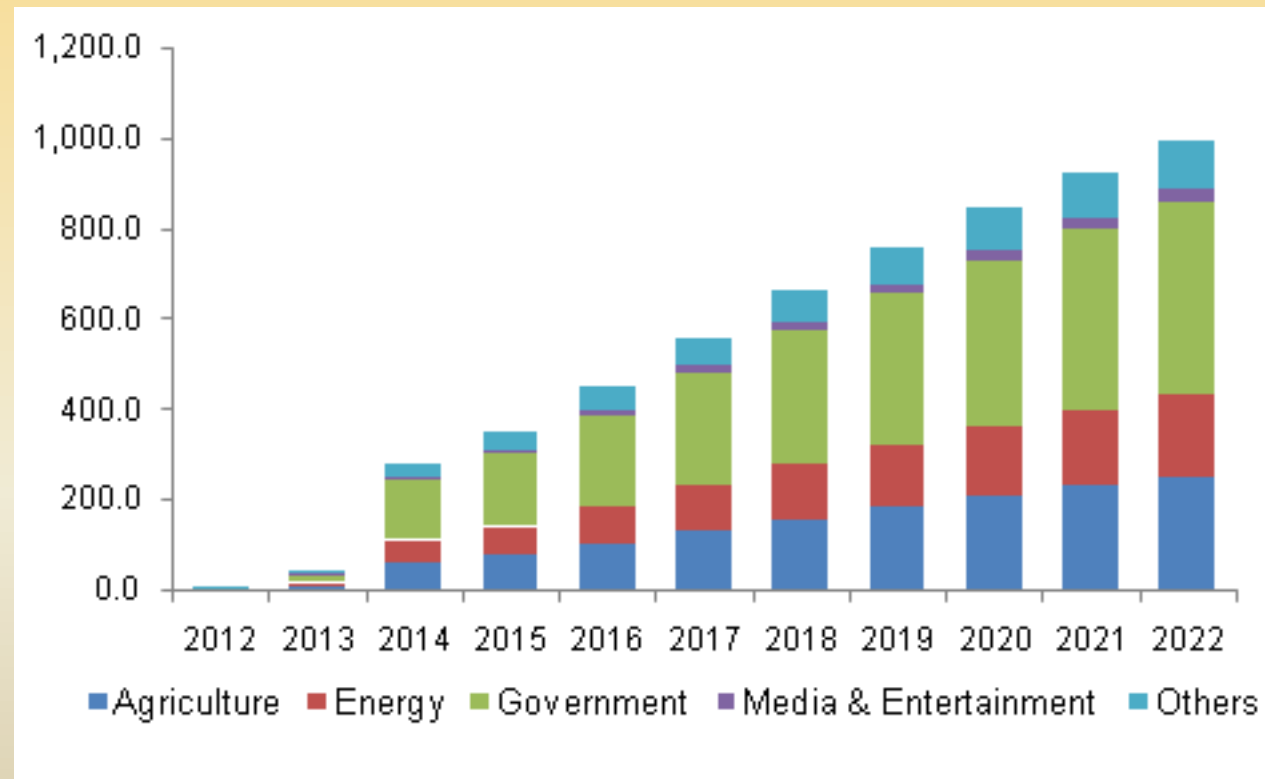


Market and Safety - Facts



Market and Safety - Facts

U.S. commercial UAV market by application, 2012-2022, (USD Million)



Market and Safety - Facts



Source: Visiongain 2015

Market and Safety - Facts



A SHORT HISTORY OF DRONES
FAA estimates that as many as 7,500 small commercial drones could be operational within five years in U.S. airspace.

2007 FAA issues a policy statement prohibiting the use of drones for commercial purposes.

2008

2009

2010

2011 FAA fines Raphael Parker \$10,000 for operating a drone for commercial purposes without a license.

2012

2013

Dec. 1, 2013: Amazon announces its intent to explore package delivery via drones.

March 6, 2014: Judge rules in favor of Parker and dismisses the FAA's fine.

March 7, 2014: FAA appeals decision in the *Huerta v. Parker* civil penalty case.

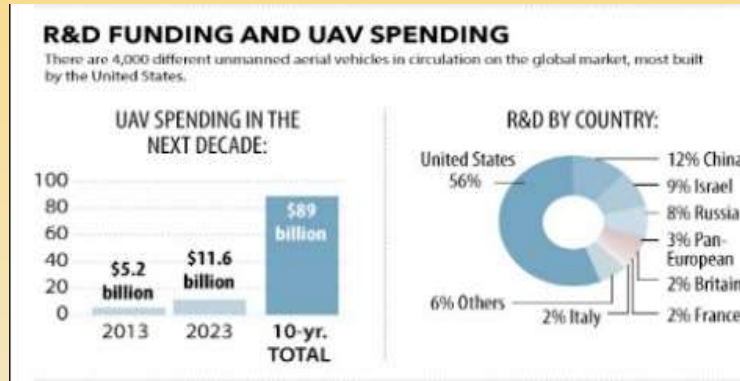
April 21, 2014: FAA announces first drone test site is operational in Nevada's Lake Mead.

2014

2015

2016

SOURCES: FAA, NPR, FORTUNE, CNN, Bleepingmag.com, motherboard.ck12.com, The Fed Group, <http://blogs.jatit.com/the-dog-bus-ness-of-commercial-drones-infographic/>



Market and Safety - Facts

- Situational Awareness (SA) / Flight Management System (FMS)
- See and Avoid vs. Sense and Avoid
- Manned vs. Unmanned
- Defined Rules vs. Technology still under development

Market and Safety - Facts

- ❑ Two categories of unmanned sensing:
 - ❑ Direct Sensing – On board
 - ❑ Human predicts (LOS) Loss of Separation and controls corrective action
 - ❑ Network Sensing – received / transmitted information
 - ❑ Network predicts (LOS) and controls corrective action

Market and Safety - Facts

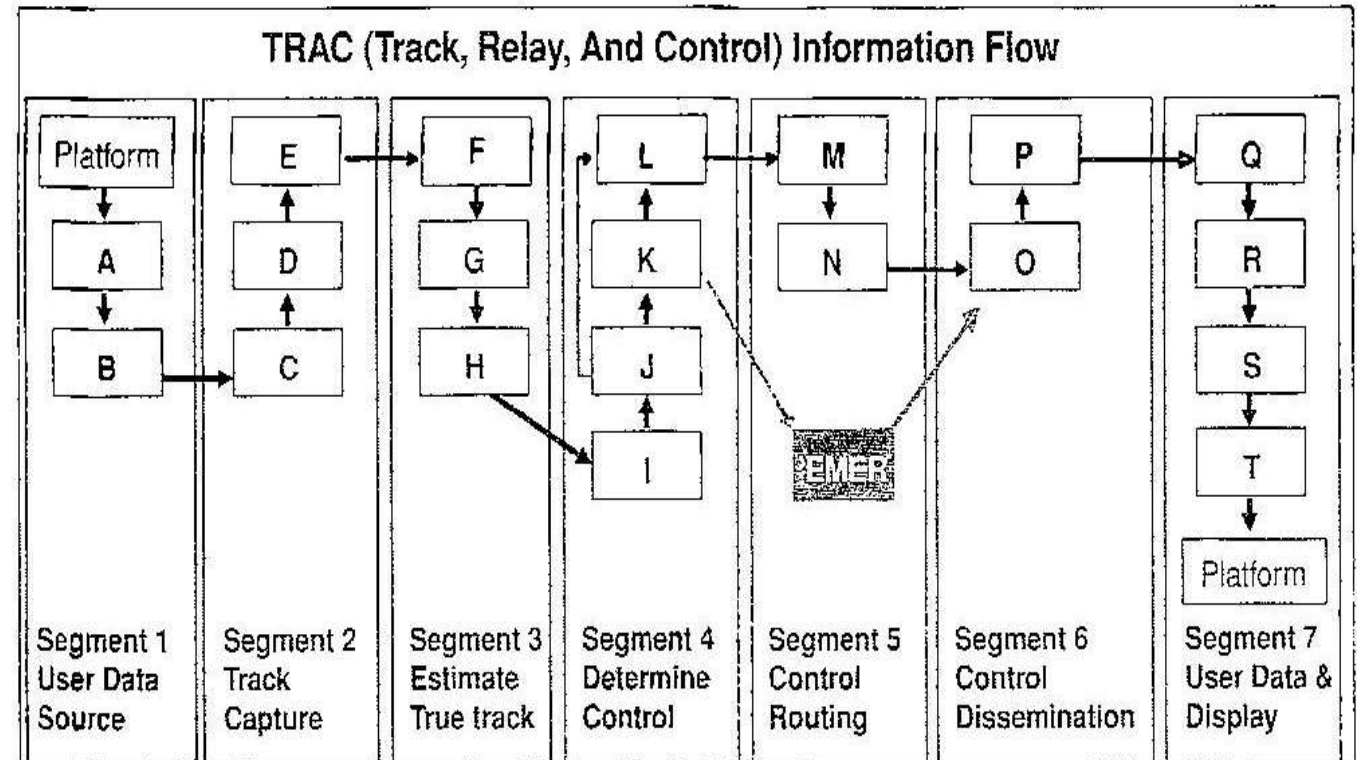
- ❑ Commercial off the shelf (COTS) hardware/software
 - ❑ Direct SA Challenges:
 - ❑ Hardware implementation requirements
 - ❑ Threat detection problems
 - ❑ No external communication with other aircraft

Market and Safety - Facts

- ❑ Commercial off the shelf (COTS) hardware/software
 - ❑ Advantages of Networked Sent
 - ❑ Hardware lighter weight
 - ❑ Track aircraft at all distances
 - ❑ Connectivity with other aircraft/internet
 - ❑ Disadvantages
 - ❑ Latency

Market and Safety - Facts

- ❑ Process for information flow
- ❑ Network based SAA system
- ❑ CIN continuously monitors aircraft tracks
- ❑ Issues SAA information
- ❑ Computes safe trajectory of aircraft
- ❑ Centralized control center



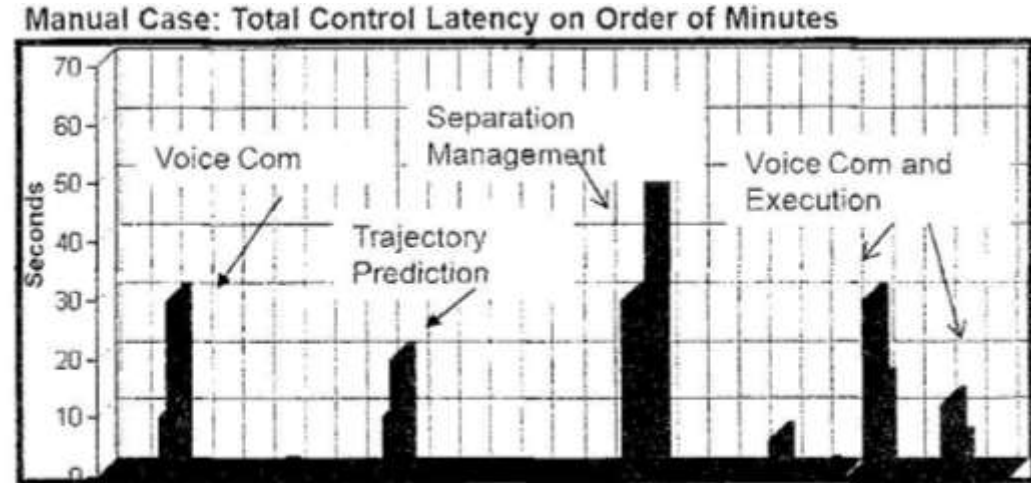
Market and Safety - Facts

□ Process in Chart 8.1

- 1 User Data Source – Process of current aircraft state data and inserted into CIN
- 2 Track Capture – Transmitted data from capture ex: satellite, ground station
- 3 – 5 Represent the process flow at centralized SAA control center
- 6 Control Dissemination – User
- 7 User Data and Display

Market and Safety - Facts

Manual:



Automated:

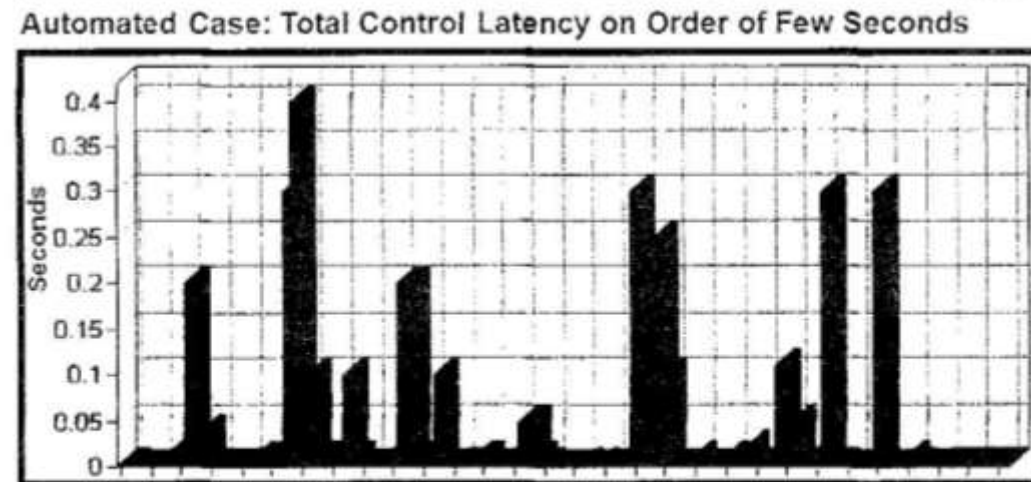
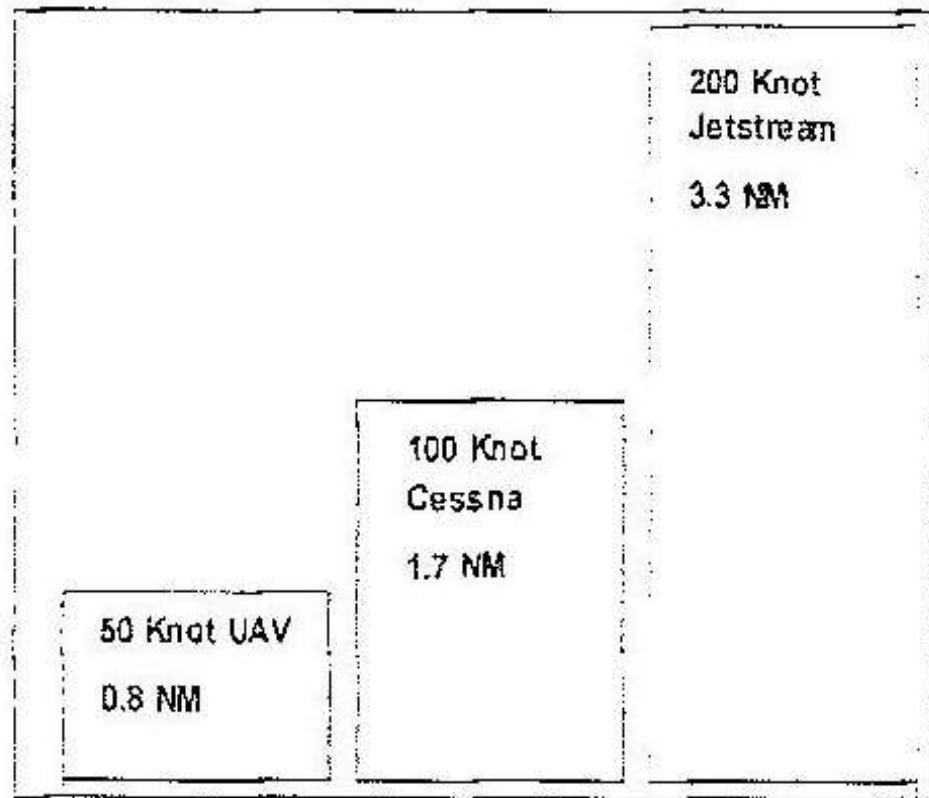
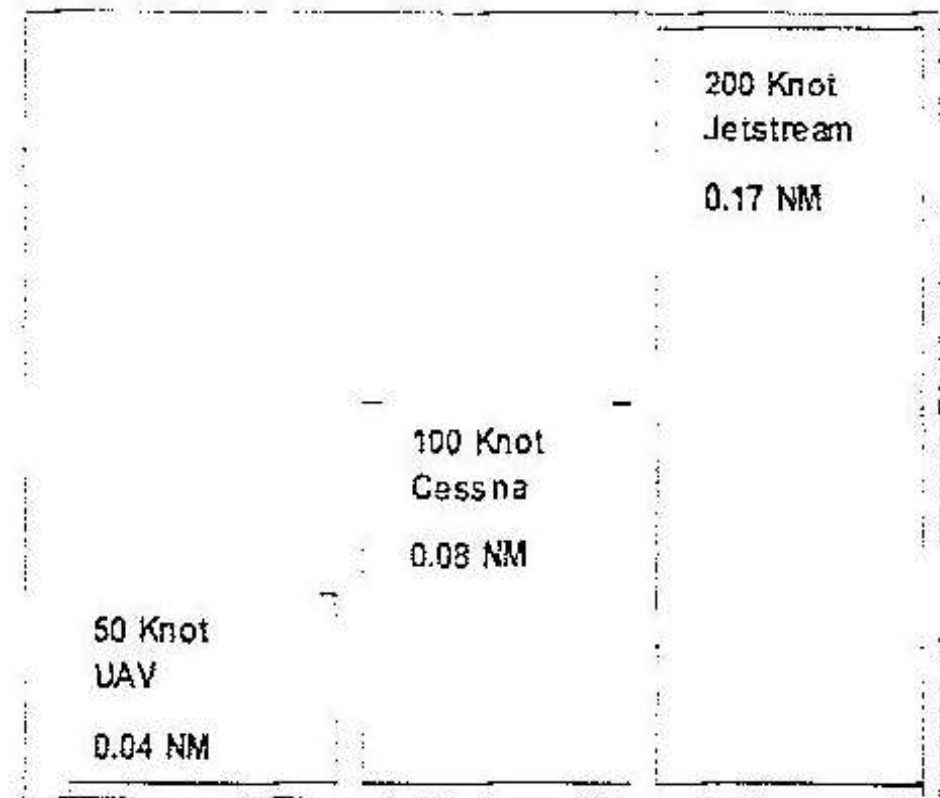


Figure 8.2 Comparison of latency for manual and automated information flows. The horizontal axis represents the segment functions listed in Table 8.2

Market and Safety - Facts



Latency Distance Uncertainty with 60 Seconds Information Latency



Latency Distance Uncertainty with 3 Seconds Information Latency

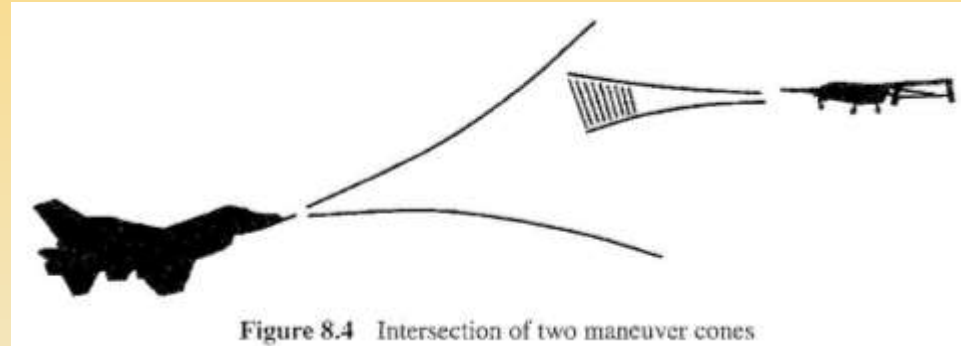
Figure 8.3 Comparison of latency distance uncertainties for information latencies of 60 seconds (left) and 3 seconds (right)

Market and Safety - Facts

- ❑ Information Latency , dt , is directly related to separation distance in which aircraft can be controlled
- ❑ Prepare aircraft state information (A) – $dt * v$, where v is velocity of aircraft
- ❑ $f(S)$ – segmented function integrates information
- ❑ $f(T)$ – segmented function initiates control action

- ❑ Therefore:
 - ❑ Latency distance – $dt * v$
 - ❑ Uncertainty – $f(B,H,I,J,Q,S)$ (segmentation of data)
 - ❑ Information Latency – $f(T)$

Market and Safety - Facts



- ❑ Elements of Automated Aircraft Separation
 - ❑ Continuous process of computer algorithms
 - ❑ Algorithms assure LOS is not compromised
 - ❑ 3 Estimate True track
 - ❑ 4 Determine Control
 - ❑ 5 Control routing

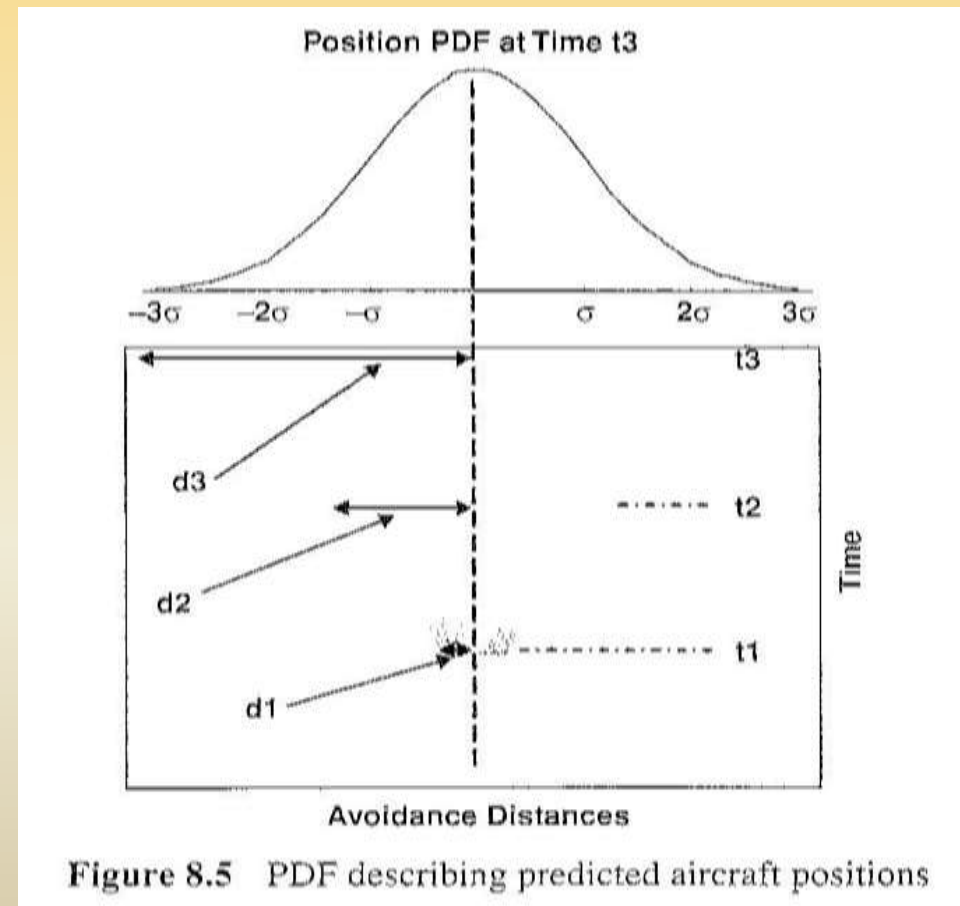
- ❑ Error continues to grow as Look ahead time increases
- ❑ Intersection of maneuver cone represents LOS

3,4,5 from Table 8.2

Market and Safety - Facts

- ❑ Look ahead error is dependent on:
 - ❑ Prediction time window
 - ❑ Aircraft Speed
 - ❑ Maneuverability
 - ❑ Weather
 - ❑ State data error
 - ❑ Information latency
- ❑ PDF represented by Gaussian curve
- ❑ Illustrates fastest mover can restore safe separation and trajectory quickest

Probability distribution function



- ❑ Curve more likely to be asymmetrical

Market and Safety - Facts

- ❑ $PDF_1 + PDF_2 + PDF_{n+1\dots} = LOS$
- ❑ Look ahead window should be larger than the information latency and safe maneuver Execution time
- ❑ Too large can create false separation results
- ❑ Separation algorithms
 - ❑ Grid based
 - ❑ Genetic Search
 - ❑ **EMERGING SYSTEMS**

Market and Safety - Facts

- ❑ Grid Based Automation Separation
 - ❑ Algorithm based on 4 dimensional, 3-special 1-time
 - ❑ Grid cell labeled occupied / not occupied
 - ❑ More advanced GBAS can populate cell with percent
 - ❑ Unoccupied can represent safe cells
 - ❑ Boundary conditions can be set

Market and Safety - Facts

- ❑ Genetic Based Separation Automation
 - ❑ Random generation of cell population
 - ❑ Scrutinize by infinite generations of population labeled as chromosomes
 - ❑ Assignment trajectories predict fitness of solution
 - ❑ Best one is plotted and selected

Market and Safety - Facts

- ❑ Contributing factors for the determination of each solution:
 - ❑ Mutual separation distance between each aircraft
 - ❑ Cull least fit solutions first
 - ❑ Subject remaining solutions to Crossover
 - ❑ Mutation genetic algorithm operators

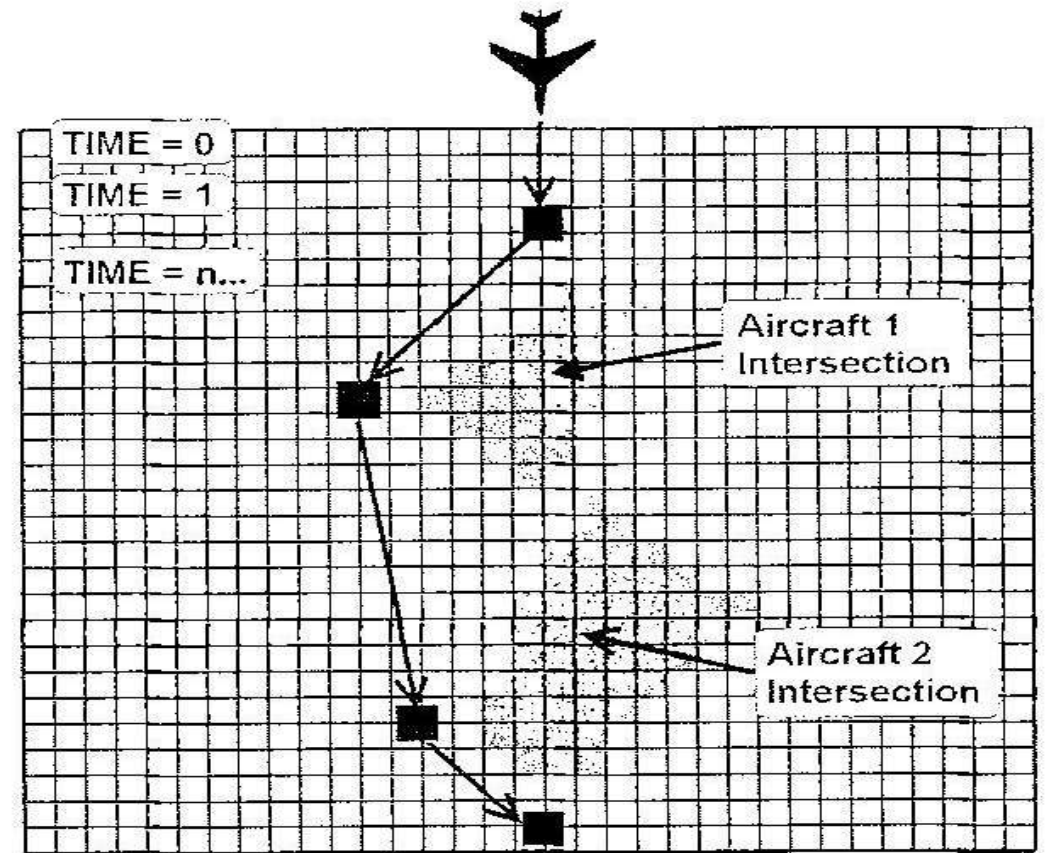


Figure 8.6 Illustration of grid-based aircraft separation management

Market and Safety - Facts

- ❑ Multiple trajectories predicted
- ❑ Algorithm attempting to de-conflict

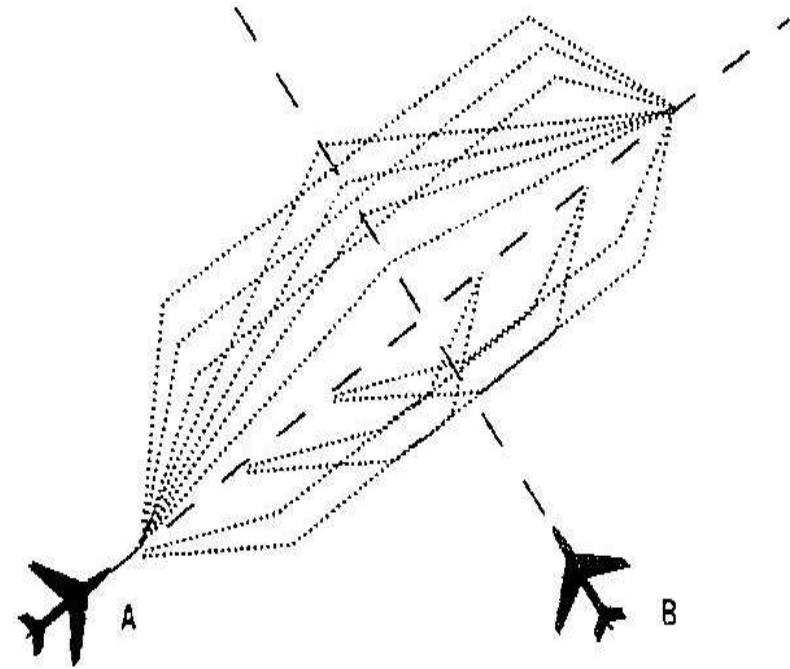


Figure 8.7 Example discretization of the infinite number of solutions to a LOS scenario, as used by a genetic algorithm for automated aircraft separation. Dashed lines represent the nominal flight paths while dotted lines represent a subset of collision avoidance maneuvers for aircraft A

Market and Safety - Facts

- ❑ Emerging Systems-Based Separation Automation – dynamic solutions that self adapt natural self-organizing systems
 - ❑ Artificial potential fields
 - ❑ Emits repulsive force on surrounding craft
 - ❑ Operational guidance can be achieved by an attractive force to waypoints
 - ❑ Artificial flocking algorithms
 - ❑ Different rules applied for together and rules applied for separation
 - ❑ Safe aircraft separation achieved by following specific rules

Market and Safety - Facts

- ❑ Safe order achieve by every aircraft

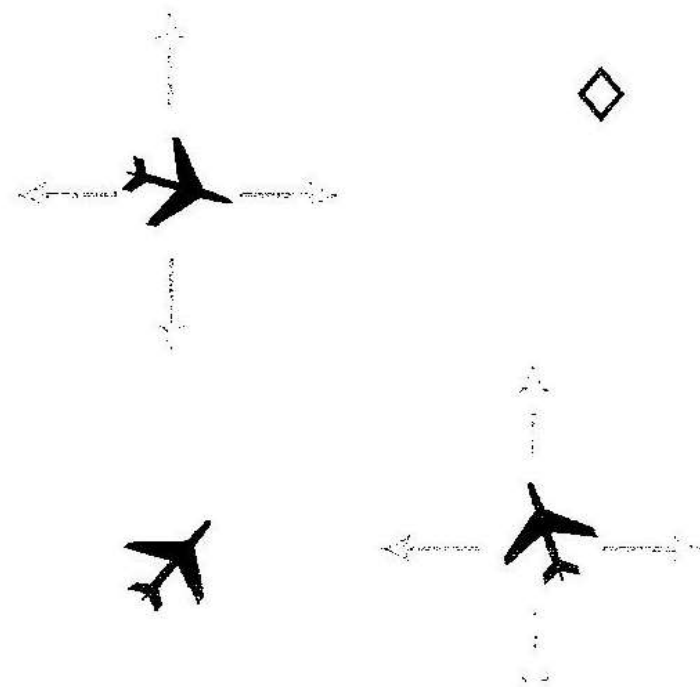


Figure 8.8 Simplification of the potential field approach to aircraft separation

Market and Safety - Facts

- ❑ Smart Skies explored future technology that supports safe and efficient use of NAS by both manned and unmanned aircrafts
- ❑ They explored key airspace automation-enabling technologies
- ❑ Prototyped automated SAA system on a CIN
- ❑ Performed under uncontrolled airspace under realistic and stressing conditions

Market and Safety - Facts

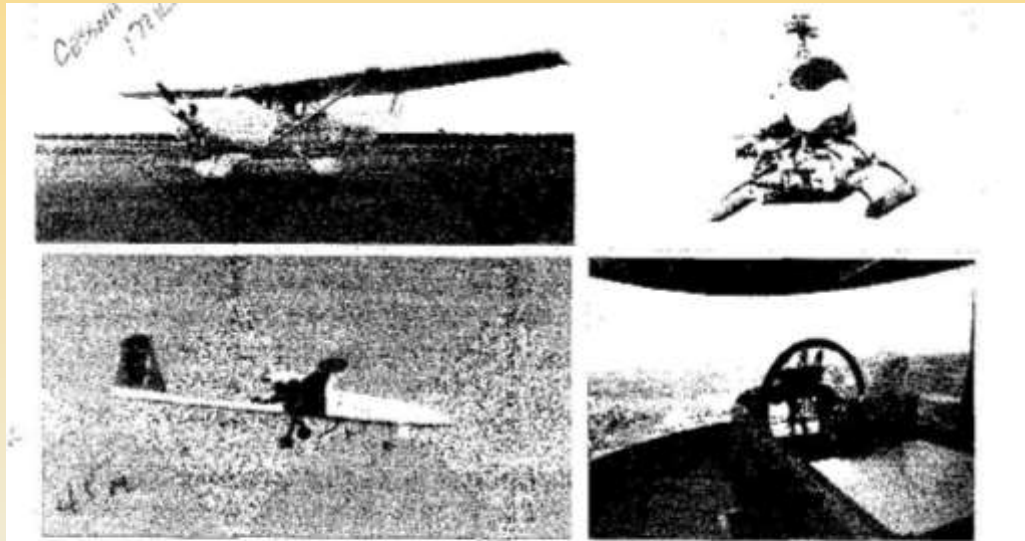


Figure 8.9 Flight test assets used during the Smart Skies flight trials. Clockwise from top-left are the ASL, CUAS, flight simulator, QUAS

Table 8.3 Real and virtual aircraft used for the Smart Skies flight tests

Real aircraft	Autonomous simulations	Piloted flight simulator
ASL - Cessna 172	Cessna 172	Cessna 172
CUAS helicopter	Jetstream (twin turboprop)	Jetstream
QUAS Flamingo	Flamingo simulation CUAS simulation	

Market and Safety - Facts

- ❑ Communication architecture – two different systems
 - ❑ Iridium LLC RUDICS
 - ❑ Telstra Next G cellular system

- ❑ Provides Connection to all aircraft, real and virtual

- ❑ Dual independent communication channels provides reliability of 99%

- ❑ Allows multiple aircraft to be tracked

Market and Safety - Facts

- ❑ Iridium LLC RUDICS
- ❑ Telstra Next G cellular system

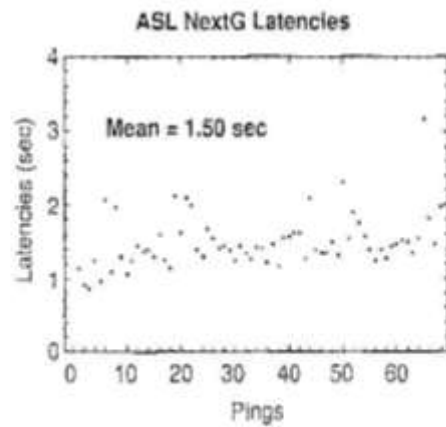
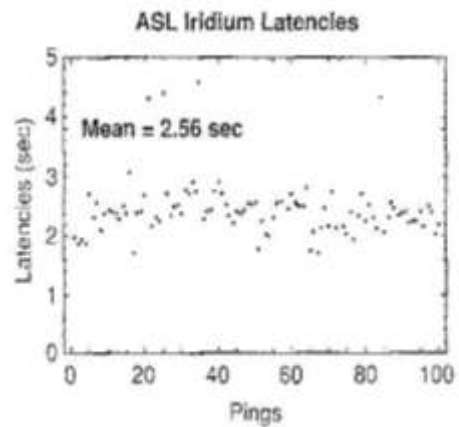


Figure 8.12 Example CIN end-to-end latencies over satellite (Iridium) and cellular (NextG) networks

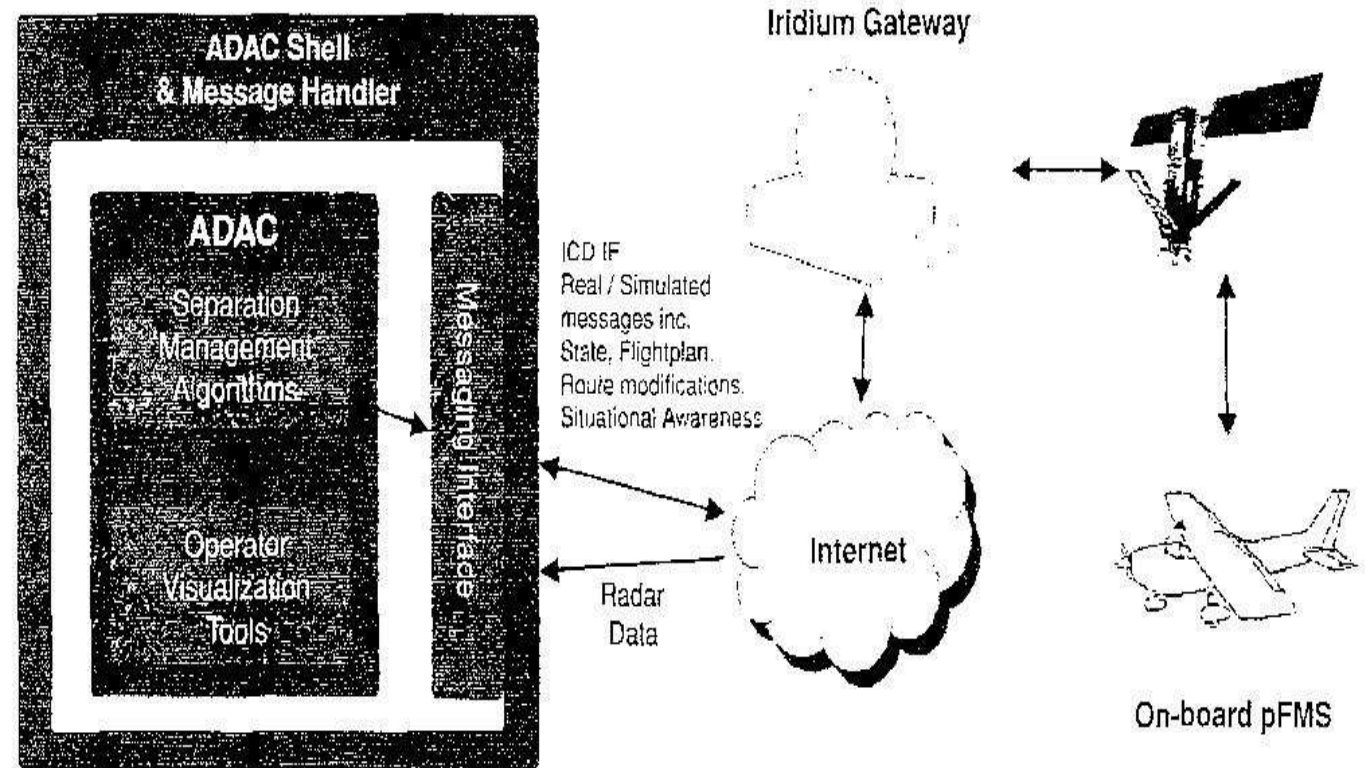


Figure 8.11 ADAC components and connectivity with the Iridium system

Market and Safety - Facts

- Messaging System
 - Allows gateway to the internet
 - Can monitor real of simulated aircraft
- Message monitors
 - Aircraft speed
 - Position
 - Altitude

Market and Safety - Facts

- ❑ Automated Separation Implementation
 - ❑ Virtual Predictive Radar
 - ❑ Boeing Proprietary
 - ❑ Successfully Managed and Separated aircraft LOS Scenarios 2-50 aircraft
 - ❑ Ability to swap-in different aircraft

Market and Safety - Facts

Smart Skies implementation summary

Table 8.6 Flight test summary

Variables impacting SM	Key flight test results		
1. Air space complexity	A. AC density and AC types: 2–50 AC over approximately 15×15 nm ² region with four aircraft types: UAS rotor craft, UAS fixed wing, Cessna, and Jetstream	B. Conflict geometry (angle of approach) Various angles of approach plus climbing and descending scenarios	C. AC speed and maneuverability CUAS: 0–10 knots QUAS: 40–60 knots ASL 80–120 knots Jetstream: 150–240 knots
2. Platform trajectory information content	A. 4D vs 7D trajectory information Results under evaluation	B. Information update rate: High (5 Hz) vs low (1 Hz) rates 0.5–1 Hz: Iridium 1–2 Hz: NextG	C. Uncooperative AC (radar) vs cooperative Uncooperative AC and MATS radar tracks successfully tracked and used to generate CTADS

3. Received information quality	A. Good communication quality: NextG, low latency (<3 s), no dropouts Iridium Nominal case of both NextG (prime) and Iridium (backup)	B. Marginal communication quality: Iridium, marginal latency (3–10 s) <i>Rarely occurred, usually associated with onboard hardware problems. If one link dropped the other link was automatically used</i>	C. Bad communication quality: Iridium, loss of communication, latency > 10 s <i>Rarely occurred, usually associated with onboard hardware problems. If one link dropped the other link was automatically used</i>
4. Operator response obedience	A. Automated vs manual Use of lateral autopilot with CTADS was successful. Easier for pilots vs manual with SA TADS	B. 4D vs 7D visualization for decisions 4D and 7D BDO displays were captured for further analysis	C. Mission success vs safety SM returned AC to flight plan after separation

Market and Safety - Issues

- ❑ America is facing a distribution of sUAV into its NAS, how will the FAA contend with sUAV carrying components and materials safely without invading privacy in areas they have never operated in before? Will FAA's efforts be harmonized internationally?
- ❑ What are the Safety issues created by sUAV and will increased sales compound this issue and how?
- ❑ Considering increased numbers of sUAV how is the best way to integrate them into the national air effectively and safely?

Market and Safety - Issue

❑ Continual safe separation distances between all aircraft and sUAV is a critical requirement to incorporating them into NAS



❑ Why It Matters

- ❑ Widespread use of commercial drones could radically alter how people do business
- ❑ Safety

Market and Safety - Issue

- Key requirement is understanding latency flow of process

Table 8.2 Information flow segment functions

Segment	Key functions
1. <i>User Data Source:</i> Prepare and transmit AC state information	A. Prepare aircraft state information for transmission this cycle B. Transmit information
2. <i>Track Capture:</i> Communication of aircraft information to SAA control center	C. Capture aircraft information D. Process data stream E. Connect and relay data stream to ground center
3. <i>Estimate True Track:</i> Derive aircraft predicted states from potentially several sources	F. Aggregate information from all aircraft this cycle G. Integrate, filter, and route received information H. Predict aircraft states using current and historical information
4. <i>Determine Control:</i> Evaluate separation constraints and perform separation management	I. Evaluate separation constraints this cycle over appropriate time windows J. Determine controls needed to achieve safe separations, perform EMER action if necessary K. Generate situation awareness information for local display L. Prepare controls and SA information for transmission
5. <i>Control Routing:</i> Determine communications path to aircraft	EMER. Prepare and route emergency information M. Establish routing for nominal transmissions this cycle N. Route nominal transmissions
6. <i>Control Dissemination:</i> Communications to aircraft	O. Establish aircraft connection
7. <i>User Data & Display:</i> Aircraft receives SA and control information and takes appropriate action	P. Capture control center information Q. Receive SA and control information R. Process control information S. Integrate all information for decision T. Perform control this cycle

Market and Safety - Indicators

- ❑ High profile companies getting into the action
 - ❑ Google
 - ❑ DHL
 - ❑ Amazon
 - ❑ Facebook
 - ❑ GoPro

Market and Safety - Indicators

- ❑ “Big box” companies doing market research i.e. Wal-Mart
- ❑ Increased video posts on YouTube
- ❑ Increasing main stream media reports
- ❑ Increasing peripheral component sales

Market and Safety - Indicators

- Increasing UAS capability



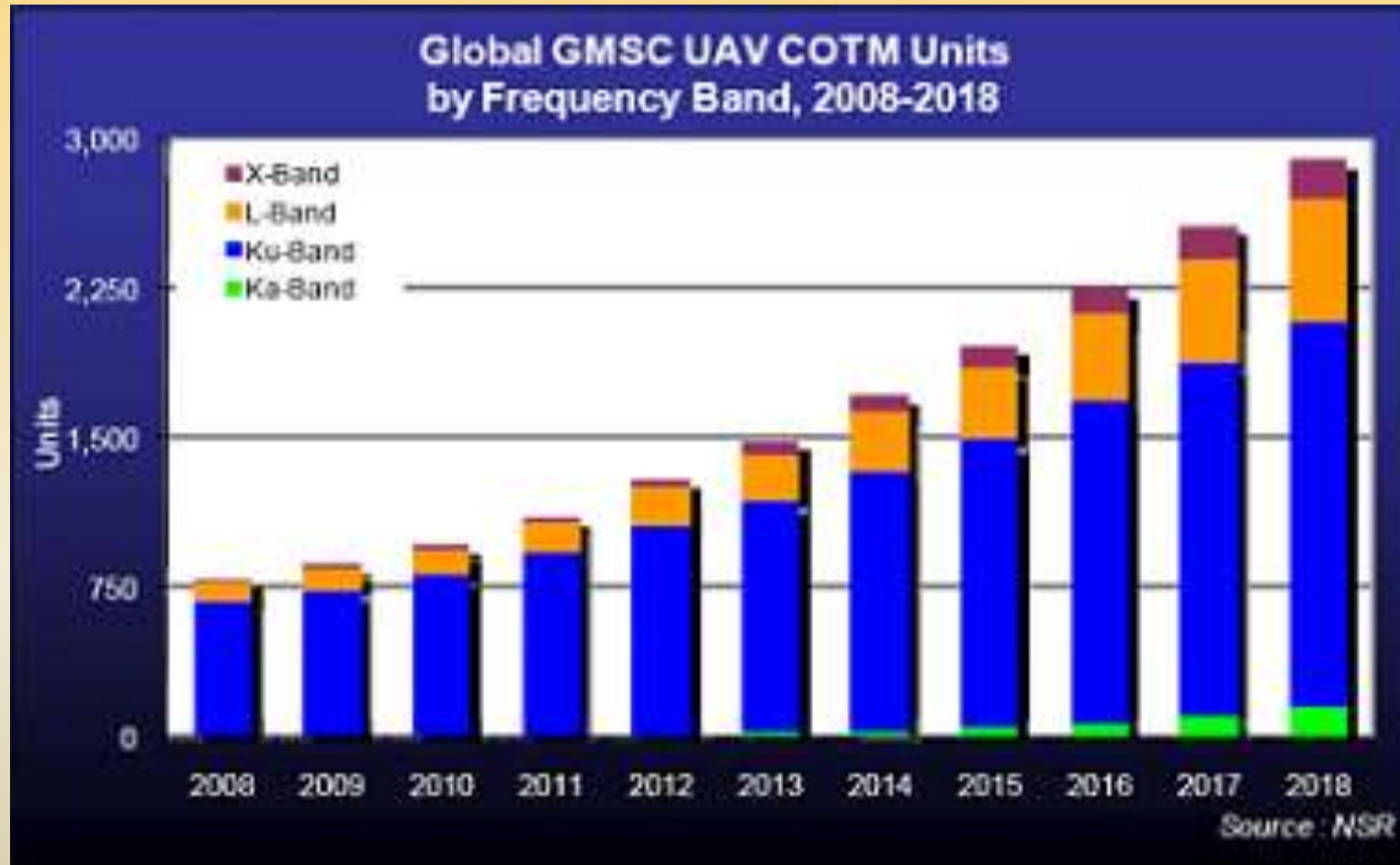
Market and Safety - Indicators

- **Hasselblad and Chinese company DJI form Strategic Partnership**

2015-11-05



Market and Safety - Indicators

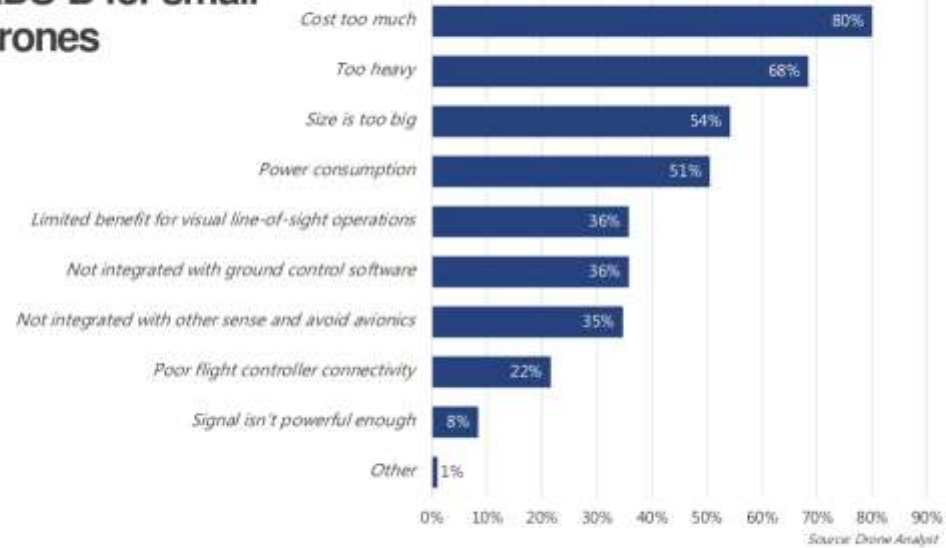


Market and Safety - Indicators

- ❑ FAA warns of ‘a million drones under people’s Christmas trees’
- ❑ FAA partners with Know Before You Fly organization
- ❑ FAA forms UAS Registration Task Force with members including: Wal-Mart, Google, Amazon, PrecisionHawk, DJI, etc.
- ❑ FAA Task Force will also explore options for streamlined system that would make registration less burdensome for commercial UAS operators

Market and Safety - Indicators

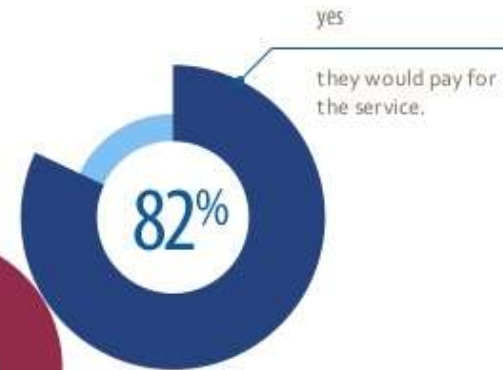
Perceptions about ADS-B for small drones



Market and Safety - Indicators

Consumers say..

they would pay a % of purchase price rather than a flat fee.



they would not pay more than \$50 per delivery.

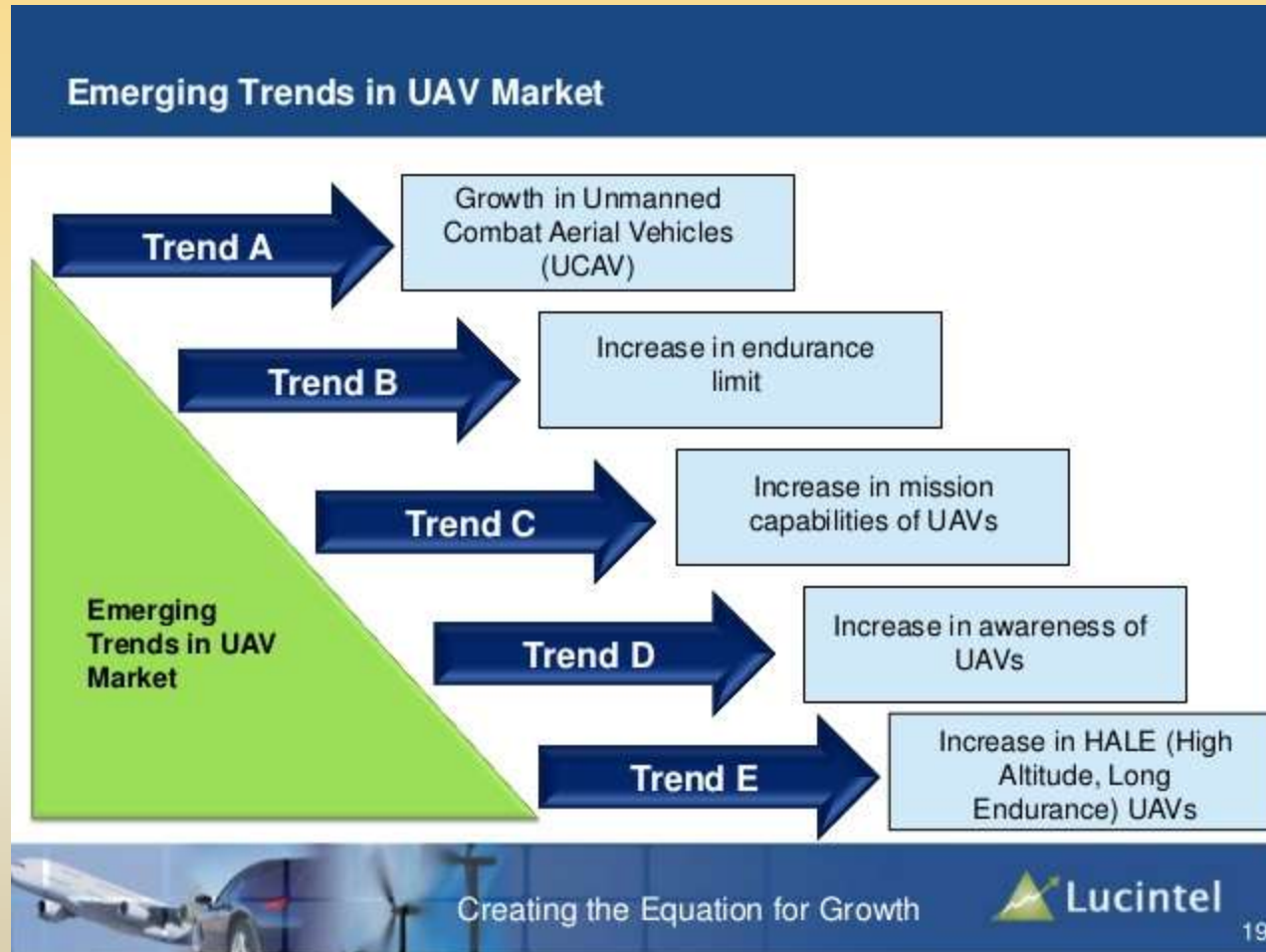


Source: Drone Analyst

A fixed charge might..

..leave many consumers out because of their unwillingness to pay more than overnight delivery.

Market and Safety - Indicators



Market and Safety - Indicators

Time Period	2015-2017			2015-2025		
Forecast	Economic Impact (Millions)	Taxes (Millions)	Jobs Created	Economic Impact (Millions)	Taxes (Millions)	Jobs Created
Total	\$13,657	\$80.22	70,240	\$82,124	\$482.39	103,776

Market and Safety - Indicators

- ❑ If FAA adopts new rules allowing commercial use of UAS in NAS, UAS products will be received rapidly into the marketplace
- ❑ The doubling rate can take place over either a three-year or six-year period
- ❑ With known rates of change in newer technologies, likely to be a three-year scenario given the fact that the potential marketplace is well aware of products unlike introduction in Japan
- ❑ The commercial agriculture market is the largest segment

Market and Safety - Indicators

Direct Spending and Employment in The U.S. from 2015-2025			
Year	Total Direct Spending	Total Direct Employment	Percent Change Over Previous Year
2015	\$1,153,370,225	11400	100%
2016	\$2,306,740,450	22800	50%
2017	\$3,460,110,675	34200	5%
2018	\$3,633,116,209	35910	5%
2019	\$3,814,772,019	37706	5%
2020	\$4,005,510,620	39591	5%
2021	\$4,205,786,151	41570	5%
2022	\$4,416,075,459	43649	5%
2023	\$4,636,879,232	45831	5%
2024	\$4,868,723,193	48123	5%
2025	\$5,112,159,353	50529	5%

Market and Safety - Indicators



Market and Safety - Indicators

- ❑ These 11 Companies Are Betting On The Drone Revolution
 - ❑ GoPro
 - ❑ Amazon.com Inc.
 - ❑ Wal-Mart Stores, Inc.
 - ❑ Alphabet
 - ❑ AeroVironment
 - ❑ Lockheed Martin
 - ❑ Northrop Grumman
 - ❑ NVIDIA
 - ❑ InvenSense
 - ❑ Ambarella
 - ❑ IXYS Corp

Market and Safety - Indicators

- ❑ Product Insights
 - ❑ Rotary blade UAVs contributed over 75% global revenue in 2013 due to ability to traverse several directions and hover
 - ❑ Easy flight control enabling aerial photography and surveillance
- ❑ Regional Insights
 - ❑ Relaxation in regulations and increasing use in law enforcement and agricultural applications in the European countries.
 - ❑ Increasing government initiatives and building retrofits have encouraged users across Asia Pacific region to use drones for various applications
- ❑ Competitive Market Share Insights
 - ❑ BAE Systems, DJI, Elbit Systems, General Atomics, AeroVironment Inc., Parrot SA, Israel Aerospace Industries, Northrop Grumman, Lockheed Martin Corporation, The Boeing Company, and Textron Inc.

Market and Safety - Judgments

- ❑ No reported accidents in 2015, but FAA concerned sUAS can very seriously harm planes
- ❑ Toys and small drones that don't present a safety threat are likely to be exempt
- ❑ Drones weighing a pound or two that cannot fly higher than a few hundred feet should be considered less risky, but heavier ones and those that can fly thousands of feet pose more of a problem
- ❑ FAA and the Transportation Department create continuing task force including government and industry officials, pilots and hobbyists
- ❑ Recommend which drones should be required to register

Market and Safety - Judgments

Application Insights

- Developing Solar powered drones to provide Internet access to remote areas
 - Google, Inc.
 - Facebook
- Government applications constituted over 40% in 2013, caused increase use
 - Law enforcement
 - Security
 - Surveillance activities

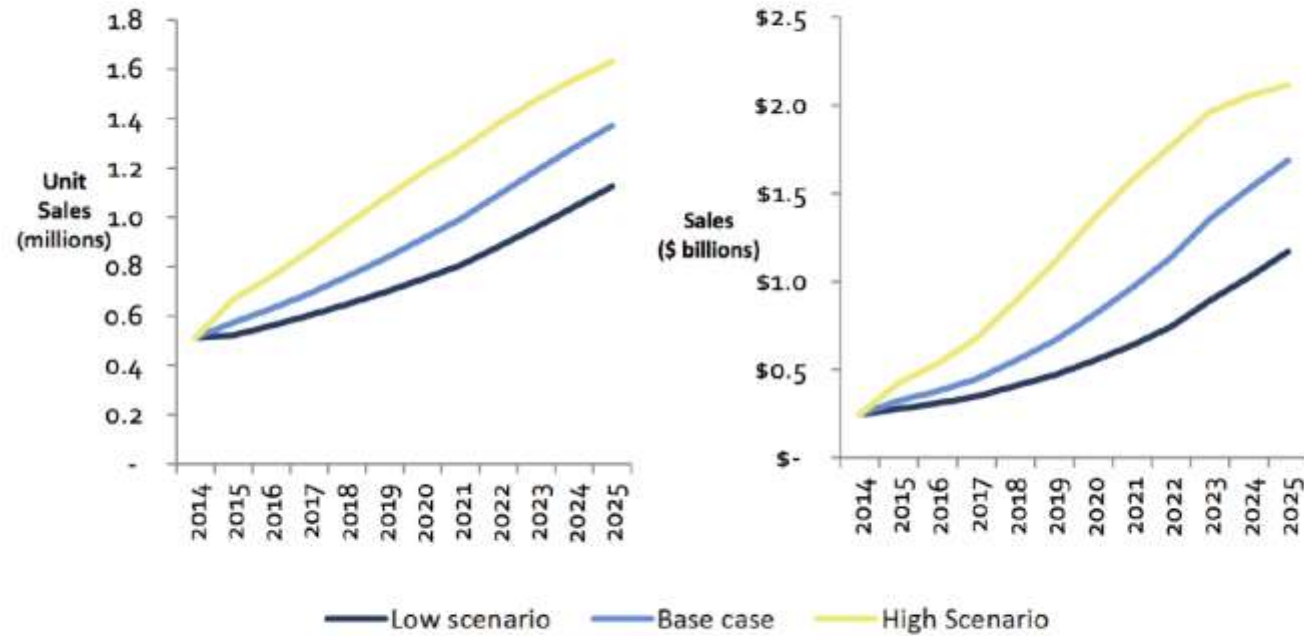
Market and Safety - Judgments

Application Insights

- Agricultural applications are expected to grow because of:
 - Increased use in crop management
 - Imaging
 - Mapping
 - Wildlife patrol
 - Fire observation
- Other applications

Market and Safety - Judgments

Accelerating Regulatory Certainty Can Push the Market for UAVs over \$2 Billion



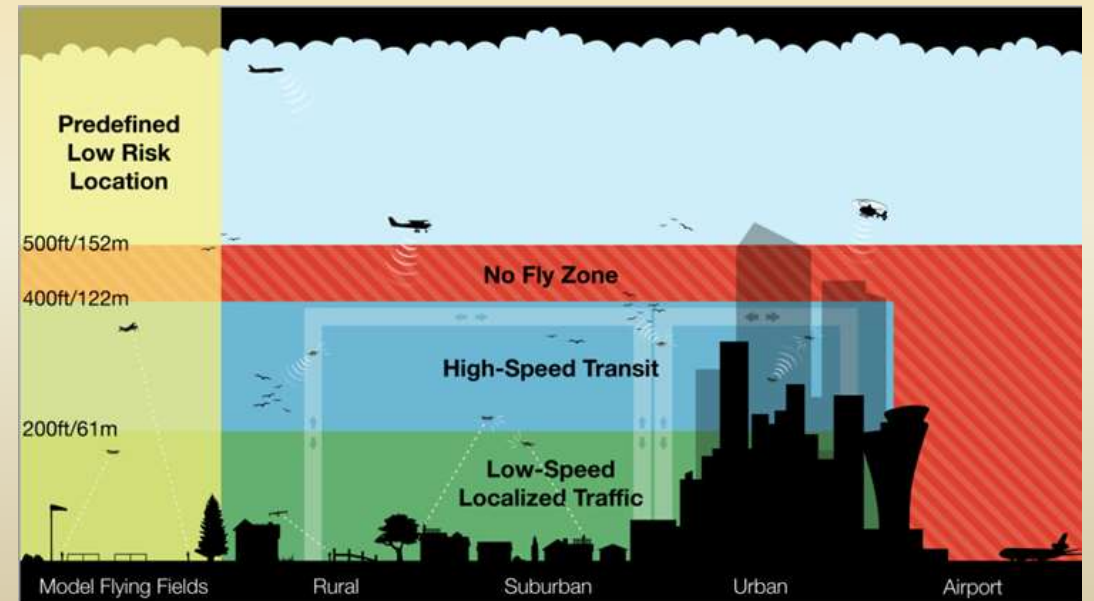
Source: Lux Research, Inc.
www.luxresearchinc.com

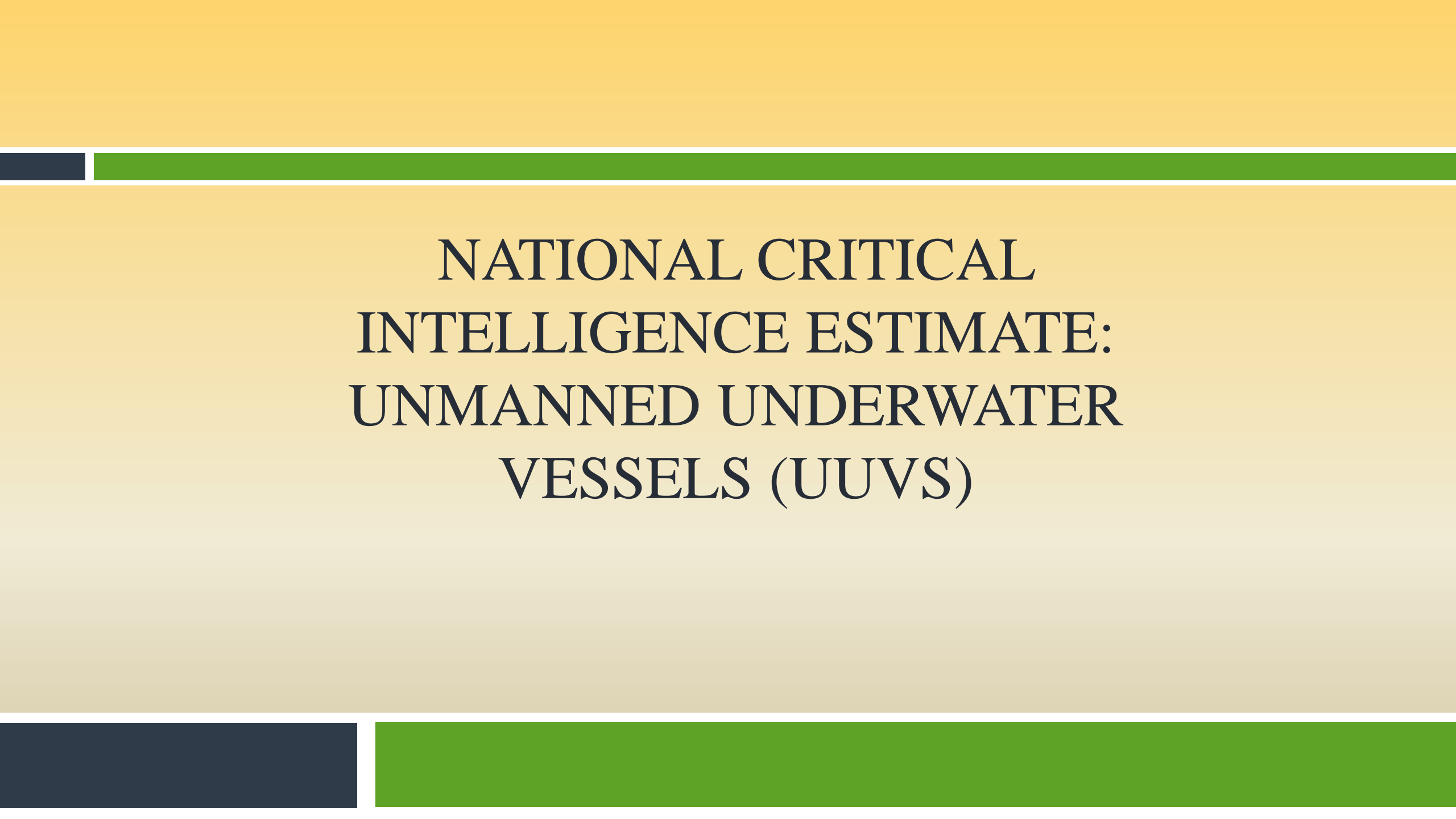
Market and Safety - Judgments

- ❑ Many still needing help with entry into drone flight
- ❑ Increase in consulting for purchase, operation, ongoing support
- ❑ Increase in number of customer reviews for peer scrutiny
- ❑ Increase in drone collaboration through social media i.e. Meetup.com

Recommendations

- Regulated Drone Highways for commercial package delivery
- Capability and Payload should determine Regulation requirement
- Beacon enabled by photocell
- Registered drones broadcast ID
- Pre-flight checklist added to box by manufacture and FAA rules and regs.
- FAA registration for commercial drones
- Sense & Avoid, Low Cost Radar, Mobile Radar
- Geofencing
- Training
- Optical-electro vision systems





NATIONAL CRITICAL
INTELLIGENCE ESTIMATE:
UNMANNED UNDERWATER
VESSELS (UUVS)

UUVs

- Collection of real-time oceanographic data
- Subsea pipeline monitoring
- Subsea telemetry control
- Submersible retrieval buoys
- River seepage monitoring
- Diver location and positioning

UUVs

- Underwater asset monitoring and location based services
- Wireless underwater lift bags
- Explosive monitoring on ships and harbors
- Mule for special forces equipment
- Mine clearing
- Black box detection

UUVs

Issues/ Difficulties:

- Communications
- Power supplies
- Single Mission capabilities
- Launch and Retrieval
- Water environment

UUVs

NRL – Navel Research Lab



- Modified UUV
- Named the 'Flimmer' – Modified flying submarine
- Capable of flying and operating under-water
- Bio-inspired Autonomous Vehicle
- Can service multiple mission plans

UUVs

1. Flight
2. Approach
3. Entry
4. Recovery

Flimmer



UUVs

Unmanned Underwater Vehicles Market (2014–2019)



UUVs

- ❑ Global Unmanned Underwater Vehicles market will exhibit robust growth next five years
- ❑ Global ROV market estimated to be \$1.2 billion in 2014 and expected to register a CAGR of 20.11% in 2019
- ❑ Global AUV market estimated to be \$457 million in 2014 and expected to register a CAGR of 31.95% in 2019
- ❑ ROV and AUV markets driven by increasing need of ROV and AUV in:
 - ❑ oceanographic studies
 - ❑ underwater inspection and maintenance
 - ❑ surveillance and security
 - ❑ offshore drilling
- ❑ Evolution of technology: better endurance, miniaturization, and enhanced payloads, ROV and AUV are efficiently used for undersea activities

UUVs

- ❑ Commercialization of ROV and AUV and increased capabilities have revolutionized growth over years
- ❑ Offshore drilling will remain prime sector for ROV
- ❑ Defense and oceanographic studies will remain major sector for AUV
- ❑ Asia-Pacific, Latin American, and African regions will be emerging markets for UUV
- ❑ SAAB (Sweden), Fugro (Netherlands), Oceaneering (U.S.), will be market leaders that occupy significant market share for ROV.
- ❑ Kongsberg (Norway), Teledyne (U.S.), Bluefin Robotics (U.S.), and Atlas Elektronik (Germany), will be the leaders in the AUV market

UUVs

Underwater Unmanned Vehicles (UUVs)

- ❑ Another legal issue for the future will be the legal status of UUVs and under what bodies they are governed
- ❑ A UUV's status has important legal ramifications
- ❑ Resolution of the vessel/non-vessel/warship issue will determine the extent to which, if at all, a UUV will be:
 - ❑ Entitled to exercise certain navigational rights
 - ❑ Allowed particular immunities
 - ❑ Eligible to carry out a number of important maritime functions
 - ❑ Subject to other international maritime legal regimes
 - ❑ Entitled to exercise belligerent rights

Summary

- ❑ Evolution of technology:
 - ❑ Better endurance
 - ❑ Miniaturization
 - ❑ Enhanced payloads
 - ❑ ROV and AUV are efficiently used for undersea activities

- ❑ UAV opportunity is expected to surpass U.S. \$7 billion over next 10 years

- ❑ Increase in demand is expected in HALE segment of UAV market

- ❑ Degree of technical change very high in UAS market in coming years

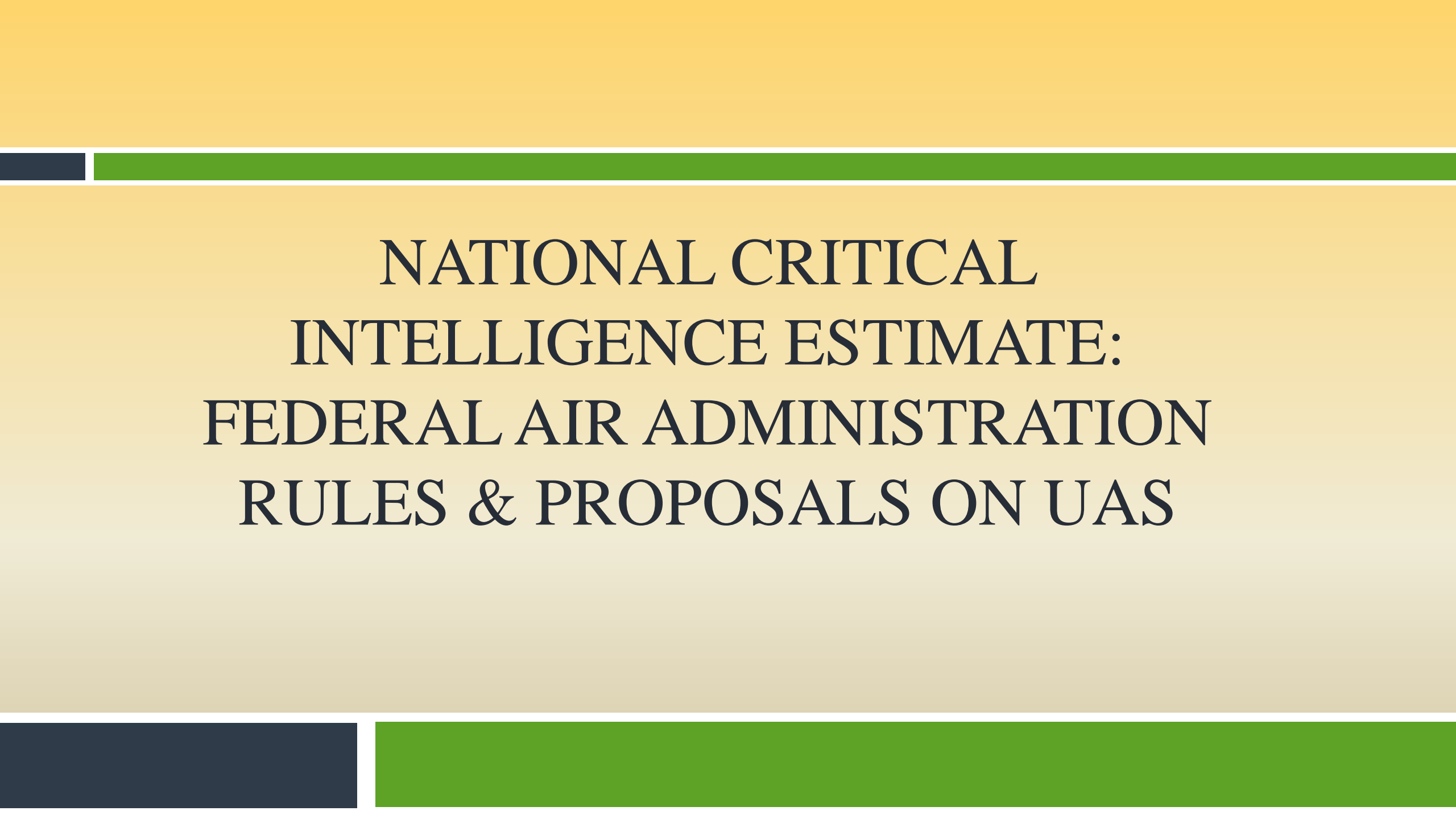
- ❑ Latest innovation: Solar powered UAV have endurance of more than 300 hours

- ❑ UAVs in development for future roles could greatly expand numbers

- ❑ UAS market is opening up many new opportunities from UAV pilots to electronics and cameras

Summary

- ❑ Military uses will include delivery of food, medicine and other supplies for troops
- ❑ Short or vertical-takeoff & landing UAVs will be useful in humanitarian aid missions
- ❑ North America continues to be leading global UAV market with ~ 60%-70%
- ❑ Asia Pacific and Europe with 20% and 16% respectively
- ❑ Significant increase in demand for UAVs from emerging countries, currently used in more than 50 countries
- ❑ A substantial increase of new entrants in UAV supply chain will occur over the next decade
- ❑ UAS market is opening up new opportunities from UAV pilots to electronics and cameras



NATIONAL CRITICAL
INTELLIGENCE ESTIMATE:
FEDERAL AIR ADMINISTRATION
RULES & PROPOSALS ON UAS

FAA Rules & Proposals - Facts

- ❑ The Federal Aviation Administration (FAA) is charged with registering and issuing a certificate of registration to the owner of an aircraft that meets requirements of 49 U.S.C. 44102
- ❑ These statutory requirements are augmented by regulations in part 47 of title 14, Code of Federal Regulations

DID YOU KNOW?

The FAA Modernization Reform Act of 2012 required the FAA to create rules for the use of unmanned aircraft in the U.S.



[Click here to learn more.](#)

FAA Rules & Proposals - Facts

- ❑ Title 14 Code of Federal Regulations
 - ❑ Civil aircraft means aircraft other than public aircraft
 - ❑ UAS fall under category of aircraft that need experimental certificates
 - ❑ Model aircraft do not fall under experimental certificates
 - ❑ Model aircraft differ from UAVs --do not carry the capacity for autonomous flight
- ❑ FAA Modernization and Reform Act of 2012 (FMRA)--Congress mandated that FAA develop comprehensive plan to safely accelerate the integration of civil UAS in the National Airspace System (NAS)

FAA Rules & Proposals - Facts

- ❑ FAA reports progress in enabling UAS operations
 - ❑ Created UAS test site program to encourage further research/testing of UAS operations in real-world environments
 - ❑ Issuing notice of proposed rulemaking, Operation and Certification of sUAS that sets forth framework for integrating sUAS operations in the NAS
 - ❑ Developing Pathfinder program to encourage research/innovation that will enable advanced UAS operations
 - ❑ Issuing exemptions under section 333 of FMRA to permit commercial operations

FAA Rules & Proposals - Facts

The FAA's Role: Safety

- UAS are inherently different from manned aircraft
- Must be safely integrated into a National Airspace System (NAS)
- NAS evolving from ground-based navigation aids to a GPS-based system in NextGen
- Provides air traffic control services
- Safe integration of UAS involves gaining a better understanding of operational issues:
 - Training requirements
 - Operational specifications
 - Technology considerations

FAA Rules & Proposals - Facts

UAS Test Site Selection Criteria

- ❑ Risk
- ❑ Safety
- ❑ Climate
- ❑ Location of ground infrastructure
- ❑ Research needs
- ❑ Airspace use
- ❑ Geography
- ❑ Aviation experience

FAA Rules & Proposals - Facts

UAS Test Site Operators

- University of Alaska
- State of Nevada
- New York's Griffiss International Airport
- North Dakota Department of Commerce
- Texas A&M University – Corpus Christi
- Virginia Polytechnic Institute and State University (Virginia Tech)

FAA Rules & Proposals - Facts

FAA UAS Test Site Map



FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ University of Alaska
 - ❑ Seven climactic zones
 - ❑ Geographical diversity with Hawaii and Oregon
 - ❑ Develop standards
 - ❑ UAS categories
 - ❑ State monitoring
 - ❑ Navigation
 - ❑ UAS operations safety

FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ State of Nevada
 - ❑ UAS Standards and operations
 - ❑ UAS Operator standards and certification requirements
 - ❑ Impact of UAS on Air Traffic Control procedures
 - ❑ How to integrate UAS with NextGen
 - ❑ Selection contributes to geographic and climate diversity

FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ New York's Griffiss International Airport
 - ❑ Develop test and evaluation processes
 - ❑ Develop verification and validation processes
 - ❑ Work subject to FAA oversight
 - ❑ Research UAS sense & avoid capabilities
 - ❑ Research complexities of integrating UAS into the congested northeast airspace

FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ North Dakota Department of Commerce
 - ❑ Develop UAS airworthiness essential data
 - ❑ Validate high reliability link technology
 - ❑ Conduct human factors research
 - ❑ Offers a test range in Temperate (continental) climate zone
 - ❑ Includes a variety of different airspace which benefits multiple users

FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ Texas A&M University – Corpus Christi
 - ❑ Develop UAS vehicle and operation system safety requirements
 - ❑ Create protocols and procedures for airworthiness testing
 - ❑ Selection contributes to geographic and climate diversity

FAA Rules & Proposals - Facts

UAS Test Site Operators

- ❑ Virginia Polytechnic Institute & State University (Virginia Tech)
 - ❑ Conduct UAS failure mode testing
 - ❑ Identify operational and technical risk areas
 - ❑ Evaluate operational and technical risk areas
 - ❑ Includes test site range locations in Virginia and New Jersey

FAA Rules & Proposals - Facts

FAA Research Goals

- System Safety & Data Gathering
- Aircraft Certification
- Command & Control Link Issues
- Control Station Layout & Certification
- Ground & Airborne Sense & Avoid
- Environmental Impacts

FAA Rules & Proposals - Facts

Two Ways for FAA to Approve UAS Operation

1. Obtain an experimental airworthiness certificate for private sector (civil) aircraft to do research and development, training and flight demonstrations
2. Obtain a Certificate of Waiver or Authorization (COA) for public aircraft
 - ❑ 545 COAs active as of December 4, 2013
 - ❑ Routine operation of UAS over densely-populated areas is prohibited
 - ❑ Class B airspace exists over major urban areas and contains the highest density of manned aircraft in the National Airspace System.

FAA Rules & Proposals - Facts

Current US (FAA) UAS Regulations

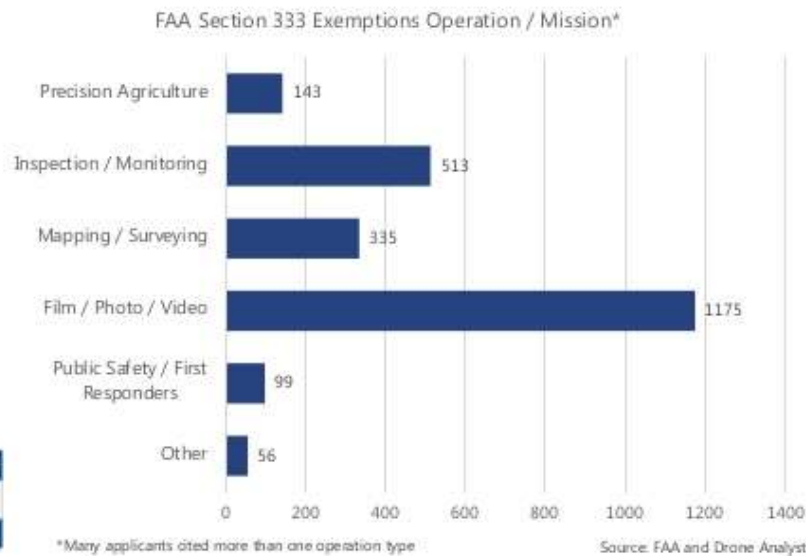
- Currently, a Certificate of Authorization (COA) is required to operate an unmanned aerial vehicle (UAV) in US national airspace
- Only federal, state, or local agencies are considered for COA awards
- FAA test sites (proving grounds) have been awarded to Virginia, Texas, Alaska, New York, North Dakota and Nevada; will conduct critical research into the certification and operational requirements necessary to safely integrate UAS into the national airspace over the next several years
- Remote Control (RC) hobbyists can operate remotely controlled vehicles for recreational uses only:
 - Not allowed for commercial business use of any kind → cannot fly to make money!
 - RC vehicle cannot exceed 400 feet above ground level (AGL)
 - RC vehicle cannot interfere with any type of air traffic - must be flown away from airports and air traffic
- FAA Modernization and Reform Act of 2012 (H.R. 658)
 - Signed into law on February 14, 2012 by President Obama
 - This bill orders the FAA to figure out how to integrate commercial UAV usage into the U.S. National Airspace System (NAS)
 - Also under the bill, the FAA is required to provide military, **commercial**, and privately-owned drones with expanded access to U.S. airspace by Sep. 30, 2015
 - That means permitting unmanned drones controlled by remote operators on the ground --also called unmanned airborne systems (UAS) or unmanned aerial vehicles (UAVs)--to fly in the same airspace as airlines, cargo planes, business jets and private aircraft.
- More information can be found at <http://www.faa.gov/about/initiatives/uas/>

FAA Rules & Proposals - Facts

- ❑ By Title 14 Code of Federal Regulations, any aircraft operation in NAS requires certificated and registered aircraft, a licensed pilot, and operational approval
- ❑ Section 333 of the FAA Modernization and Reform Act of 2012 (FMRA) grants Secretary of Transportation authority to determine whether an airworthiness certificate is required for a UAS to operate safely in NAS
 - ❑ This authority is being leveraged to grant case-by-case authorization for certain unmanned aircraft

FAA Rules & Proposals - Facts

Exemptions by market use case



Petitions Granted	Petitions Closed
1,658	399

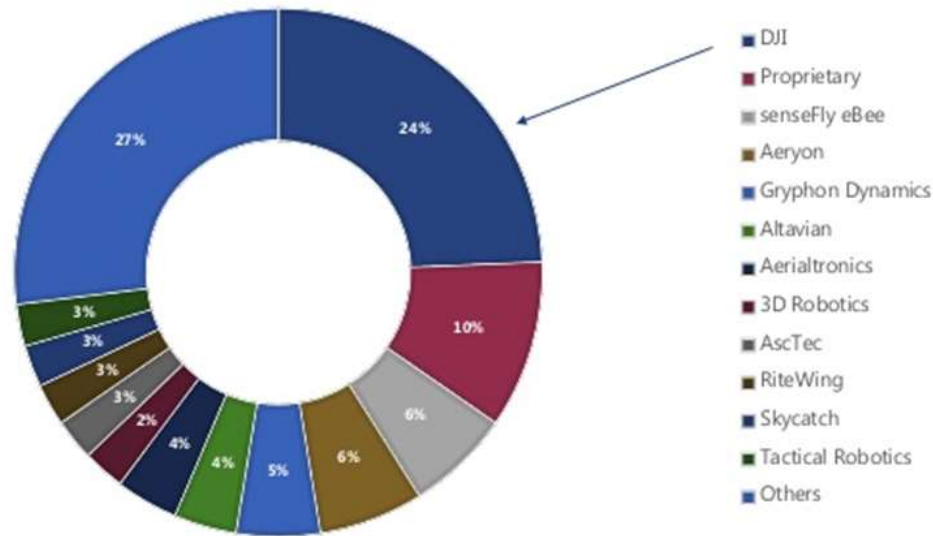
As of 9/22/2015

- ❑ Most exemptions are used commercially
- ❑ Testing delivery systems and use in field

FAA Rules & Proposals - Facts

Answer

Section 333 Exemptions as of March, 2015



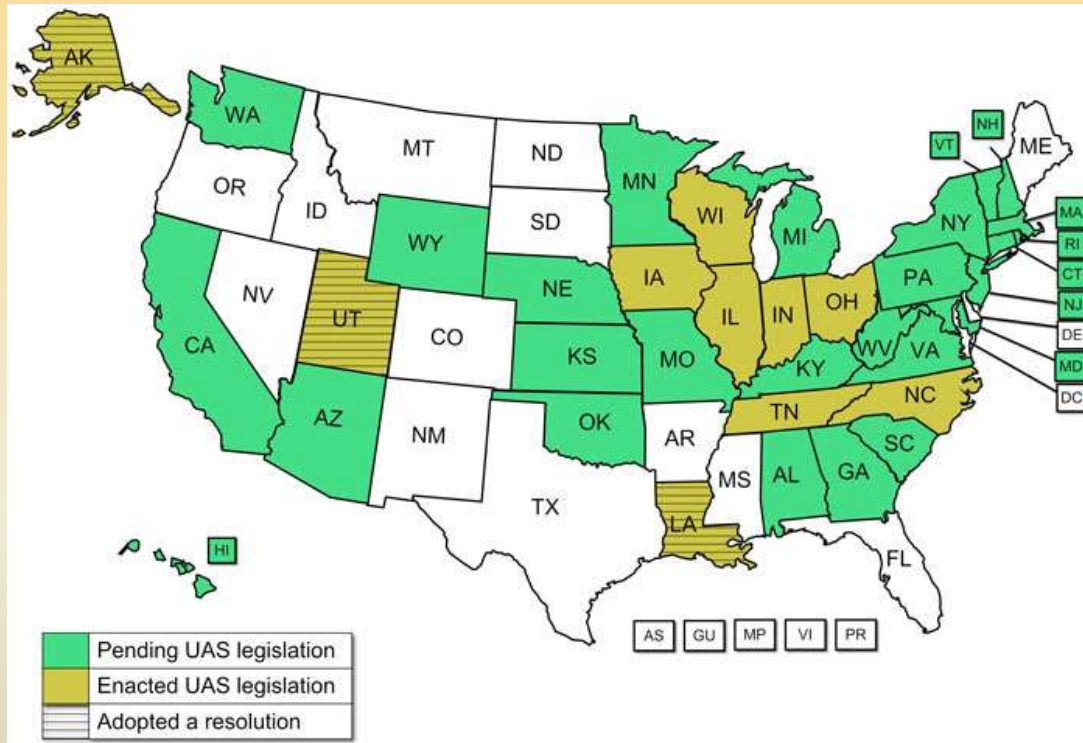
Source Cooley, LLP

Drone Analyst
INSTITUTE FOR THE COMMERCIAL DRONE INDUSTRY

- ❑ Others include: Google, Amazon, Wal-Mart
- ❑ DJI - Chinese Drone Manufacturer working in U.S.
- ❑ Other companies build closed testing facilities and do not need exemptions

FAA Rules & Proposals - Facts

- 43 states have introduced more than 150 bills and resolutions affecting the UAV industry



FAA Rules & Proposals - Facts

- ❑ FAA Task Force created to discuss registration of UAS headed by chairs from FAA and Google recommends:
 - ❑ UAS between the weights 0.55lbs-55lbs (0.25kg-25kg) that are operated outdoors need registered
 - ❑ Unlike manned aircraft, registration number will belong to operator, so one number can apply to all of his/her aircraft
 - ❑ The registrant must be over 13 years old, no citizenship requirement or fee to register
 - ❑ Registrants must provide name and address
 - ❑ Other personal information optional

FAA Rules & Proposals - Facts

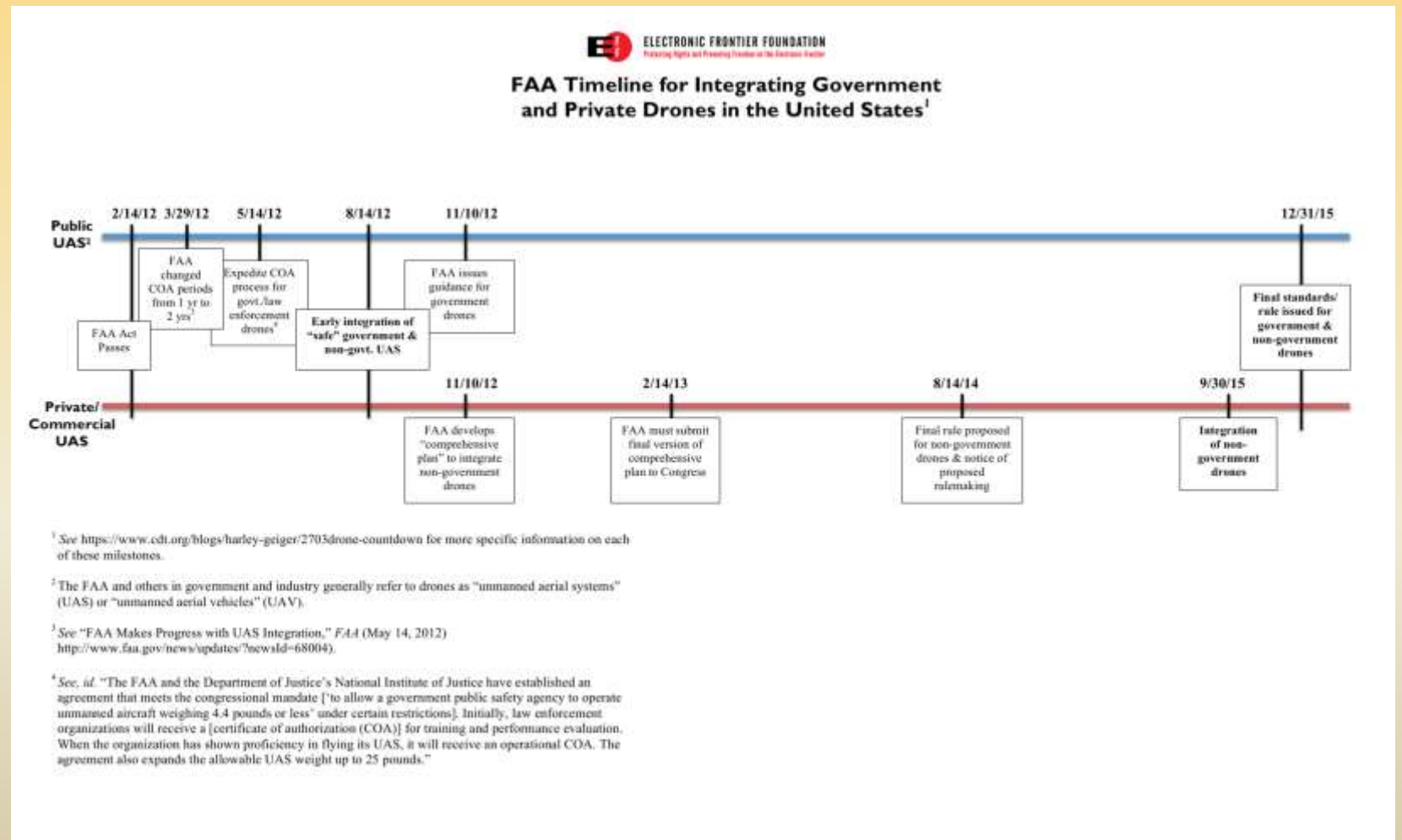
- ❑ The registration process should occur online through multiple avenues
- ❑ The application could be on FAA's website but also through vendor and stakeholder websites
- ❑ Operators will only need to register aircraft before they fly, instead of at point of sale
- ❑ Registration mandatory prior to operation of a UAS in NAS
- ❑ Whether owner chooses to rely on serial number or affix FAA-issued registration number to UAS, marking must be accessible and maintained in a condition that is readable and legible

UAS Registration Task Force Aviation Rulemaking Committee Recommendations Summary 11/21/2015

- ❑ The FAA wants to implement registration process within 30 days
- ❑ Task Force wants the FAA to accept recommendations in entirety
- ❑ Task Force recommends that the FAA establish a clear and proportionate penalty framework for violations
- ❑ Not Addressed: Federal regulations do not specifically define how FAA should address cybersecurity vulnerabilities for aircraft operating in NAS

FAA Rules & Proposals - Facts

Timeline addition:
11/21/15
FAA Unmanned Aircraft
Systems Registration Task
Force Aviation
Rulemaking Committee
Task Force
Recommendations
Final Report



FAA Rules & Proposals - Facts



FAA Rules & Proposals - Facts

Drone Rules & FAA Regulations: Consumer vs. Commercial Use

Commercial use is currently banned by the FAA, but how do we know the difference?

Who is a consumer?

- You're not making money on the footage (and no one else is)
- You're not doing anything that would need approval from the FAA

And basically, you follow community guidelines, no fly zones, FAA tips for flying, and common sense

Who is a commercial user?

- You sell any photos or videos taken by a drone, i.e. wedding or concert photography
- You're monetizing on any videos or photos uploaded to the internet
- You carry out services for farming, filming a scene for a movie, etc.
- You use drones for other professional services, like security or deliveries

Regulations for Consumer Use

- Don't fly by airports (not even close), national parks, or military bases
- Keep your drone under 400 feet and fly under obstacles, not over them
- Don't let your drone stray out of your eyesight (especially for models with automated GPS flight capabilities)
- Don't fly drunk or on drugs

Proposed Commercial Regulations

- Businesses must use drones under 55 lbs.
- The operator must be within visual line-of-sight of the unmanned aircraft.
- All unmanned aircraft must be flown during daylight hours.

BUY THE BEST DRONE

buythebestdrone.com

FAA Rules & Proposals - Facts

Canadian Proposals

- ❑ UAVs 55lbs (25kgs) or less that are operated within visual line-of-sight
- ❑ Establish classifications including a proposal for possibility of having a very small (lower threshold) category of aircraft
- ❑ Clarify terminology
- ❑ Establish aircraft marking & registration requirements

FAA Rules & Proposals - Facts

Canadian Proposals

- ❑ Address personnel licensing & training
- ❑ Introduce more rigorous safety requirements
- ❑ Create greater awareness of legal responsibilities of UAV operators
- ❑ Mitigate the risks UAVs could pose to other airspace users, as well as people and property on the ground

FAA Rules & Proposals - Facts

Canadian Proposals

- ❑ This new and rapidly evolving industry introduces regulatory challenges
- ❑ This is why Transport Canada:
 - ❑ May have to adjust new regulations in a few years to account for new technologies and market demands
 - ❑ Will use both regulatory / non-regulatory instruments to enhance awareness
 - ❑ Collaborate with key industry partners

FAA Rules & Proposals - Facts

- ❑ FAA Notice of Policy: UAS Operations in the NAS (72 Fed. Reg. 6689 (Feb. 13, 2007))
- ❑ Regulatory standards need to be developed to enable current technology for unmanned aircraft to comply with Title 14 CFR
- ❑ In order to ensure safety, operator is required to establish the UAS airworthiness either from FAA certification
- ❑ Applicants have to demonstrate that a collision with another aircraft or other airspace user is extremely improbable
- ❑ The pilot-in-command concept is essential to safe operation of manned operations
- ❑ The FAA's UAS guidance applies pilot-in-command concept to unmanned aircraft and includes minimum qualification and currency requirements

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

- ❑ Operator Certification and Responsibilities
- ❑ Pilots of a small UAS would be considered “operators”
- ❑ Operators would be required to:
 - ❑ Pass an initial aeronautical knowledge test
 - ❑ Be vetted by Transportation Security Administration
 - ❑ Obtain an unmanned aircraft operator certificate

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

- ❑ Operator Certification and Responsibilities
 - ❑ Pass a recurrent aeronautical knowledge test every 24 months
 - ❑ Be at least 17 years old
 - ❑ Make available to FAA the sUAS for inspection or testing, and any associated documents / records required to be kept

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

- ❑ Operator Certification and Responsibilities
 - ❑ Report an accident to FAA within 10 days of any operation that results in injury or property damage
 - ❑ Conduct a preflight inspection, to include specific aircraft and control station systems checks, to ensure sUAS is safe for operation
- ❑ Proposed rule would not apply to model aircraft that satisfy all criteria specified in Section 336 of Public Law 112-95

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

- ❑ Operational Limitations
 - ❑ Unmanned aircraft must weigh less than 55 lbs. (25 kg)
 - ❑ Visual line-of-sight (VLOS)
 - ❑ Small unmanned aircraft may not operate over any persons not directly involved in the operation

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

- ❑ Operational Limitations
 - ❑ Daylight-only operations
 - ❑ Must yield right-of-way to other aircraft, manned or unmanned
 - ❑ First-person view camera cannot satisfy “see-and-avoid” requirement but can be used as long as requirement is satisfied in other ways
 - ❑ Maximum airspeed of 100 mph (87 knots)
 - ❑ Maximum altitude of 500 feet above ground level
 - ❑ Minimum weather visibility of 3 miles from control station

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

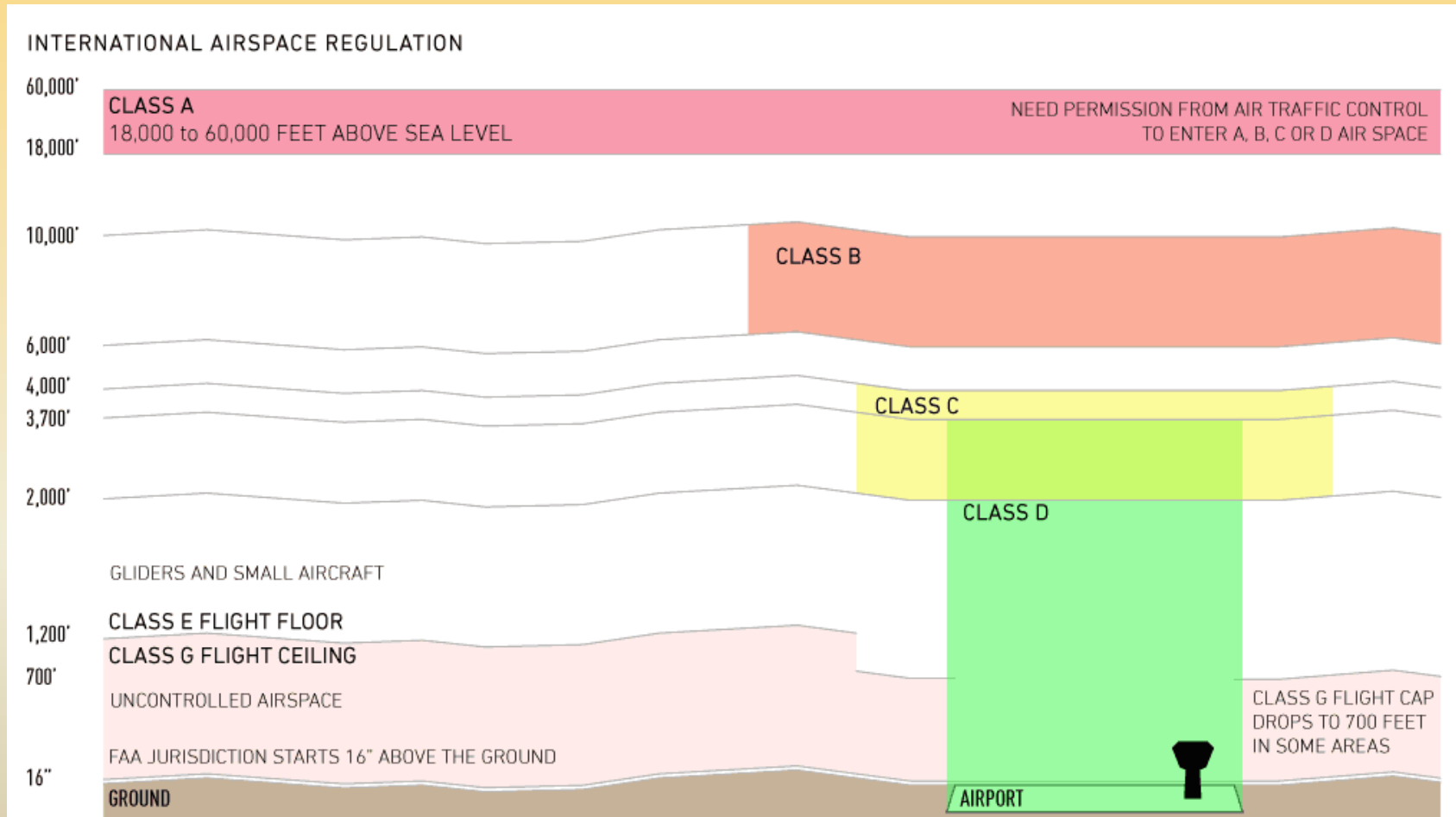
- ❑ Operational Limitations
 - ❑ No operations are allowed in Class A (18,000 feet & above) airspace
 - ❑ Operations in Class B, C, D, E and G airspace are allowed with the required air traffic control permission
 - ❑ No person may act as an operator or visual observer for more than one unmanned aircraft operation at one time
 - ❑ No careless or reckless operations

FAA Rules & Proposals - Facts

sUAS Notice of Proposed Rulemaking

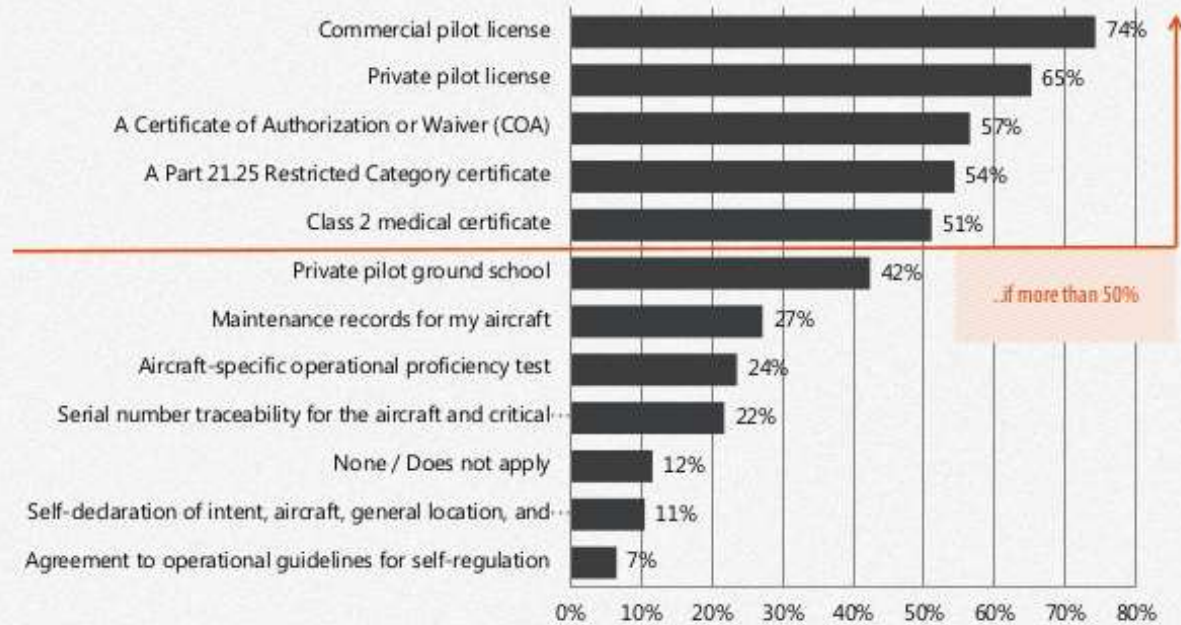
- ❑ Operational Limitations
 - ❑ Requires preflight inspection by operator
 - ❑ A person may not operate a sUAS if he or she knows or has reason to know of any physical or mental condition that would interfere with safe operation of a sUAS
 - ❑ Proposes a micro-UAS option that would allow operations in Class G airspace, over people not involved in operation, provided operator certifies / she has requisite aeronautical knowledge to perform operation

FAA Rules & Proposals - Facts



FAA Rules & Proposals - Facts

Unfavorable rules..



FAA Rules & Proposals - Facts

UAV/Drone Use By the U.S.

- **Military Operations of Surveillance and Attack Enemy Targets**
- **DOD and FAA UAV/Drone Development and Research**
- **FAA's six selected UAV/Drone Research Sites**
- **U.S. Movie Industry using UAV/Drones for Commercial Ventures**
- **Hobbyist Model Aircraft/ UAV/Drone Used Status**
- **Cannot be Used For Profit**
- **Cannot be Used for 501c Non-Profits Search and Rescue Organizations**

FAA Rules & Proposals - Facts

FAA on UAV's (Drones)

- **There are no current FAA regulations for the use commercial use of UAV/Drones**
- **U.S. Congress has charged the FAA to develop new regulations and laws for this new up and coming industry**
- **Drones cannot be used for commercial paid purpose**
- **Only allowable use of UAV/Drones is under the hobbies status**
- **Six research centers has been authorized for UAV/Drone Flight and Development (Texas A&M University at Corpus Christi is one of those sites**
- **FAA has refuses to give except regulations to Search and Rescue organizations like Texas Equu-Search to find lost individuals**
- **FAA gave Certificates of exception to four of the six major movie film producers to allow the use of UAV/Drones in making movies for profits**

FAA Rules & Proposals - Issues

- ❑ What rules and regulations can the FAA enact to ensure the safety and privacy of Americans from amateur or malevolent use of UAS?
- ❑ Is registration of UAS impossible for the FAA?
- ❑ What are the most effective technologies the FAA can implement to incorporate UAS into the NAS?

FAA Rules & Proposals - Indicators

Application Use of UAV's (Drones)in Public Safety

- **Military Surveillance and Target Acquisition**
- **Law Enforcement Traffic Monitoring and Crowd Control**
- **Law Enforcement Major Highway Multiple Vehicle Accident**
- **Law Enforcement High Risk Warrants and Arrest**
- **Fire Fighting Tactical View of Fire Scene**
- **Fire Fighter High Angle Rescue or Collapse Structure**
- **CERT UAV's/Drones in Support of Local Authorities**
- **Search and Rescue of Lost Child or Lost Adult**
- **Water Ways Search of Lost Person(s) and Water Craft**
- **HAZMAT Ariel View of Scene**
- **Train Derailments.**
- **Natural Disaster Sites Ariel Surveys for Emergency Management**
- **Agriculture, Wildlife, Flood Plains, and Land Management**

FAA Rules & Proposals - Indicators

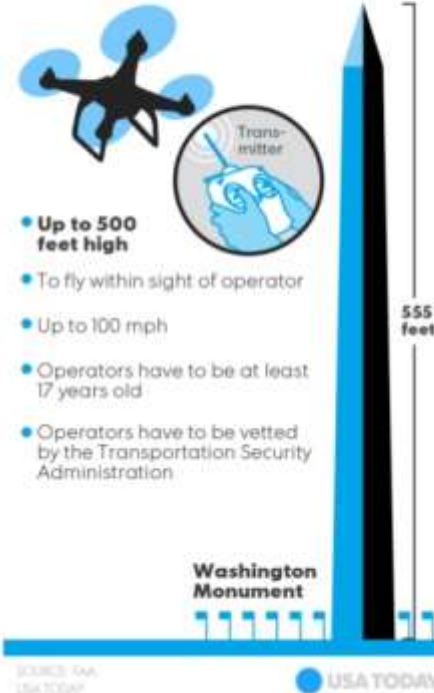
Existing Restrictions

Aircraft must be less than 55 lbs. (25 kg)

Daylight operations only

Cannot fly over people not involved with the operations

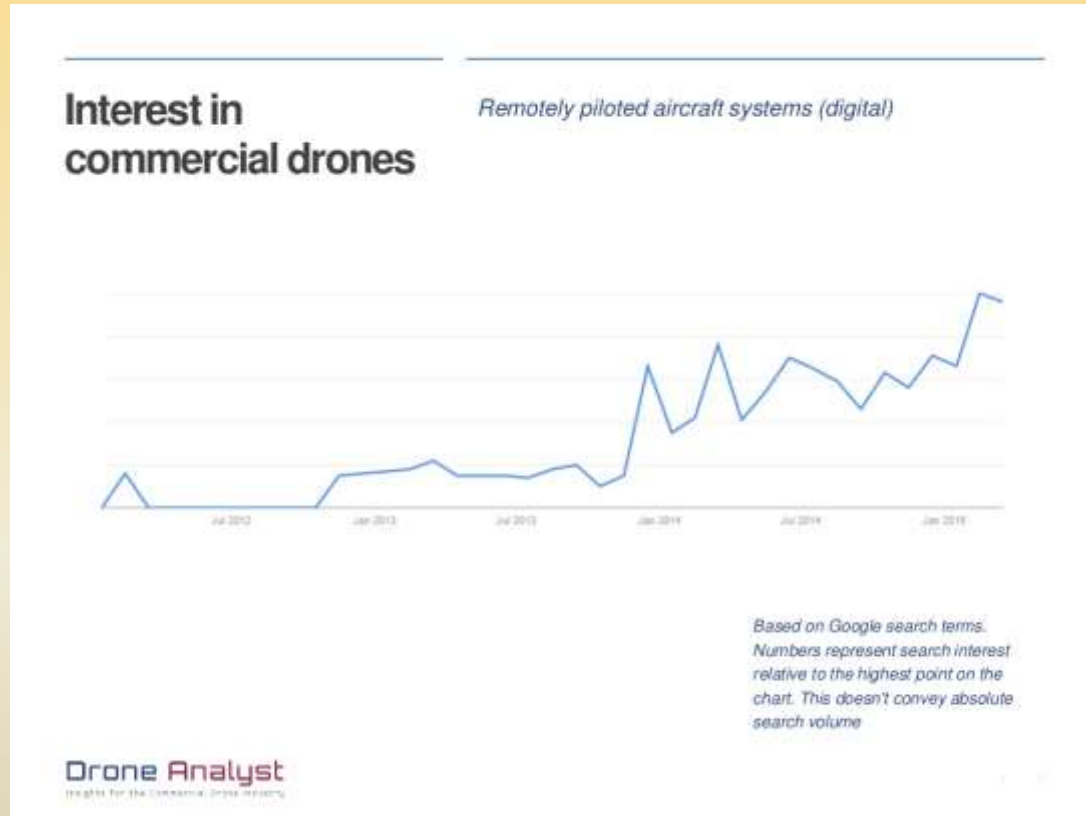
WHAT THE PROPOSAL WOULD ALLOW FOR COMMERCIAL DRONES



FAA Rules & Proposals - Indicators

- ❑ Movement to commercially insure UAVs
- ❑ Some companies already advertising:
- ❑ Transport Risk Management can provide “hull” and liability insurance for all risks of ground and flight:
 - ❑ Multi-rotor UAS / UAV
 - ❑ Fixed Wing UAS / UAV
 - ❑ Single Rotor UAS /UAV
 - ❑ Civilian and Law Enforcement Drone
 - ❑ RPAS

FAA Rules & Proposals - Indicators



- ❑ Increased interest in commercial drones
- ❑ Leads to increased production and sales of commercial drones

FAA Rules & Proposals - Indicators

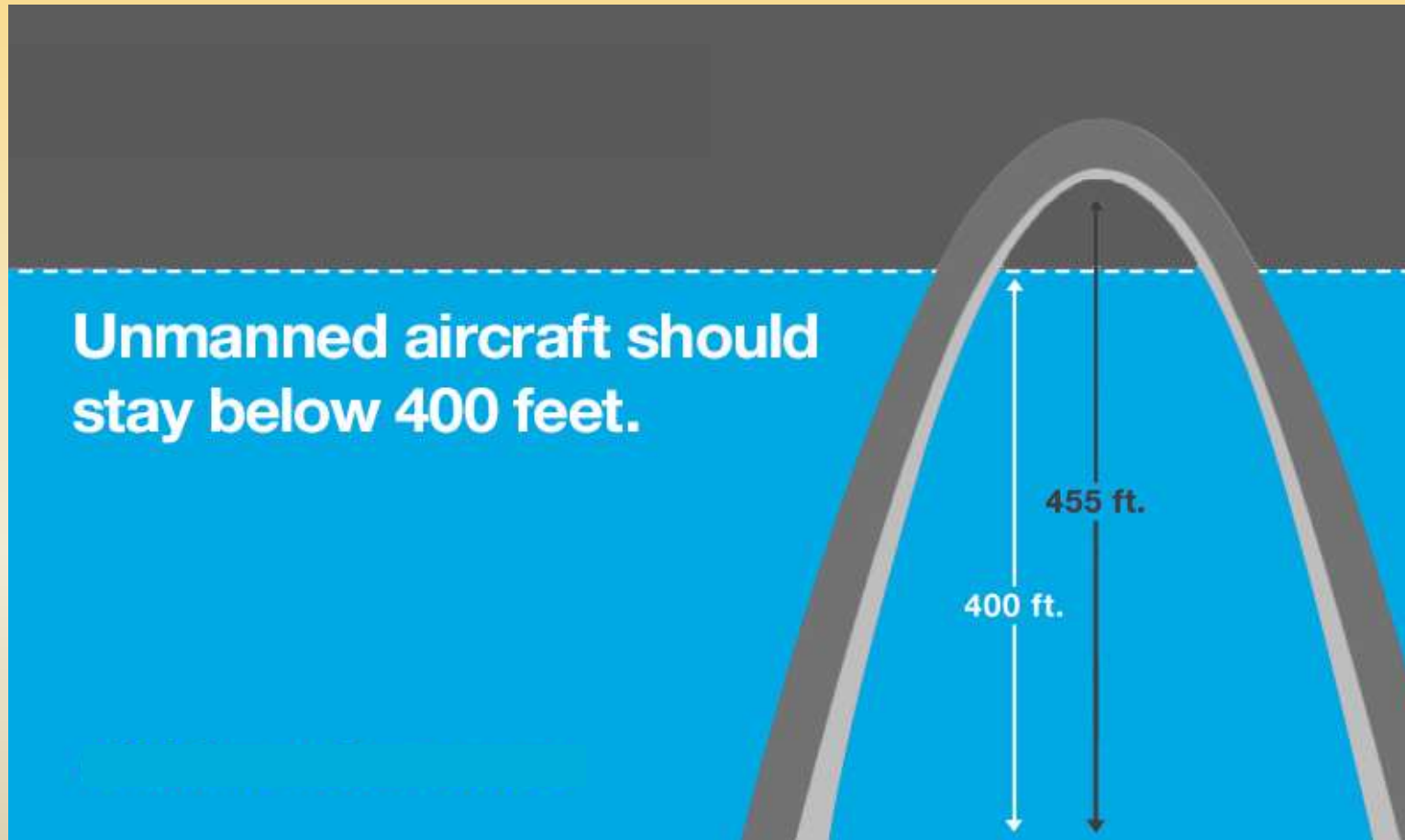
- ❑ **Commercial UAV Platforms & Applications**
 - ❑ Real Estate
 - ❑ Construction
 - ❑ Utilities
 - ❑ Agriculture
 - ❑ Maritime
 - ❑ Railroad
 - ❑ Archaeology
 - ❑ Videography
 - ❑ Media

FAA Rules & Proposals - Indicators

- ❑ Increased sightings of UAS by aircraft pilots
- ❑ FAA expands Unmanned Aircraft Pathfinder efforts to track UAS near airports
- ❑ Denver International Airport and the FAA partner to raise awareness about safe unmanned aircraft operations
- ❑ No Drone Zones for large events/airports
- ❑ Building of UAS testing and development centers for institutions and companies

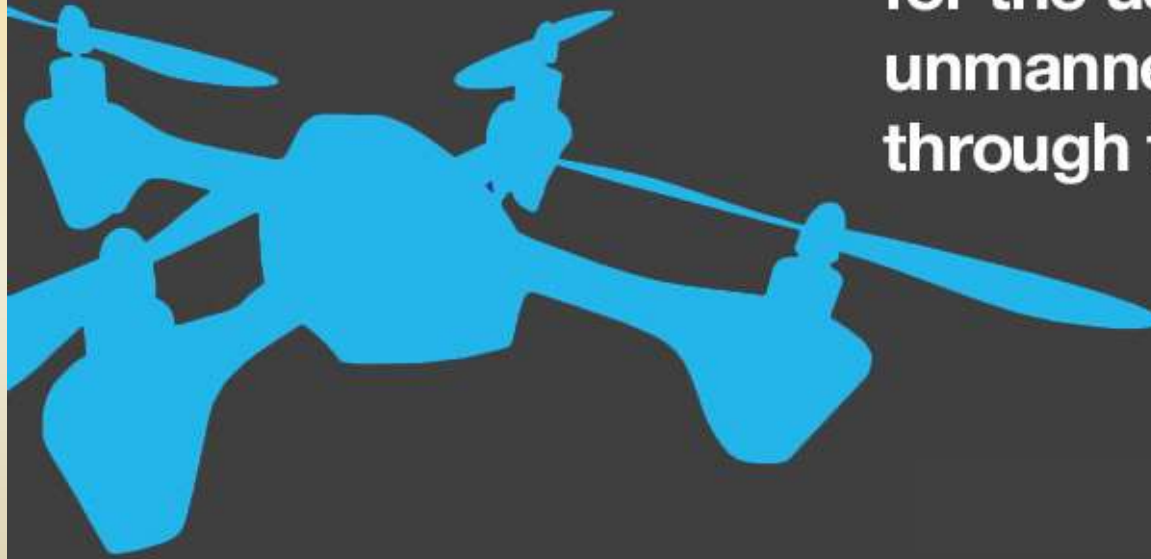


FAA Rules & Proposals - Indicators



FAA Rules & Proposals - Indicators

**Businesses can
request exemptions
for the use of
unmanned aircraft
through the FAA.**



FAA Rules & Proposals - Indicators

- ❑ European Transportation Committee discuss drone safety:
 - ❑ Develop technology to ensure safety and privacy, tackle illegal use
 - ❑ Easing cross-border drone sales and services
 - ❑ Safety rules should match risk levels
- ❑ Increase of testing of drones for public service: ‘City of the future’
- ❑ Pilot sightings of drones doubled between 2014 and 2015, including reports involving incidents at sports events, flights near manned aircraft, and drones that interfered with wildfire operations

FAA Rules & Proposals - Indicators

- ❑ Distinction in regulations between Radio Controlled Aircraft and UAS
 - ❑ Recreational handheld controlled devices vs. semi-autonomous drones
 - ❑ RC hobbyists and self policing
 - ❑ RC not subject to FAA certification



FAA Rules & Proposals - Indicators

- ❑ Satellites and UAVs
 - ❑ The 500-foot ceiling proposed by FAA in Notice of Proposed Rulemaking for commercial operation of sUAS is not upper limit of aerial data-capture capabilities
 - ❑ Many commercial drones capable of operating at altitudes above 500 feet, at suborbital altitudes, above reach of data privacy regulations that might stem from FAA's sUAS rules
 - ❑ Resolution / quality of imagery and data captured by commercial satellites is steadily improving and increasingly in demand

FAA Rules & Proposals - Indicators

- ❑ Satellites and UAVs
 - ❑ Under current regulatory trajectory, a company could be subject to different degrees of data privacy requirements, despite similarity in images / other data collected by satellites and drones
 - ❑ Different government agencies promulgate patchworks of regulatory schemes and guidelines for operation of commercial drones and satellites
 - ❑ Difficult for private citizens and commercial operators to know rights and duties with respect to collection, storage, and dissemination of personal data and images via commercial aerial platforms

FAA Rules & Proposals - Indicators

- ❑ Botlink--application designed to keep users safe and in compliance with FAA regulations while operating drones
 - ❑ With experience with military UAS operations Botlink creators are bringing a high level of expertise to commercial UAS market
 - ❑ The new application enables drone operators to control multicopter or fixed-wing UAS via an easy-to-use interface
 - ❑ Real-time FAA data overlays show locations of manned aircraft along with controlled airspace around airports

FAA Rules & Proposals - Indicators

- ❑ U.S. Senator Charles Schumer to introduce a proposal that aims to make geofencing of drones mandatory soon, following a number of reports of close shaves between the unmanned aircraft and regular planes.
- ❑ The geofencing of drones would use GPS and other technology to impose geographical limits on their movement
- ❑ Manufacturer DJI has already begun testing geofencing technologies so they are a possible regulatory tool

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ UAS must operate safely, efficiently, and compatibly with service providers and other users of the NAS so that overall safety is not degraded
- ❑ UAS will have access to NAS, provided they have appropriate equipage and ability to meet requirements for flying in various classes of airspace
- ❑ Routine UAS operations will not require creation of new special use airspace, or modification of existing special use airspace
- ❑ Except for some special cases, such as sUAS with very limited operational range, all UAS will require design and airworthiness certification to fly civil operations in NAS

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ UAS pilots will require certification, though some of the requirements may differ from manned aviation
- ❑ UAS will comply with ATC instructions, clearances, and procedures when receiving air traffic services
- ❑ UAS pilots (the pilot-in-command) will always have responsibility for unmanned aircraft while it is operating
- ❑ UAS commercial operations will need to apply operational control concept as appropriate for type of operation, but with different functions applicable to UAS operations

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ Aviation insurer Global Aerospace Inc. recommendations for companies interested in using drones and considering a third-party service to operate them
 - ❑ Choose the best system for the job. Define mission for using drone to narrow search from among an estimated 800 small drone manufacturers in the world. That includes determining whether the operator will supply raw or processed data.
 - ❑ Choose a safe operating system. Legislation does not differentiate between drone operating with a 3-pound foam wing and a 25-pound unit. The latter is going to need a more active risk mitigation plan because of the dangers from the higher weight.

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ Maintain a safe distance. Although FAA requires flights to be at least 500 feet from all people, drones need to be closer than that for many purposes. If that's the case brief everyone in that area about the operation.
- ❑ Have a qualified drone pilot with the necessary training and certification for the job and one who meets all of the insurer's requirements.
- ❑ Manage risk. Geofencing technology, which sets virtual boundaries around actual places and prevents the drone from wandering where it should not be.

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ Require routine drone maintenance from third-party operators
- ❑ Require insurance. The drone operator should have liability limits of \$1 million to \$5 million per occurrence
- ❑ Carry non-owned insurance. This provides coverage for any third-party damage caused by the drone operator.

FAA Rules & Proposals – Indicators

Industry Policy Recommendations

- ❑ What needs to happen for future of drone growth to take off?
 - ❑ Increasing levels of certification oversight - FAA must remain committed to development of technical and regulatory standards, policy guidance, and operations procedures
 - ❑ Government-industry collaboration is paramount to success and must focus on process, quality, and timely results
 - ❑ FAA expects to gain experience in applying existing airworthiness regulations during type certification process with early UAS adopters

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- What needs to happen for the future of drone growth?
 - Reduced operating limitation/restriction – Regulation has been the main barrier to drone adoption and operational flexibility
 - FAA asserts there is much progress to be made increasing access for UAS without severely comprising safety or privacy
 - FAA has placed high priority on development of rules for sUAS that will increase access to NAS and provide an initial opportunity for commercial operations

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

- ❑ Electronic Frontier Foundation recommends that FAA:
 - ❑ Develop and provide a model privacy policy for test site operators
 - ❑ Add additional types of privacy-specific data to its data collection and reporting requirements
 - ❑ Require test site operators to conduct privacy-specific tests
 - ❑ Incorporate privacy protections developed through FAA's test site program throughout FAA's unmanned aircraft authorization process
 - ❑ Make drone flight data available and easily accessible to public

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

Recommendations to FAA

1. Acknowledge that the current regulatory void has left businesses either sitting on the sidelines or operating in the absence of appropriate safety guidelines.

2. Concede that the recreational community has proven that community-based safety programming is effective in managing a growing level of activity.

3. Grant the April 9, 2014, request by the AUVSI and AMA and the 31 other organizations to expedite the rulemaking process for UAS operations in the U.S. airspace and allow the limited use of small UAS for commercial purposes before the final rulemaking is completed.

4. Make good on the February 6, 2007, Policy Statement advisory pledge here to:

"... [create] a different category of unmanned vehicles that may be defined by the operator's visual line of sight and are also small and slow enough to adequately mitigate hazards to other aircraft and persons on the ground."

5. Abide by the Regulatory Flexibility Act and balance the safety goals of regulations with the needs and capabilities of small businesses and other small entities providing sUAS services

FAA Rules & Proposals - Indicators

Industry Policy Recommendations

Recommendations to manufacturers and operators

1. Educate yourself. *As this study shows, too many business owners and operators do not understand current rules or advisories. See my website for links to the most relevant ones.*

2. Regulate yourself. *Start by adopting standards for your aircraft and users. A good place to start is with the seven standards released by ASTM International Committee F38 on Unmanned Aircraft Systems.*

3. Collaborate. *Form a working relationship with the organizations that have already put in place operational guidelines such as AMA, RCAPA, and PARCAP.*

4. Find your public voice. *Actively examine and then voice your opinion when an FAA notice of proposed rulemaking (NPRM) about UAS is made public.*

Also, don't assume that AUVSI is speaking on your behalf and in your favor even though it may seem so.

5. Buy insurance. *There are aviation insurance contracts which have no Federal Aviation Regulation (FAR) exclusions.*

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ Drones are the future of the Internet of Things (IoT)
- ❑ IoT applications are typically composed of:
 - ❑ A sensor “at rest,” e.g., on a highway or a bridge or a thermostat that gathers input (like weather conditions or seismic activity)
 - ❑ A connection (via the Internet) between the sensor and a back-end data collection infrastructure
 - ❑ A back-end data collection infrastructure that’s commonly based in the cloud

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ Drone technology is evolving very rapidly
- ❑ Drones are already beginning to efficiently replace connected sensors at rest with one device that is:
 - ❑ deployable to different locations
 - ❑ capable of carrying flexible payloads
 - ❑ re-programmable in mission
 - ❑ able to measure just about anything, anywhere

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ Airspace access has regulatory and technological issues
- ❑ Issues need addressed before UAS are authorized for unrestricted access to NAS
 - ❑ Lack of prescriptive standards and regulations governing routine operation of UAS in NAS
 - ❑ Collaboration of air traffic controllers with UAS operators has to be defined
 - ❑ Automated separation assurance algorithms for seamless and safe operation of UAS in high density environments

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ Regulations needed for certification of UAS operators and maintenance activities
 - ❑ Secure and reliable communications have to be established between control and UAS with minimum performance standards
 - ❑ Reliability and airworthiness regulations
 - ❑ Stringent development process for hardware and software, reliability analysis, failure mode and effect analysis, risk classification
 - ❑ Redundancy in hardware and software
 - ❑ Dissimilarity and installation integration segregation of critical components

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ Regulatory standards no less demanding than manned systems nor more demanding because technology permits
- ❑ Develop reliable algorithms for fault detection and isolation using analytical redundancy combined with algorithms that make it possible to control vehicle in faulty situations, to be able to terminate or recover vehicle without an accident and stop harm
- ❑ Need for sense and avoid systems on UAVs in NAS

FAA Rules & Proposals - Judgments

UAS Future Challenges

- ❑ High level of autonomy to take advantage of UAV platform
- ❑ Ability for one person to monitor many UAVs
- ❑ Longer durability and robustness to weather conditions and turbulence
- ❑ One major concern is that the reams of video collected by UAS could be used against private citizens
- ❑ There needs to be an effort to make sure UAS protect basic human rights and not infringe upon them

FAA Rules & Proposals - Judgments

Existing Regulations and Standards

- ❑ Impossibility of obtaining type certificate and consequently certificate of airworthiness
- ❑ FAA has experimental certificates
- ❑ Safety as paramount objective:
 - ❑ Type certification of specific model of aircraft usually granted due to development by certified design organization which by its quality assurance process the appropriate design to applicable certification
 - ❑ Airworthiness / maintenance of specific units granted by manufacture of type certified aircraft in certified production organization
 - ❑ Safety of each flight ensured by airworthiness of aircraft, skills of certified pilots which are considered last resorts

FAA Rules & Proposals - Judgments

- ❑ UAVs need:
 - ❑ Air Traffic Control System
 - ❑ Identification and Location Broadcast System
 - ❑ Mapping System
 - ❑ Sense and Avoid (SAA)
 - ❑ Flight Plans

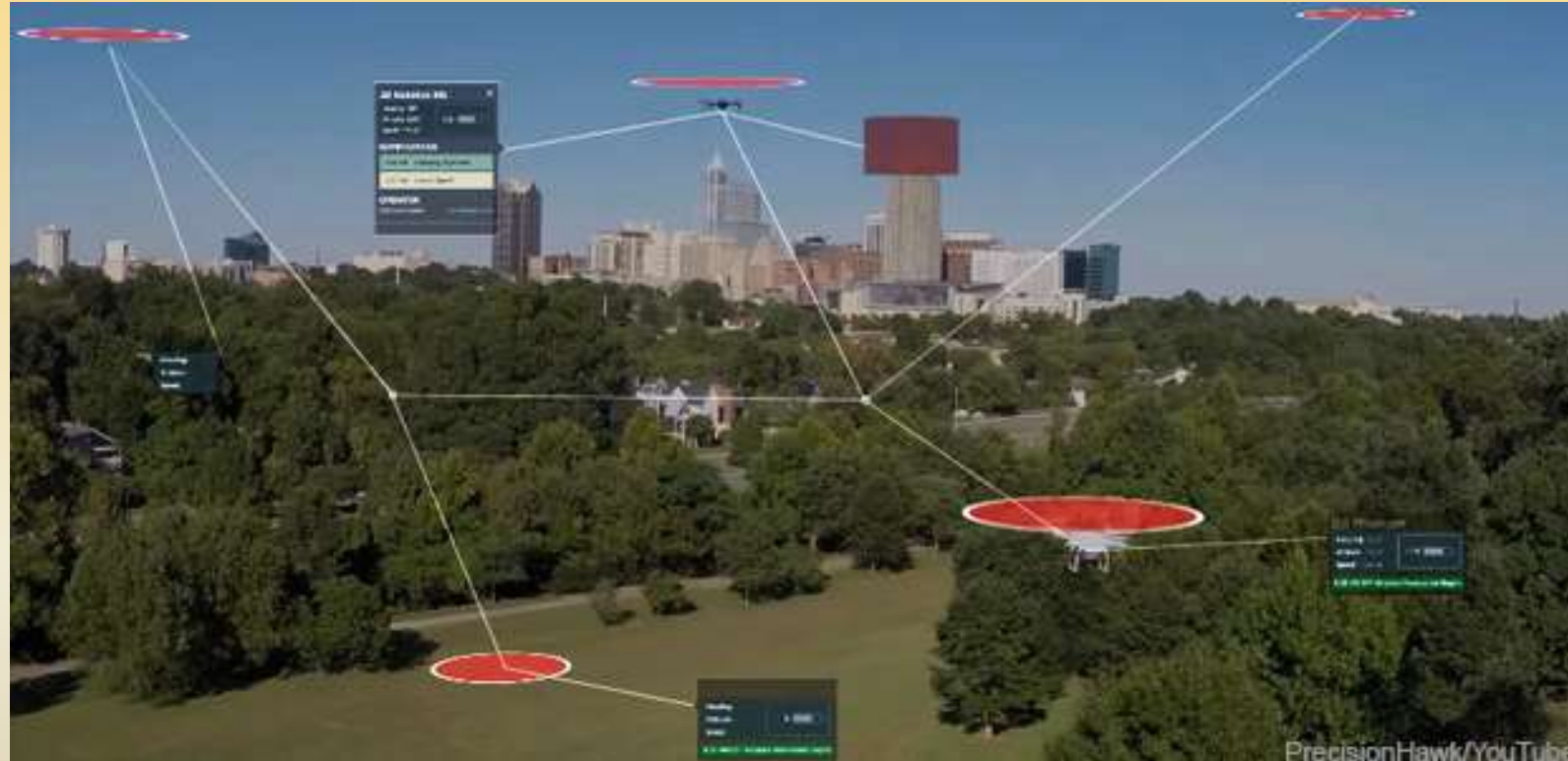
FAA Rules & Proposals - Judgments

Air Traffic Control System

- ❑ PrecisionHawk, a terrestrial data acquisition and analysis company, tests Low Altitude Traffic and Airspace Safety platform (LATAS) an air traffic control system for UAS
- ❑ Using LTE and satellites, LATAS connects airspace safety technologies such as:
 - ❑ Detect and avoid
 - ❑ Dynamic geo-fencing
 - ❑ Aircraft tracking

FAA Rules & Proposals - Judgments

LATAS
Air
Traffic
Control
System



FAA Rules & Proposals - Judgments

- Google has proposed that drones employ ADS-B, an **Identification and Location Broadcast System** used on existing aircraft

What is it?

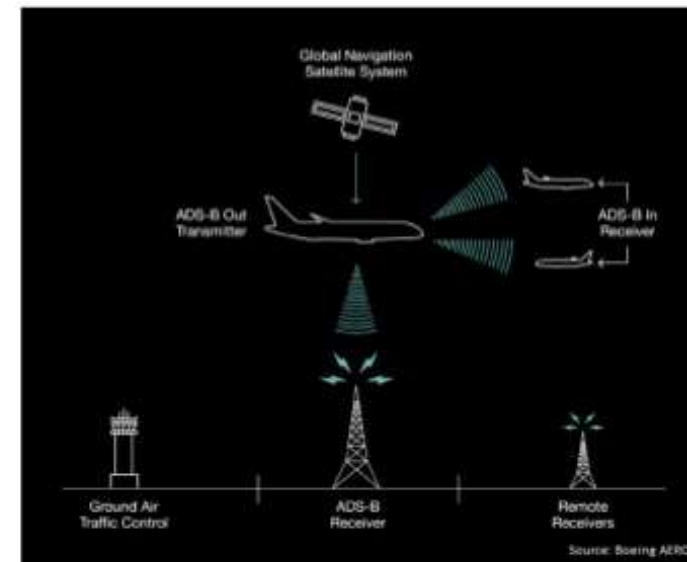
Automatic: it works in the background

Dependent: depends on other aircraft being equipped

Surveillance: it's a technology to track aircraft

Broadcast: each aircraft broadcasts its position and velocity

Automatic Dependent Surveillance – Broadcast (ADS-B)



FAA Rules & Proposals - Judgments

Sense and Avoid

- Detect and avoid
 - Mid-air collisions with other flying traffic according to the right-of-way rules
 - Terrain and other obstacles
 - Hazardous weather
 - Perform functions and maintain separation, spacing and sequencing, as done by manned aviation

FAA Rules & Proposals - Judgments

Sense and Avoid

- ❑ SAA requirements
 - ❑ Detection range of hazardous objects
 - ❑ Minimum miss distance
 - ❑ Field of regard, right-of-way
 - ❑ Measurement accuracy, reliability, update rate
 - ❑ Avoidance maneuver

FAA Rules & Proposals - Judgments

Sense and Avoid

- SAA design
 - Detect
 - Track
 - Evaluate
 - Prioritize
 - Declare
 - Determine action
 - Command

FAA Rules & Proposals - Judgments

Sense and Avoid

- SAA requirements function of type of communications relay
 - Beyond line of site communications
 - Direct radio frequency communications
 - Terrestrial networks
 - Satellite communication

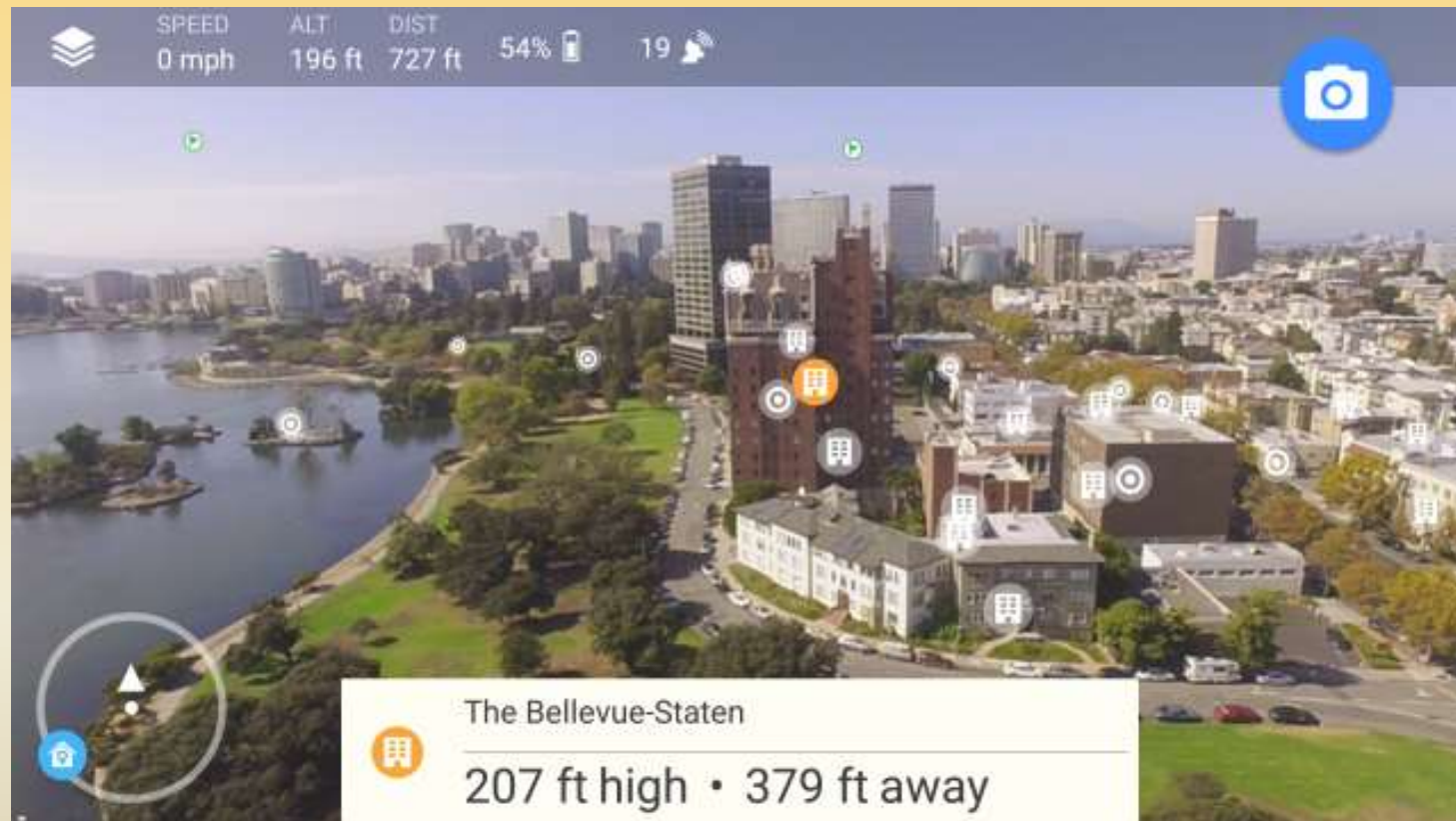
FAA Rules & Proposals - Judgments

Mapping System

- ❑ Hivemapper
 - ❑ Mapping program that turns a smartphone into an augmented-reality viewfinder when it is paired with a DJI drone
 - ❑ Gives information on where drone owners can fly
 - ❑ The app also shows users when they're getting too close to a building and alerts them to change course
 - ❑ Hivemapper users will be able to add new information to the map

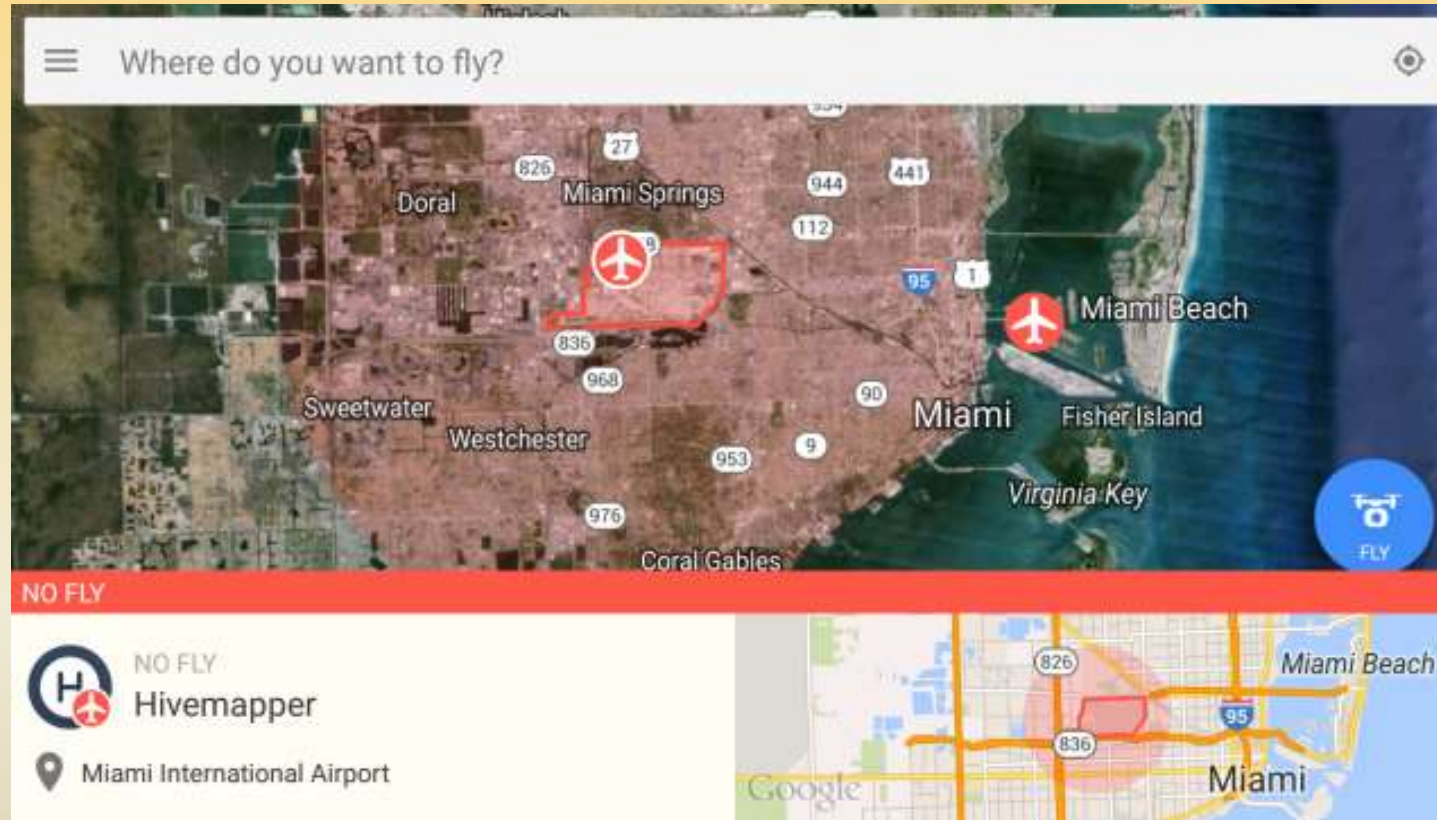
FAA Rules & Proposals - Judgments

- Mapping System:
Hivemapper interface



FAA Rules & Proposals - Judgments

- Mapping System:
Hivemapper
interface



FAA Rules & Proposals - Judgments

Flight Plans

- ❑ Distributed Drone Flight Path Builder System
 - ❑ Novel approach to flexibly divide a large area into sub regions
 - ❑ Dynamically adjust them to optimally cover with single drone flight
 - ❑ Combines spatial data and drone limitations or constraints modeled as linear inequalities to automate flight path of drones
 - ❑ The distributed implementation presents way to handle large datasets

FAA Rules & Proposals - Judgments

Flight Plans

- The sub region level distribution allows horizontal scalability
- The technique is useful for a host of drone applications
- Real-Time Visual-Inertial Mapping, Re-localization and Planning Onboard UAVs in Unknown Environments

FAA Rules & Proposals - Judgments

Flight Plans

- ❑ Tools help with Aeronautical Decision Making and Crew Resource Management
 - ❑ Gathering of information and analyzing to make decisions regarding drone flight and plans
 - ❑ Records of past flights or basic drone flight plan outlines helps pilots be more informed and make better decisions about flights
 - ❑ Mitigates hazardous attitudes
 - ❑ For good Aeronautical Decision Making it is recommended to keep a detailed flight plan to learn from past mistakes or refresh on a course of action

FAA Rules & Proposals - Judgments

Flight Plans:
Flight Log

FN	Flight Date	Location	AirFit	(FW/RW/SRW)	Camera	LOS/FPV	BATT#	Day/Night	FD	Notes/Lessons Learned
1								● ●		
2								● ●		
3								● ●		
4								● ●		
5								● ●		
6								● ●		
7								● ●		
8								● ●		
9								● ●		
10								● ●		
11								● ●		
12								● ●		

FW: Fixed Wing / RW: Rotary Wing / SIM: Simulator
FN: Flight Number / Logbook Legend / FD: Flight Duration
AirFit: Airframe Number
LOS: Line of Sight / FPV: First Person View


Example for
Aeronautical
Decision
Making

FAA Rules & Proposals - Recommendations

- ❑ **Certificates** – Use of experimental certificates and exemptions to temporary regulations will not give FAA power to regulate the UAS market. Certifications for private citizens, companies and institutions need to be clearly defined for use of UAS
- ❑ **Insurance** -- Use of liability coverage necessary, some companies already advertising for coverage on many types of sUAS with full coverage on damage to the sUAS
- ❑ **Tracking system** -- Using air traffic control systems and location broadcasting systems UAS need to be accounted for and be visible to all other aircraft manned or unmanned

FAA Rules & Proposals - Recommendations

- ❑ **Geofencing** – Systems using GPS and mapping systems that set virtual boundaries around actual places, impose geographical limits on their movement and prevent UAS from going into undesignated airspace
- ❑ **Training** -- Eight hours of voluntary training to certify UAS pilots for all sUAS, can be online videos or simulations run by commercial and / or FAA entities or classes hosted by FAA certified instructors
- ❑ **Registration** – Needs to be voluntary with no fees or fines or else there will be no way to enforce registration with such widespread growth of the UAS market
- ❑ **Sense and Avoid** – Detect and Avoid and communication systems needed for all UAS military, private or commercial



National Critical Intelligence
Estimate: Cyber Terrorism /
Counter Terrorism Implications
of UAS

Cyber Terrorism / Counter Terrorism Implications - Facts

- Black Swan Events
 - A metaphor describing an event that
 - comes as a surprise
 - has a major effect
 - often inappropriately rationalized after the fact with the benefit of hindsight

Cyber Terrorism / Counter Terrorism Implications - Facts

Black Swan Events

- ❑ 1964: Personal Computer
- ❑ 1969 29 Oct: Internet
- ❑ 1973: Global Positioning System (GPS)
- ❑ 2001 11 Sept: Flights 11 and 175 WTC, NYC
Flight 77 Pentagon, Washington DC
Flight 93 Somerset County Pennsylvania
- ❑ 2011 04 Dec: Iran-US RQ-170 Sentinel incident
- ❑ 2014 10 Jun: FAA Approves First Commercial UAS Flights over Land

Cyber Terrorism / Counter Terrorism Implications - Facts

- ❑ Soliciting industry stakeholders
 - ❑ Participate in a new ASISP Working Group
 - ❑ Established December 18, 2014
 - ❑ Deliver recommendations to the ARAC
- ❑ Federal regulations do not specifically define how the FAA should address cybersecurity vulnerabilities for aircraft operating in the U.S. National Airspace System.

Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- ❑ Office of Homeland Security
 - ❑ Implement the Homeland Security Advisory System
 - ❑ Identify and assure protection of critical infrastructures
 - ❑ Provide timely warning system
 - ❑ Coordinate collaborating among federal, state, and local governments and the private sector

Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- ❑ Eight Guiding Principles
 - ❑ Safeguard privacy and constitutional freedoms
 - ❑ Develop technologies and expertise to combat terrorist threats
 - ❑ Assure public safety, public confidence, and services
 - ❑ Establish responsibility and accountability

Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- ❑ Eight Guiding Principles
 - ❑ Encourage and facilitate partnering among all levels of government and between government and industry
 - ❑ Encourage market solutions wherever possible
 - ❑ Facilitate meaningful information sharing
 - ❑ Foster international cooperation

Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- Secure Critical Infrastructures
 - Unmanned Aerial Systems
 - Water
 - Dams
 - Energy
 - Nuclear Power Plants
 - Chemical Industry and Hazardous Materials

Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- Secure Critical Infrastructures
 - Public Health
 - Telecommunications
 - Government Facilities
 - Defense Industrial Base
 - Commercial Key Assets

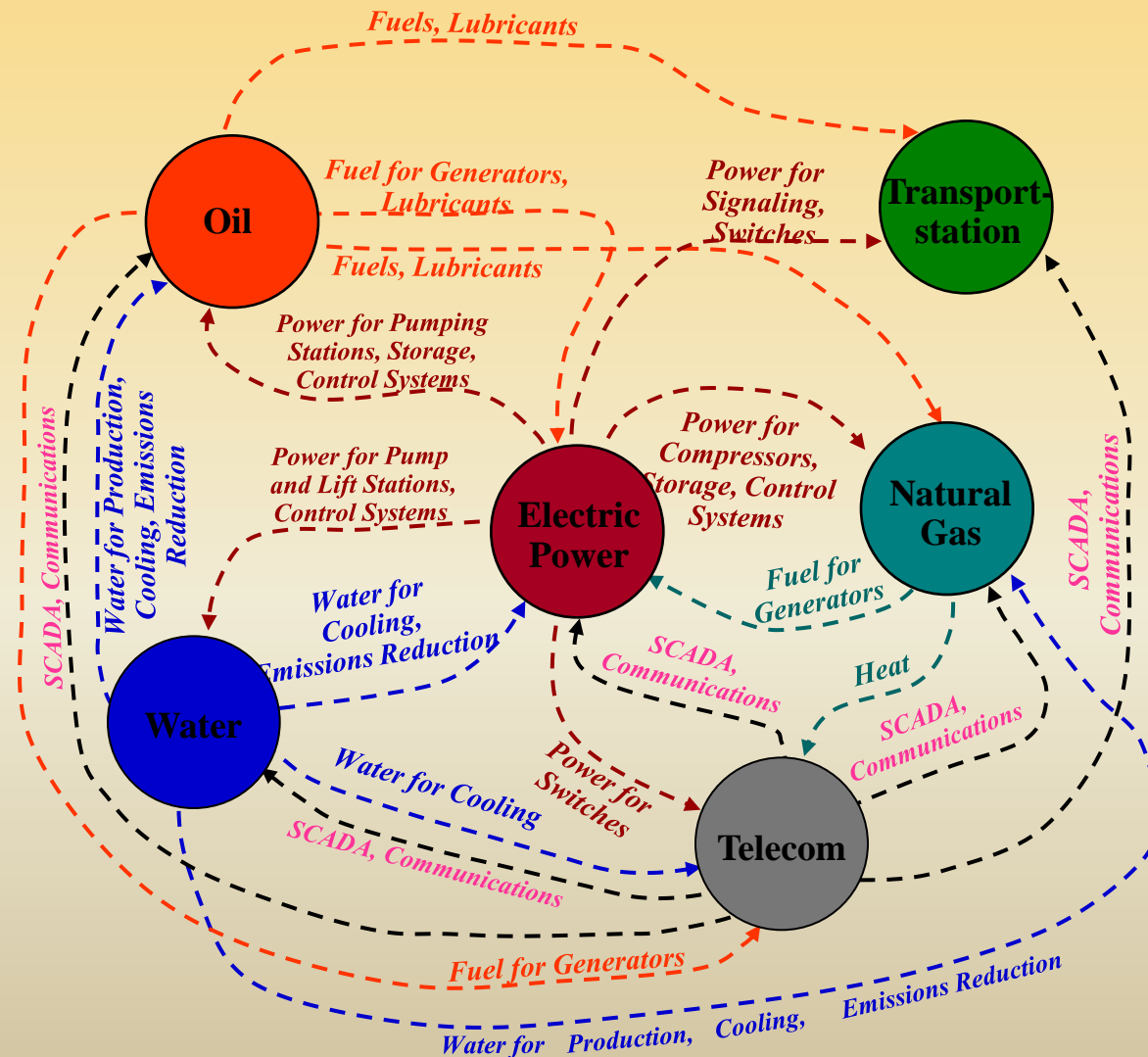
Cyber Terrorism / Counter Terrorism Implications - Facts

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets

- Secure Critical Infrastructures
 - Transportation
 - Postal and Shipping
 - National Monuments and Icons
 - Agriculture
 - Banking and Finance

Cyber Terrorism / Counter Terrorism Implications of UAS - Facts

SCADA & Infrastructure Interdependencies



Cyber Terrorism / Counter Terrorism Implications - Facts

- ❑ The National Infrastructure Protection Plan
 - ❑ Partnering for Critical Infrastructure Security and Resilience
 - ❑ Critical Infrastructure Risk Management (CIRM) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.
 - ❑ CIRM can be tailored toward and applied on an asset, system, network, or functional basis, depending on the fundamental characteristics of the decisions it is intended to support and the nature of the related infrastructure.
 - ❑ CIRM complements and supports the Threat and Hazard Identification and Risk Assessment (THIRA) process conducted by regional, State, and urban area jurisdictions.

Cyber Terrorism / Counter Terrorism Implications - Facts

- ❑ City of Chicago Information Security Office (ISO)
 - ❑ Oversees cybersecurity across all areas of the city
 - ❑ Critical infrastructure
 - ❑ Water Department supplies fresh water to over 44% of Illinois residents
 - ❑ Aviation Department manages Chicago O'Hare and Midway airports
 - ❑ Public Safety Department
 - ❑ Security Information Event Management – SIEM Software
 - ❑ Logs and manages over 10,000 events per second
 - ❑ Event growth expected to double by the end of 2014

Cyber Terrorism / Counter Terrorism Implications - Facts

Information Security Office Shared Services

- ❑ Critical Application Access Recertification (CAAR)
Perform ad-hoc and quarterly review of access rights to ensure proper governance and control.
- ❑ Firewall Change Review (FCR)
Provide secondary approval and segregation of duties (SoD) to firewall change request process.
- ❑ Firewall Recertification (FR)
Perform ad-hoc and quarterly review of rules and configuration to ensure proper governance and control.
- ❑ Incident Response (IR)
Identify, respond and remediate suspicious or malicious cyber activity.

Cyber Terrorism / Counter Terrorism Implications - Facts

Information Security Office Shared Services

- ❑ Policy and Governance (POL)
Build and maintain the City's Information Security policy set which governs direction and minimum technical requirements
- ❑ Network Security Monitoring (NSM)
Monitor and Respond to suspicious and malicious network based traffic.
- ❑ Perimeter Security (PS)
Validate technical security controls through active testing (aka white hat hacking).
- ❑ Enterprise Risk Assessment and Reporting (RISK)
Regularly assess the City's current risk posture against targeted risk posture.
Provide real-time feedback on existing, mitigated and accepted risks.

Cyber Terrorism / Counter Terrorism Implications - Facts

Information Security Office Shared Services

- ❑ Enterprise Risk Assessment and Reporting (RISK)
Regularly assess the City's current risk posture against targeted risk posture.
Provide real-time feedback on existing, mitigated and accepted risks.
- ❑ Security Architecture Review (SAR)
Review RFPs and partner with Project and Technical teams to review proposed solutions to ensure alignment to Policies and Best Practices.
- ❑ Security Awareness and Training (SAT)
Provide security specific awareness and education training to user and technical community.
- ❑ Threat and Vulnerability Management (TVM)
Constant monitoring and communication of cyber threat landscape and evaluation of internal technical readiness.

Cyber Terrorism / Counter Terrorism Implications - Facts

Florida Center for Cybersecurity
at the University of South Florida

Cyber Threats

- ❑ System and Environmental Failures – single point of failure (SPOF); lack of failure/safety prevention; lack of reliability assurance
- ❑ Violent Acts of Man – terrorist attack; hostage situation; warfare
- ❑ Errors and Omissions – negligent acts; unintentional or intentional exclusions; failure to act; failure to act without error or mistake; wrong conduct or wrong judgment

Cyber Terrorism / Counter Terrorism Implications - Facts

Florida Center for Cybersecurity
at the University of South Florida

Cyber Threats

- ❑ Insider Attack – malicious attack on a system, computer or network conducted by a member of the organization with authorized system access
- ❑ Insider Abuse and Unauthorized Acts – insecure or harmful acts and conduct of a member of the organization with authorized system access
- ❑ External Attack -- malicious attack on a system, computer or network conducted by a person or entity external to the organization who does not have authorized system access

Cyber Terrorism / Counter Terrorism Implications - Facts

Florida Center for Cybersecurity
at the University of South Florida

Cyber Threats

- ❑ Acts of Nature – Natural Disaster – earthquake, hurricane, storms, fire
- ❑ Hazardous Conditions – Improper Configuration; Maintenance Issues; Chemical/HAZMAT
- ❑ Dependency Failures – Service failures – e.g., improper inheritance, check execution or notifications failure, improper services or host dependency configuration; invalid time period

Cyber Terrorism / Counter Terrorism Implications - Facts

Florida Center for Cybersecurity
at the University of South Florida

Cyber Threats

- ❑ Autonomous Systems and Malicious Code – exploitation of the routing policy of a network; code injection, scripts, executables, or any other code intended to cause undesired affects, security breaches or system damage
- ❑ Physical Intrusion and/or Theft – successful attempt to gain unauthorized physical access; successful attempt to access, remove, destroy, or modify an asset
- ❑ Legal and Administrative Action – action or decisions made by a system stakeholder, employee or agent, often of a legal nature and sometimes resulting in legal consequences

Cyber Terrorism / Counter Terrorism Implications - Facts

Subject Matter Experts (SME)

- ❑ **Nichols:** **Terrorism – The Mutating Threat**
- ❑ **Ryan:** **INFOSEC by Design**
- ❑ **Nestler:** **Drones and Cybersecurity**
- ❑ **Hathaway:** **5 W's of U.S. Cybersecurity**
- ❑ **Spafford:** **Cybersecurity in Crisis – 9 F's**
- ❑ **Parker:** **Traditional / Modern INFOSEC**
- ❑ **Mumm:** **Managing the Integration and Harmonization of the NAS for UAS**

Nichols: Terrorism – The Mutating Threat

- ❑ The idea of Terrorism as chrysalis –embracing violent jihad to transform society is not new
- ❑ Jihadist ideology is not synonymous with Islam, however, it is hard to separate the two. Jihadists attract naïve acolytes, confuse opponents & constrain counter-terrorism efforts, which might be interpreted as assaults upon the religion itself.
- ❑ Jihadists goals are not: autonomy, independence, revolution, control of the reins of government or political reform
- ❑ Jihadism is more than a military doctrine: It is about conversion & personal salvation of society
- ❑ Broad goals achievable only through perpetual war & incitement

Nichols: Terrorism – The Mutating Threat

- ❑ al-Qaeda is the most famous modern Jihadist terrorist group. War has formally been declared on U.S. twice: MB in 1991 & UBL in his 1996 Fatwa
- ❑ Global in nature, well financed, they communicate more than any other previous terrorist group in history
- ❑ No previous clandestine leaders have issued so many videos, audio tapes, backed up by a vast array of local leader statements; recruiting materials, field manuals, memoirs & recorded testaments of suicide bombers
- ❑ Jihadists exploit the latest communications technologies
- ❑ The rise of al-Qaeda coincides with the spread of the Internet
- ❑ Communications are direct, unmediated, unfettered, & have established a virtual terrorist community without intervening & vulnerable hierarchy

Nichols: Terrorism – The Mutating Threat

- ❑ Innovation is the watchword for al-Qaeda
- ❑ Ideology is founded in religion
- ❑ Emphasis is on radicalization
- ❑ Communications are voluminous, assessable & effective
- ❑ Organization is distributed & flat
- ❑ Notions of violence & pursuit of slaughter as a means of personal transformation
- ❑ Campaign is globally waged & financed
- ❑ Innocents are denied (targeting of fellow Muslims) & seen as collateral damage
- ❑ Organized quest to obtain / manufacture / use WMDs
- ❑ Lack of capability, not lack of will, is the principal barrier to escalation

Nichols: Terrorism – The Mutating Threat

- ❑ Tomorrow's Terrorism is chrysalis & surprise
- ❑ Armed conflicts in Afghanistan & Iraq will continue into the future [regardless of the political leadership or rhetoric in America.] History is instructive: previous insurgencies & guerrilla wars are measured in decades
- ❑ al-Qaeda, despite setbacks, decentralized & disrupted leadership, will remain the dominant threat for the future
- ❑ The Jihadist enterprise has yet to run its course. UBL as a personal role model is less critical dead or alive
- ❑ The process of radicalization will continue. Internet recruitment will flourish
- ❑ Jihadists are becoming most proficient in their craft of violence & in their communications – especially online distance learning & PR

Nichols: Terrorism – The Mutating Threat

- ❑ TARGETS: terrorists have seldom successfully attacked CIS. Targets include: bridges, tunnels, ports, power plants, electrical grids, waterworks, refineries
- ❑ These tend to be large, inherently robust facilities & complex networks difficult to destroy
- ❑ Attacking CIS requires multipart operations, simultaneous attacks & continuous campaign
- ❑ al-Qaeda prefers symbolic targets or concentrations of people that guarantee high body counts & lots of PR coverage. The quest still is for a 911 event with primary, secondary & tertiary effects
- ❑ Because of the Internet, constraints limiting terrorist violence have eroded

Nichols: Terrorism – The Mutating Threat

- ❑ Warfare is changing
- ❑ Technology & the development of terrorist tactics are putting increasingly destructive power in the hands of smaller groups
- ❑ USA fields the most powerful military forces in the world
- ❑ But conventional military strategies are limited when USA is *losing the PR war*
- ❑ Asymmetrical thinking necessary to defeat the message & present adaptive counterinsurgency doctrines to be effective
- ❑ Warfare against al-Qaeda is a game of Information Superiority

Nichols: Terrorism – The Mutating Threat

- ❑ **INFORMATION RESPONSE:** Terrorists & their supporters are using the media – especially the internet for propaganda, global fund raising, recruiting & indoctrination; secure communications, strategy, operational plans, test runs, information collection & logistics.
- ❑ For the CT specialist, the internet is a low cost form of monitoring terrorist mind-set, understanding ideological & operational activities
- ❑ Of the jihad websites, only a dozen websites are directly linked to al-Qaeda & its associated groups
- ❑ Key decision makers that conceptualize, formulate & direct global jihad strategy are only a handful of individuals
- ❑ These few should be our main targets for the U.S. counter-terrorism mission

Ryan: What can you do with Encryption?

- Protection
 - Systems to keep information assets safe from disclosure, misuse or destruction
 - Adding Security features PRE not Post Design!

- Detection
 - Systems that recognize vulnerabilities and penetrations

- Correction
 - Response teams for network emergencies
 - Re-engineering to patch/correct vulnerabilities penetration

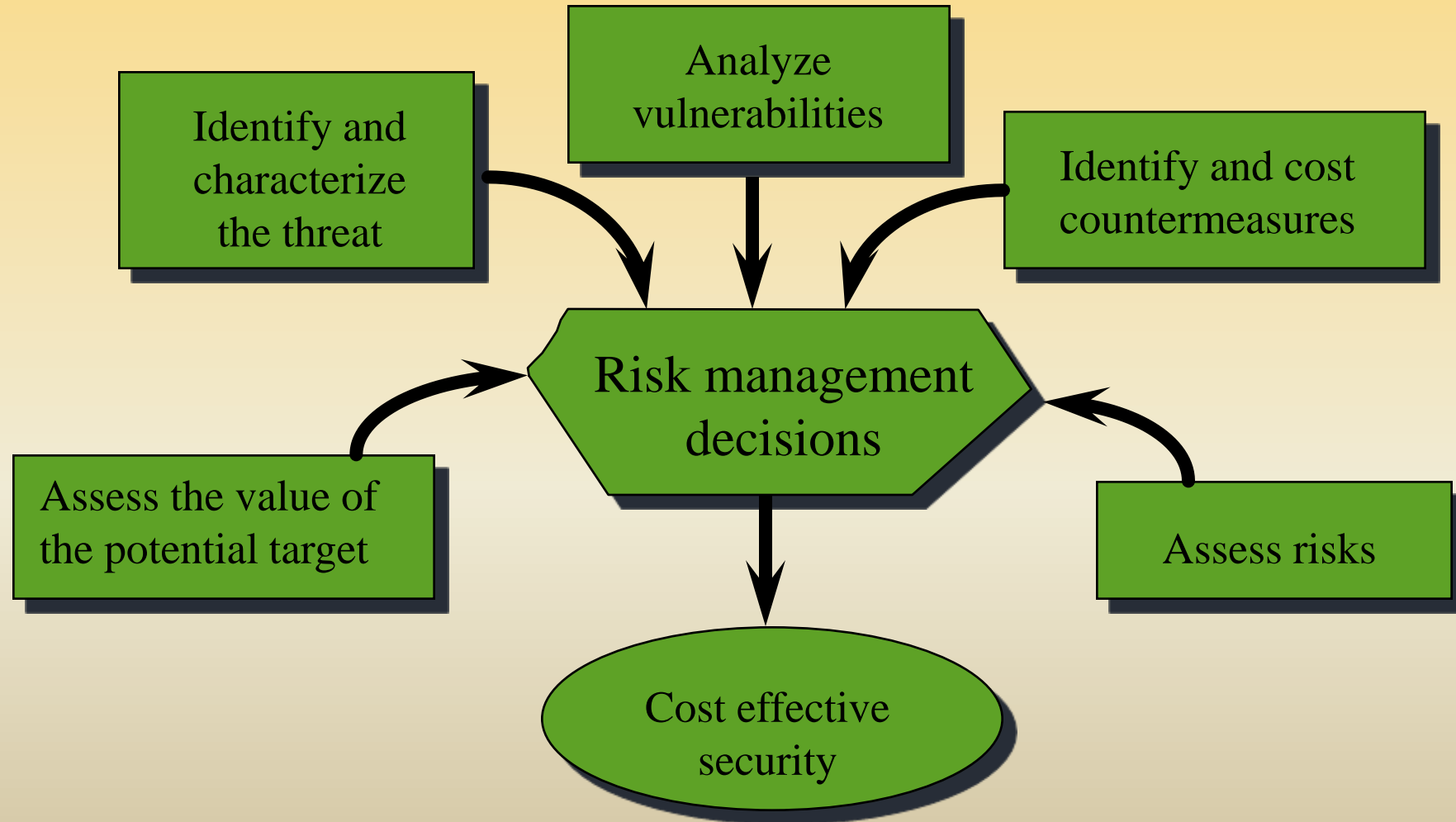
Ryan: What can you do with Encryption?

- ❑ Risk = Threats x Vulnerabilities x Impact
Countermeasures
- ❑ Threats: virus, worms, DNS attacks, Malware, etc. REAL
- ❑ Vulnerabilities: characteristic of the network or operating system, software allowing access

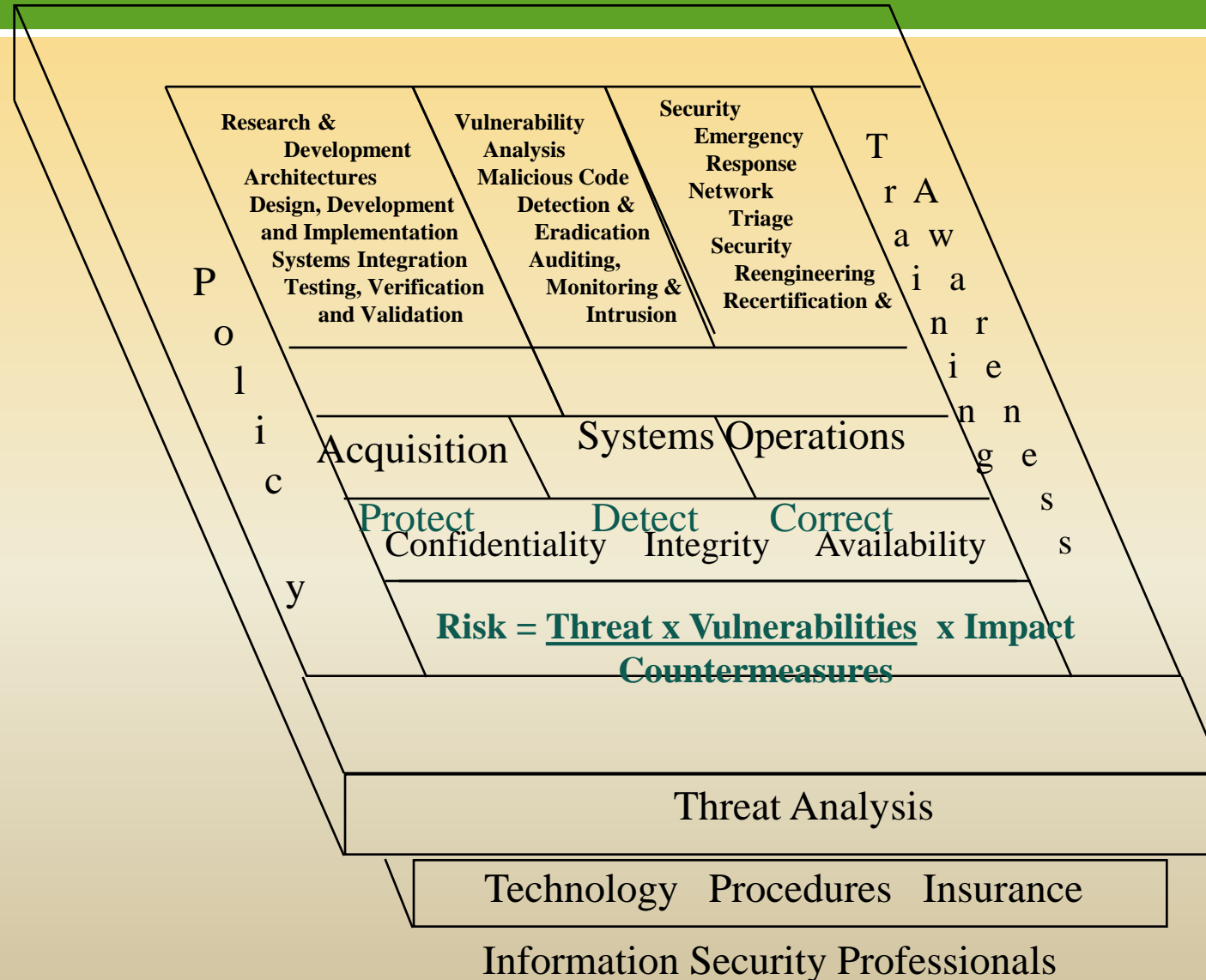
- ❑ Impact: value of the loss of information

- ❑ Countermeasures: Elements of protection, detection and correction
- ❑ Use an integrated approach to mitigate risk

Ryan: The Risk Management Process



Ryan: What can you do with Encryption?



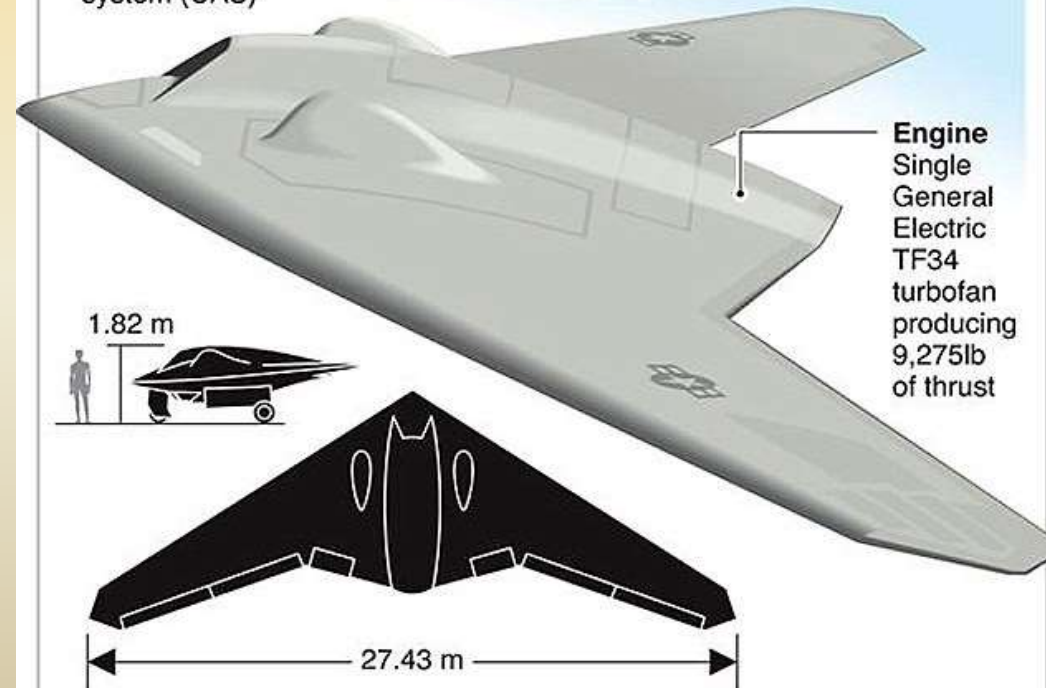
Nestler: Drones and Cybersecurity

Used in the bin Laden raid

U.S. RQ-170 SENTINEL

Operated by the U.S. Air Force's Air Combat Command's 432nd Wing, the drone supports combatant needs for intelligence, reconnaissance and surveillance

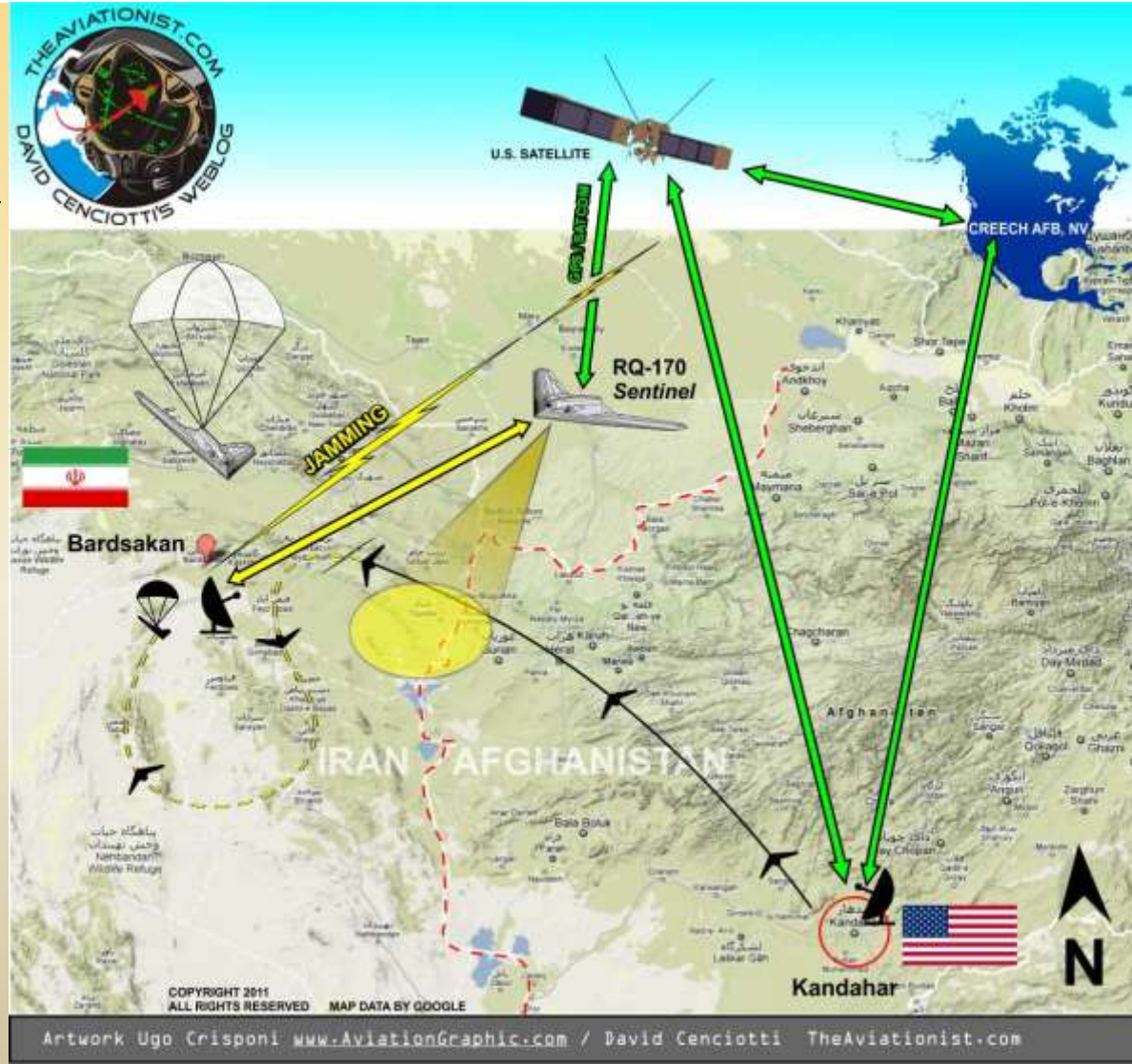
▶ Aircraft type Low observable, unmanned aircraft system (UAS)	▶ Operating altitude 15,240 m	▶ Material Composite	▶ Manufacturer Lockheed Martin
--	---	--------------------------------	--



Sources: af.mil, airforce-technology.com

Nestler: Drones and Cybersecurity

Iran captures RQ-170 Sentinel drone



- ❑ RQ-170 is no longer the American cutting edge robot tech
- ❑ Circuitry, lenses, memories and sensors survived the crash landing
- ❑ Evaluated, tested, copied and, possibly, improved with the help of Russia and China
- ❑ Chinese delegation in Iran to copy the U.S. stealth RQ-170 drone captured in 2011.

Nestler: Drones and Cybersecurity

- ❑ December 4, 2011 – The government of Iran claims that an aircraft was brought down by its cyber warfare unit stationed in Kashmar
- ❑ December 5, 2011 - U.S. military sources confirmed that the remains of an RQ-170 had been captured by Iranian forces
- ❑ December 6, 2011 - U.S. officials acknowledged that a drone crashed in or near Iranian airspace and that it belonged to the CIA and not to ISAF
- ❑ December 8, 2011 – Iranian government released footage of a captured RQ-170

Nestler: Drones and Cybersecurity

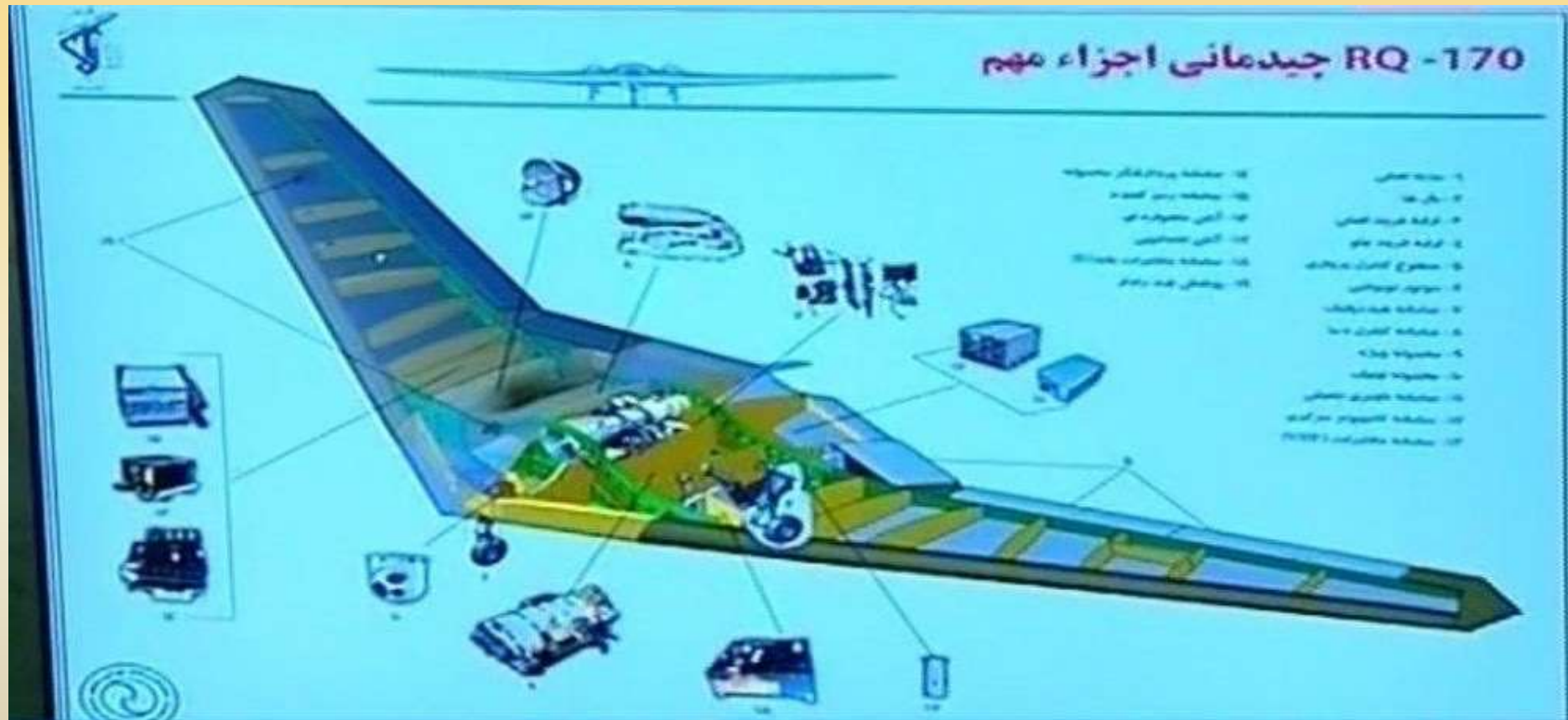
CAPTURED



Nestler: Drones and Cybersecurity



Nestler: Drones and Cybersecurity



Nestler: Drones and Cybersecurity

CLONED

Iran starts
cloning of
American spy
drone



Nestler: Drones and Cybersecurity



Nestler: Drones and Cybersecurity

Tehran copied the Sentinel as a toy and sent one to the U.S. as a mocking response to America's request to hand over the aircraft.



Nestler: Drones and Cybersecurity

An Iranian man shows miniature toy model of U.S. drone RQ-170 with slogan quoted by Iran's late founder of Islamic Republic Ayatollah Ruhollah Khomeini reading in Farsi, "we will step on the United States" in Tehran



Nestler: Drones and Cybersecurity

Should Have Seen it Coming

- Not the first time - intercepted video in 2009
- SkyGrabber: the \$26 software used by insurgents to hack into U.S. drones
 - Iraqi Shiite Militants used the software to see video feeds of Predator drones flying in the area
- No online internet connection needed
 - Tune a satellite dish to the correct frequency and location
 - Grab the signal with SkyGrabber
 - Decode and watch the video
- U.S. Military officials have known since the 1990s the signals were unencrypted

Nestler: Drones and Cybersecurity

The Headlines Keep Coming ...

- ❑ Russian jets intercept U.S. predator drones over Syria, Official say – Fox
- ❑ North Dakota Legalizes Armed Police Drones – NPR
- ❑ UK defense firm unveils electromagnetic anti-drone defense shield – Digital Trends
- ❑ Anti-drone shoulder rifle lets police take control of UAVs with targeted radio pulses –Digital Trends
- ❑ China unveils new anti-drone laser – Washington Post

Nestler: Drones and Cybersecurity



- ❑ 1.2-mile range laser
- ❑ Can bring down small low-flying aircraft within five seconds of locating target
- ❑ Weapon can be installed on vehicles
- ❑ Shot down more than 30 drones in a recent test a "100 per cent success rate"
- ❑ Effective against aircraft flying at up to 50 meters per second up to a maximum altitude of 500 meters, Xinhua said.



Nestler: Drones and Cybersecurity

Security Habit of Mind

- Four Questions
 - How does it work?
 - How is it vulnerable/threats?
 - How can it be hardened?
 - How can be detected and respond?

A system not just a vehicle

Communication systems

- GPS

- Compass

Video transmitter

- Wi-Fi

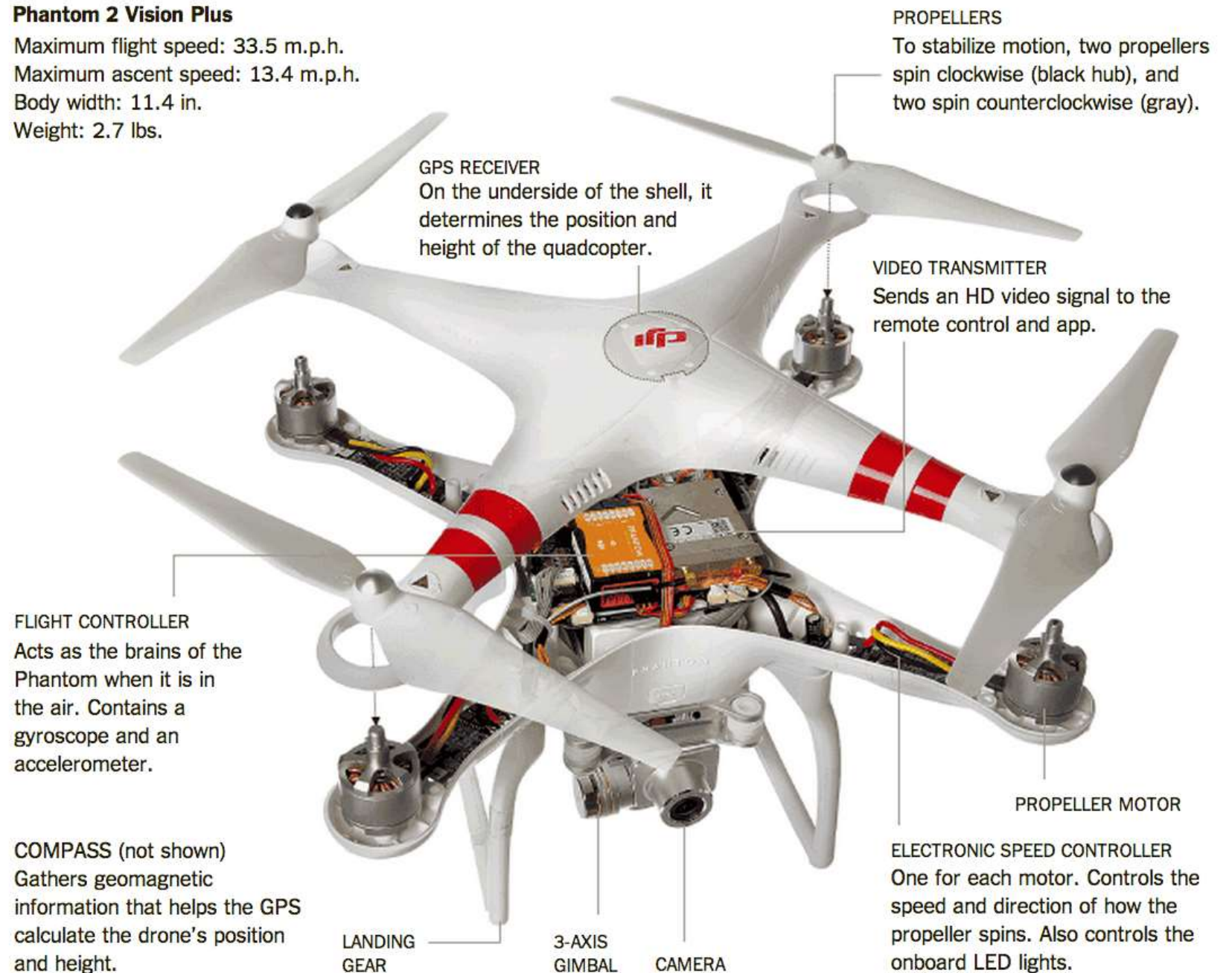
- Radio Controller

Control systems

- Flight controller and Electronic speed controller controls the blades

Phantom 2 Vision Plus

Maximum flight speed: 33.5 m.p.h.
Maximum ascent speed: 13.4 m.p.h.
Body width: 11.4 in.
Weight: 2.7 lbs.



Nestler: Drones and Cybersecurity

Two Things Needed by Cybersecurity Professionals

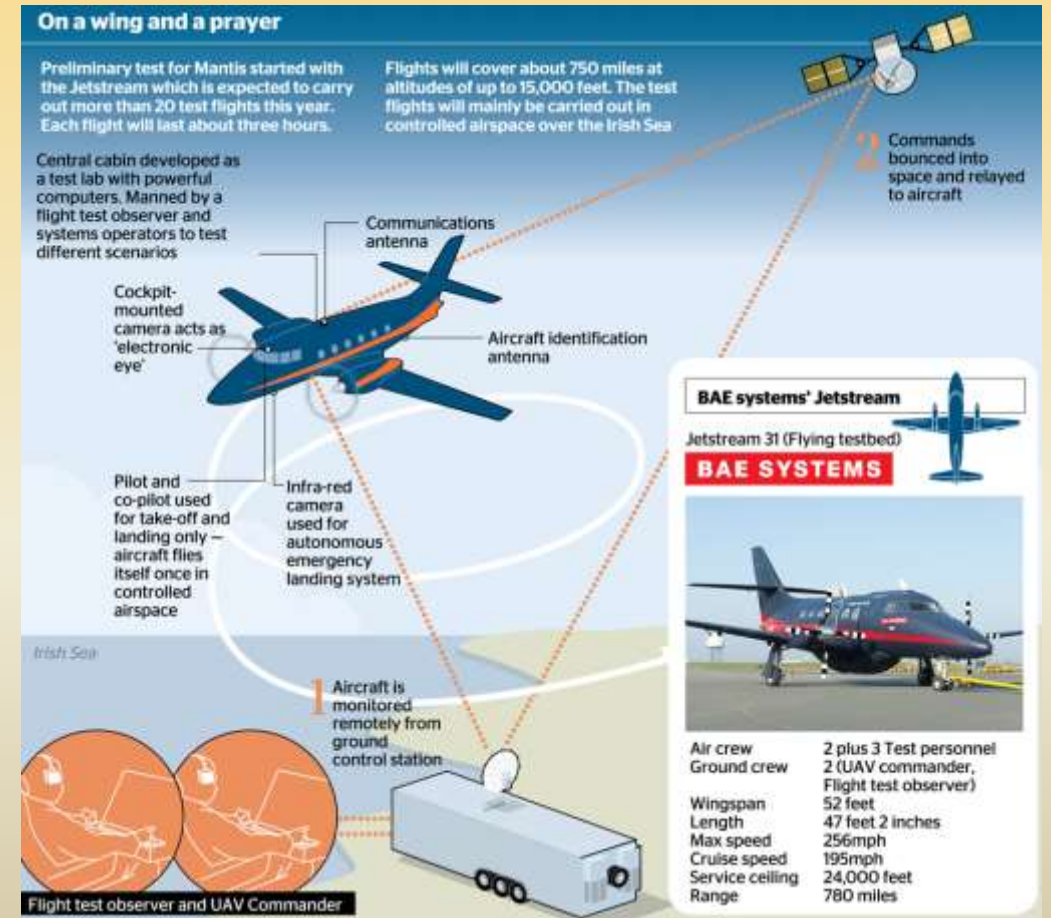
- ❑ Research shows - What is not needed
 - ❑ Content
 - ❑ Instructors
- ❑ What is needed
 - ❑ Interest, Passion
 - ❑ Problem Solvers
 - ❑ Self learners

Nestler: Drones and Cybersecurity

Will AI and Drones Merge?



“AI is a bad idea” --- Stephen Hawking



Melissa E. Hathaway's 5 W's of Cybersecurity

- ❑ “Our Government & Private Sector Networks & Information are being exploited on an Unprecedented Scale by a Growing Array of State & Non State Actors”
 - ❑ No sector without Compromise
 - ❑ Corporate Intellectual Property Stolen *at alarming rate*
 - ❑ Government networks targeted to steal information & gain understanding of mission critical dependencies & vulnerabilities
- ❑ “Persistent presence on these networks & No assurance that EVERY network has not been penetrated & infected with hidden software that could be triggered in a crisis to disrupt or destroy data or communications”

Melissa E. Hathaway's 5 W's of Cybersecurity

- ❑ “Cybersecurity so critical...U.S. Government needs to investigate the market supply chain of IT products.”
- ❑ To do this 5 questions must be asked:
 - ❑ Who designed the technology?
 - ❑ Who built the technology?
 - ❑ Who operates & maintains the technology?
 - ❑ Who upgrades the technology?
 - ❑ Who retires the technology?
- ❑ Each of these points of interface of the device with hardware, software, & technology design, presents an opportunity to introduce or exploit vulnerability

Melissa E. Hathaway's 5 W's of Cybersecurity

Globalization is a problem

- ❑ Company with close ties to a rival nation state (China, Russia, Iran) might permit bugs to be inserted somewhere in the supply chain
- ❑ Compromised technology installed in U.S. Mission Critical Applications
 - ❑ If U.S can not protect its networks, Adversaries jeopardize information by:
 - ❑ Steal Data from a target personal device, system or network
 - ❑ Alter crucial operating system data
 - ❑ Deny information by shutdown or DDOS block
 - ❑ What Ifs: erroneous weapons data? Fault early warning systems? Insert erroneous manufacturing data to be activated at a future date?

Melissa E. Hathaway's 5 W's of Cybersecurity

Solutions

- Comprehensive & coordinated effort to share information with private sector
- Government MUST Apply stricter risk models to private sector while funding research & development in technologies to secure cyberspace for U.S. citizens
- Public Awareness campaign – Individual weakness is common vulnerability
- Execute the National Cybersecurity Initiative
- Reduce number of access points between federal agencies & external computer networks to below 100. (There are currently ~ 3500)

Spafford: Cybersecurity In Crisis – 9 F’s

Observations

- ❑ “America has long been in the age of the computer & with companies’ increased reliance on computers & the Internet comes an alarming rate of crimes perpetrated via the Internet.”
- ❑ “We have people committing cybercrime offenses again & again, but it has been calculated as less than five percent of these crimes are prosecuted.”
- ❑ “More money is spent keeping people from bringing fingernail clippers on planes than is spent on Cybersecurity.”
- ❑ “Your Facebook is potentially viewable by two billion people.”

Spafford: Cybersecurity In Crisis – 9 F's

State of Cybersecurity

- ❑ Well over 180,000 known viruses & worms in wild
- ❑ 8000+ known system vulnerabilities & growing @ 20/day
- ❑ Damages are “hidden” of \$60 Billion / year & growing
- ❑ Spam is 90% at some ISPs
- ❑ #1 growth Crime is ID theft
- ❑ Organized cybercrime is increasing
- ❑ Facebook is potentially viewable by two billion online users

Spafford: Cybersecurity In Crisis – 9 F's

Why is U.S. INFOSEC getting worse?

- Increasing features & size of platforms
- Not based on secure design principles
- Coded by untrained personnel
- Confusing & unnecessary options
- Inconsistent configurations
- Forced by revenue cycles

Spafford: Cybersecurity In Crisis – 9 F's

Unsafe Operation & Insufficient Expertise

- Culture of patching
- Overly homogenous
- Acceptance of failures
- Myth of general purpose countermeasure
- Myth of the secure perimeter
- INFOSEC requires more than customer service
- Too few educational programs
- Insufficient support of R&D training
- Mistaking hacking for expertise

Spafford: Cybersecurity In Crisis – 9 F's

Major Failings

- ❑ Failing to understand the problem - It's the information, NOT the computer
- ❑ Failing to understand the threat - Related to not understanding the motives & methods of the attackers
- ❑ Failing to include the people
- ❑ Failure to build to a sound design - Too much accommodation of bad legacy code
- ❑ Placing too much trust in market pressure to provide highly trustable systems ... and then not using the market to good effect

Spafford: Cybersecurity In Crisis – 9 F's

Major Failings

- ❑ Relying on patching instead of on getting it right the first time
- ❑ A failure to protect holistically - Point protection is necessary but not sufficient
- ❑ Failure to provide any adequate deterrence in addition to protection: lack of tools; lack of funding; lack of priority; international
- ❑ Too much information is kept out of the hands of people who can use it: Company reticence; Over-classification

Spafford: Cybersecurity In Crisis – 9 F's

Solutions

- Need Balance in Research
- What are the systems after next?
- Need to grow the talent pool
- Need significant investment in R&D with longer focus
- Need investment in law enforcement – Includes reporting
- New research must forget the past & focus on: Malware, program flaws, privacy mechanisms, authentication, forensics, protocols, MLS design, intrusion detection & prevention, covert channels, crypto, digital cash, data mining, cyber terrorism, security architecture, residues, data pedigree, self-checking code, DRM

Parker: Traditional INFOSEC Framework

- Preservation of:
 - Confidentiality
 - Integrity
 - Availability

- Information from:
 - Disclosure
 - Modification
 - Destruction
 - Use

Parker: Traditional INFOSEC Framework

- By:

- Prevention

- Detection

- Recovery

- To:

- Reduce loss

- Reduce risk of loss

Parker Analysis: Modern INFOSEC Framework

- Preservation of six elements:
 - Availability
 - Utility
 - Integrity
 - Authenticity
 - Confidentiality
 - Possession of information

Parker Analysis: Modern INFOSEC Framework

- ❑ From accidental or intentional :
 - ❑ Destruction
 - ❑ Interference
 - ❑ Use of false data
 - ❑ Modification or replacement
 - ❑ Misrepresentation or repudiation
 - ❑ Misuse or failure to use

Parker Analysis: Modern INFOSEC Framework

- ❑ From accidental or intentional :
 - ❑ Access
 - ❑ Observation or disclosure
 - ❑ Copying
 - ❑ Stealing
 - ❑ Endangerment

Parker Analysis: Modern INFOSEC Framework

- By :
- Avoidance
- Deterrence
- Prevention
- Detection
- Mitigation
- Transference
- Sanction
- Recovery
- Correction

Parker Analysis: Modern INFOSEC Framework

- To:
 - meet a standard of due care
 - avoid loss
 - reduce loss
 - eliminate loss

Parker Analysis: Modern INFOSEC Framework

- Government controls include:
 - Employee clearances
 - Principle of need-to-know
 - Mandatory access control
 - Classification of information
 - Cryptography

Parker Analysis: Modern INFOSEC Framework

- Business controls include:
 - Need-to-withhold
 - Discretionary access control
 - Copyright and patent
 - Digital signatures

Mumm: Managing the Integration of the NAS for UAS

**Industrial
Revolution**

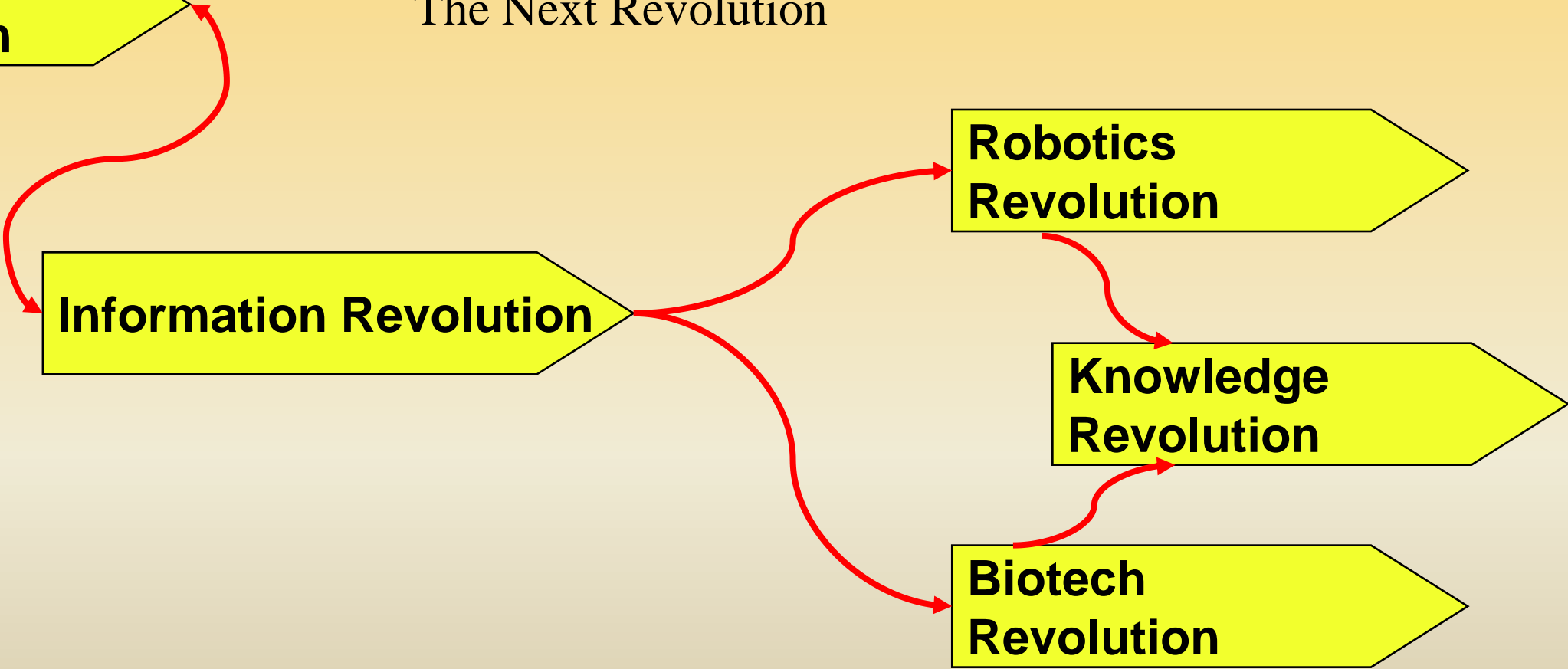
The Next Revolution

Information Revolution

**Robotics
Revolution**

**Knowledge
Revolution**

**Biotech
Revolution**

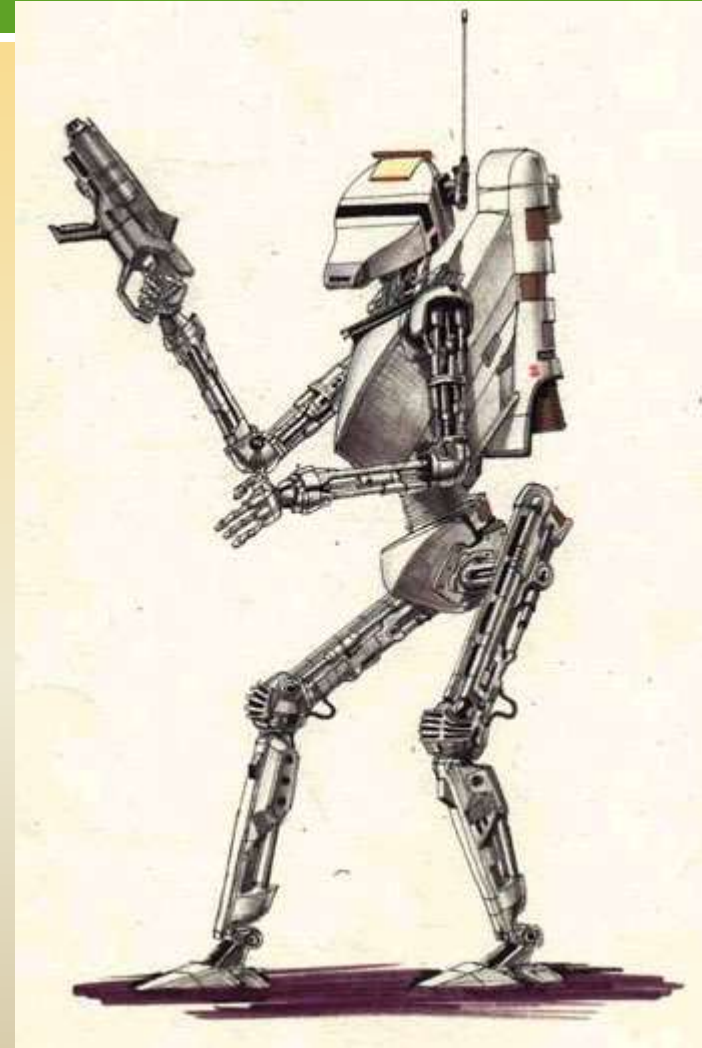


Mumm: Managing the Integration of the NAS for UAS

Levels of Autonomous Behavior



Mumm: Managing the Integration of the NAS for UAS



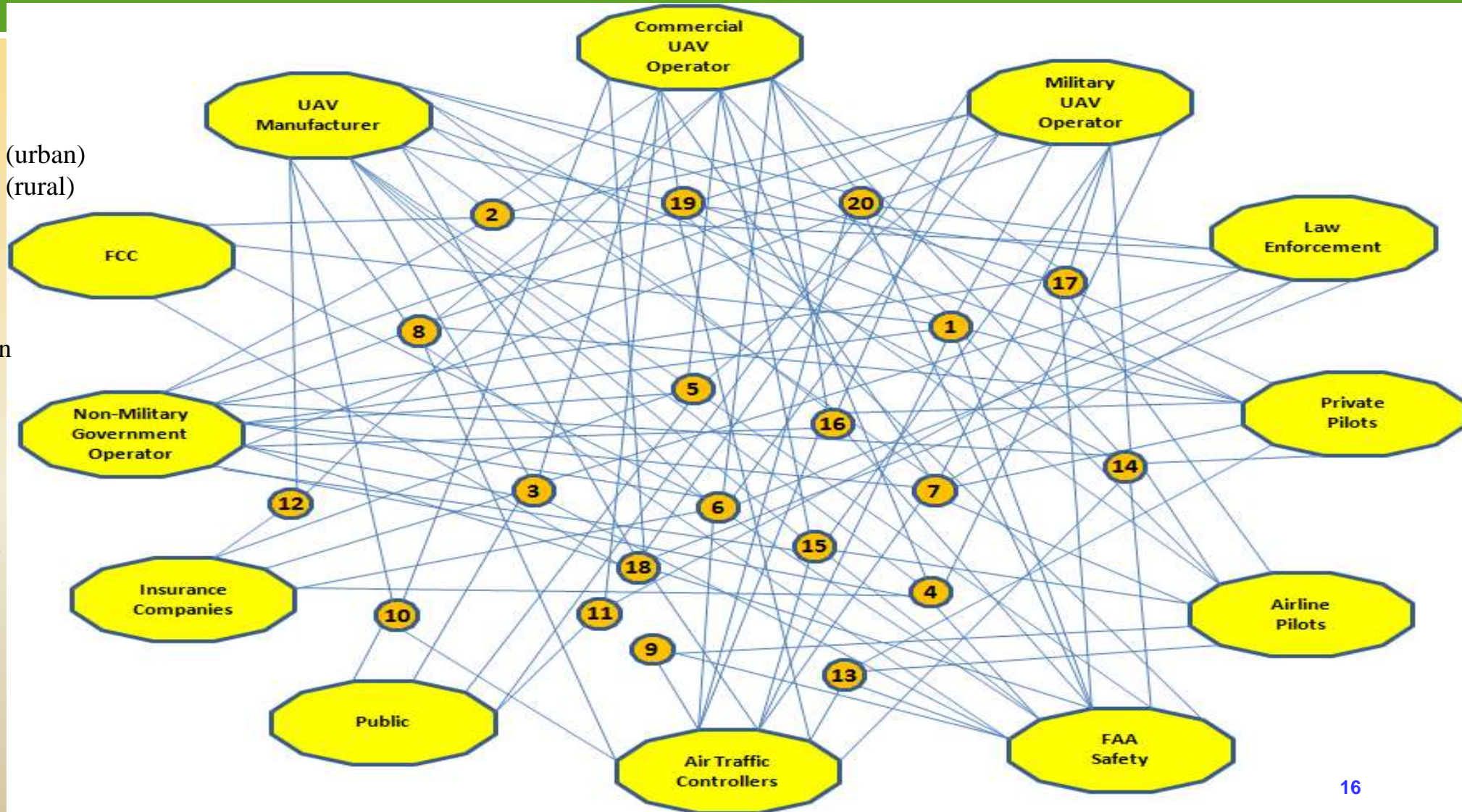
Robo Sapiens

As technology advances it will provide a level of autonomy which will allow the vehicle to make some of the decisions on its own. If you have a weapon on the platform, you would never want to give up control.

Mumm: Managing the Integration of the NAS for UAS

UAV Integration Complexity Network

- 1 Sense and Avoid
- 2 Frequency Management
- 3 Protection of people & property (urban)
- 4 Protection of people & property (rural)
- 5 Air Worthiness
- 6 Licensing
- 7 File and Fly
- 8 Required Equipment
- 9 Airport Terminal area congestion
- 10 Noise
- 11 Privacy
- 12 Insurance
- 13 Airway Congestion
- 14 Next Generation ADSB
- 15 Next Generation Info Network
- 16 Transponders
- 17 See and be seen
- 18 Voice communications
- 19 E Airspace
- 20 G Airspace



Mumm: Managing the Integration of the NAS for UAS

Civilian UAV Missions

- ❑ Government applications
 - ❑ Power by the hour versus acquisition
 - ❑ Less price sensitive
 - ❑ More interested in the product than the operations
 - ❑ NASA (Earth and Mars)
- ❑ Commercial applications
 - ❑ Must be profitable over the long term
 - ❑ Very difficult to build a profitable picture around a single mission or mission area
 - ❑ Every mission is a potential revenue stream
 - ❑ Must have convenient access to the National Air Space System



Mumm: Managing the Integration of the NAS for UAS

Potential Early Commercial Adopters

- ❑ Amazon
- ❑ Real Estate Companies
- ❑ Dominoes
- ❑ UPS/FedEx
- ❑ Forest Fighting Service Companies
- ❑ Insurance Companies
- ❑ News and Quasi-News Organizations

Mumm: Managing the Integration of the NAS for UAS

Current Limitations / Challenges

- ❑ Real-Time Imagery
 - ❑ How good is good enough
 - ❑ NIIRS
 - ❑ NTSC vs. 480p vs. HDTV
- ❑ Attrition Rate
 - ❑ Military-Commercial impact (Insurance)
- ❑ Flight Control and Multiple UAV operations
 - ❑ It's the brain stupid
 - ❑ Manpower costs
- ❑ Integrated Manned / Unmanned Systems
- ❑ Leadership and laws-public perceptions and threats to sovereignty -local-national-international

Mumm: Managing the Integration of the NAS for UAS

UAVs in Urban Operations

- ❑ Surveillance and Reconnaissance
 - ❑ Nodes and Networks
 - ❑ Force Protection
 - ❑ Situational Awareness
 - ❑ Fire Support (Lethal and Non-lethal)
- ❑ Counter Sniper
 - ❑ Mini UAVs
- ❑ Communication problems and solutions
 - ❑ UAV control in urban canyons
 - ❑ Radio relay for troops in urban canyons
- ❑ Psychological Warfare
 - ❑ News paper and leaflet drops
 - ❑ Voice
 - ❑ Lights, Camera, No-Action (Behavior Modification)

Cyber Terrorism / Counter Terrorism Implications - Facts

Radar Surveillance

- Radar: Radio Detection and Ranging
 - Active
 - Collocated transmitter and receiver
 - Radio signals emitted toward an object
 - Reflected signals intercepted and interpreted
 - Passive
 - No dedicated transmitter
 - Listen to echoes
 - Broadcast signals and see if they bounce back

Cyber Terrorism / Counter Terrorism Implications - Facts

Radar Surveillance

- Surveillance Applications
 - Military
 - Targeting
 - Tracking
 - Defense
 - Civilian
 - Monitor moving vessels
 - Hazards
 - Threats
 - Environmental changes
 - Weather systems

Cyber Terrorism / Counter Terrorism Implications - Facts

Radar Surveillance

❑ Radar Systems

❑ ADT

- ❑ Automatic Detection and Tracking
- ❑ Tracks moving vehicles and marine vessels

❑ PA

- ❑ Phased-Array Radar
- ❑ Beam sweeps back and forth

❑ SAR

- ❑ Synthetic-Aperture Radar
- ❑ Beam sweeps back and forth

Cyber Terrorism / Counter Terrorism Implications - Facts

Radar Surveillance

- ❑ Radar Systems
 - ❑ CW
 - ❑ Continuous-Wave Radar
 - ❑ Transmits and Receives at the same time
 - ❑ Frequencies differ for incoming and outgoing waves
 - ❑ Specialized Radars
 - ❑ Weapons
 - ❑ Scientific Research
 - ❑ Doppler Radar
 - ❑ Doppler Shift
 - ❑ An object is in motion relative to a reference point

Cyber Terrorism / Counter Terrorism Implications - Facts

Radar Surveillance

- ❑ Identification Systems
 - ❑ IFF - Identification friend or foe
 - ❑ IFFN - Identification friend, foe, or neutral
 - ❑ Security, Surveillance and Defense
 - ❑ Warn of movement, vessels, projectiles, and unidentified objects
 - ❑ Commercial security systems
 - ❑ Satellite early warning
 - ❑ Ballistic missiles defense

Cyber Terrorism / Counter Terrorism Implications - Facts

Infrared Surveillance

- ❑ Infrared Categories Based on Wave's Length
 - ❑ Short-wavelength infrared SWIR
 - ❑ Wavelength 1-3 μm
 - ❑ Medium-wavelength infrared MWIR
 - ❑ Wavelength \sim 3-5 μm
 - ❑ Long-wavelength infrared LWIR
 - ❑ Wavelength \sim 8-14 μm

Cyber Terrorism / Counter Terrorism Implications - Facts

Infrared Surveillance

- ❑ Infrared Categories Based on Distance from Visible Light
 - ❑ Near-infrared NIR
 - ❑ Wavelength 0.7-0.9 μm
 - ❑ Middle-infrared MIR
 - ❑ Wavelength 0.9-20 μm
 - ❑ Far-infrared FIR
 - ❑ Wavelength 20-1000 μm

Cyber Terrorism / Counter Terrorism Implications - Facts

Infrared Surveillance

- ❑ Common Applications
- ❑ Targets
 - ❑ People (customers, intruders)
 - ❑ Wildlife (game, injured livestock, research animals, insects, birds migrating at night)
 - ❑ Astronomical bodies
 - ❑ Electrical faults
 - ❑ Circuit boards

Cyber Terrorism / Counter Terrorism Implications - Facts

Infrared Surveillance

- ❑ Common Applications
- ❑ Targets
 - ❑ Fires
 - ❑ Arson
 - ❑ House fires
 - ❑ Forest fires
 - ❑ Drug-growing operations
 - ❑ Underground or building piping systems
 - ❑ Heat ducts and hot water pipes
 - ❑ Buildings (roofs, walls)

Cyber Terrorism / Counter Terrorism Implications - Facts

Aerial Surveillance

- ❑ Aerial Surveillance Craft
 - ❑ Wing-Lofted Craft
 - ❑ Lighter-Than-Air Craft
 - ❑ Self-Powered Craft
 - ❑ Launched Probes and Orbital Craft
 - ❑ Projectiles

Cyber Terrorism / Counter Terrorism Implications - Facts

Aerial Surveillance

- Context
 - Scientific Inquiry
 - Government Applications
 - Commercial Applications
 - Nonprofit and Public Welfare Applications
 - Personal Applications

Cyber Terrorism / Counter Terrorism Implications - Cyber Security Architecture (CT/CTI- CSA)

- Application Specific Integrated Circuits (ASICs)
ADVANTAGES (Nichols & Lekkas)
- New/Unknown Attack Vectors
- Secure Wireless LAN environments

Cyber Terrorism / Counter Terrorism Implications - Cyber Security Architecture

Application Specific Integrated Circuits (ASICs) ADVANTAGES

- ❑ End-to-end security of real time communications
- ❑ Bi-directional authentication content
 - ❑ Voice
 - ❑ Fax
 - ❑ Data
 - ❑ Streaming video
- ❑ Sustained operation at broadband speeds up to 8-16 GBit / sec full duplex
- ❑ Improvement of quality of link due to embedded and unique signal recovery

Cyber Terrorism / Counter Terrorism Implications

- Cyber Security Architecture

Application Specific Integrated Circuits (ASICs) ADVANTAGES

- ❑ Very low cost per unit, additional reductions possible if embedded on SOC (system on a chip) for hard or soft IP core
- ❑ Low probability of detection and superior anti-jam characteristics
- ❑ Security is independent of infrastructure

Cyber Terrorism / Counter Terrorism Implications - Cyber Security Architecture

New/Unknown Attack Vectors

- ❑ System Complexity Increases, Attack Vectors Increase.
- ❑ Move to ASIC Key Storage with Proprietary Software Controls.
- ❑ Key Storage
 - ❑ Cryptographic keys stored in open areas
 - ❑ Cryptographic units stored in open areas

Cyber Terrorism / Counter Terrorism Implications - Cyber Security Architecture

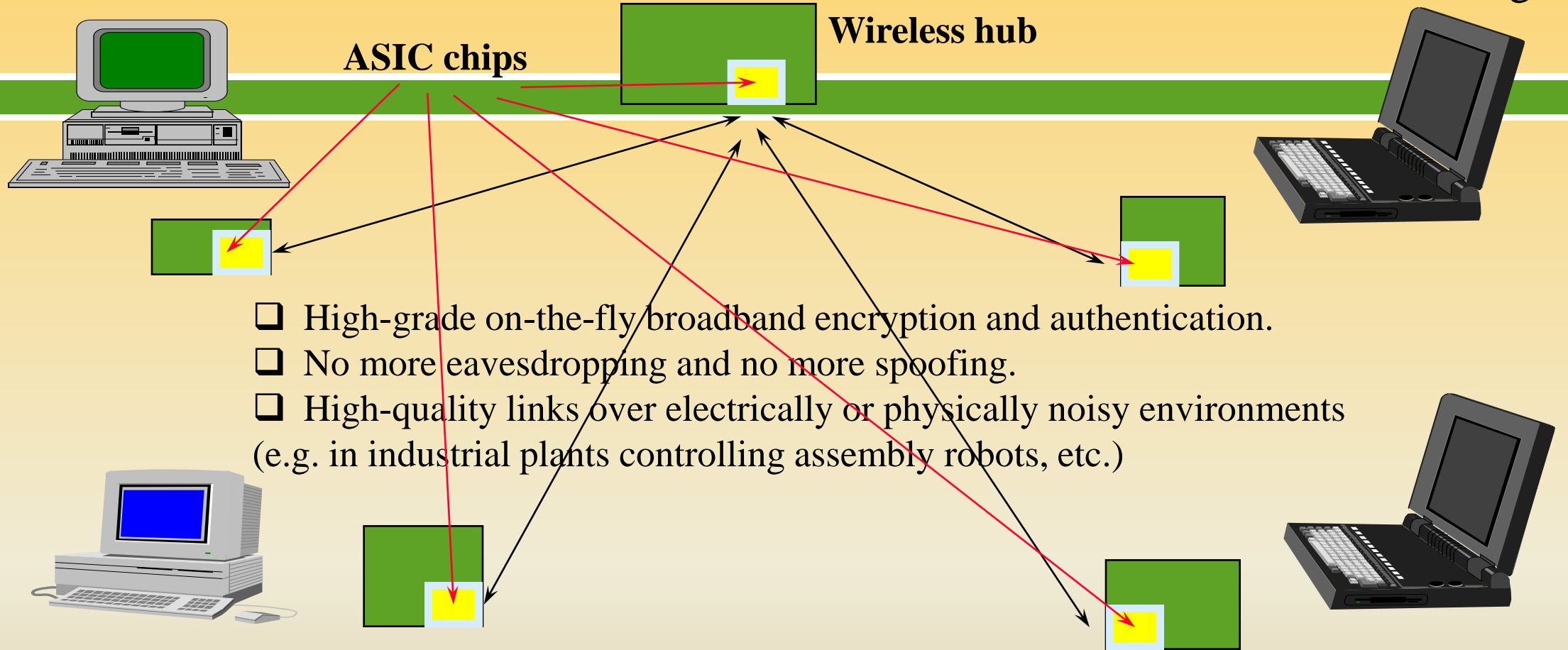
New/Unknown Attack Vectors

- ❑ Complexity: refer back to the poor implementation across a MAN, it was a highly complex network which was (like most networks) put together in an ad hoc fashion.
 - ❑ Trustworthy Computing initiative
 - ❑ Some operating systems, including Windows moving towards a hardware/software combination
 - ❑ Keys are stored in hardware ASIC and accessed directly by the operating system
- ❑ Recently some portions of the Windows NT and Windows 2000 source code were stolen off the Internet
 - ❑ What threats lie in wait when these systems face cyber attack?

Building A

CT/CTI- CSA - Secure Wireless LAN

Building A or B



- High-grade on-the-fly broadband encryption and authentication.
- No more eavesdropping and no more spoofing.
- High-quality links over electrically or physically noisy environments (e.g. in industrial plants controlling assembly robots, etc.)

Wireless secure modem
or our chip on motherboard
or embedded in an access unit

With appropriate small antenna
mobile user can be securely
operational from hundreds of yards
away from hub or building

Cyber Terrorism / Counter Terrorism Implications - Issues

- What are the risks to U.S. national security from open source information on its UAS performance?
- While increasing surveillance via UAS, how will the U.S. safeguard American citizen Rights to Privacy?
- What best practices can assist the FAA in creating (dynamic and/or scalable) public policy that incorporates UAS training, safety assessment, regulation, and countermeasures for preventing collisions?

Cyber Terrorism / Counter Terrorism Implications - Indicators

- ❑ Hackers could gain unauthorized access
 - ❑ Aircraft systems and networks
 - ❑ Results in malicious use of networks, and loss or corruption of data
 - ❑ Software applications
 - ❑ Databases
 - ❑ Configuration files
 - ❑ By software worms, viruses, or other malicious entities

Cyber Terrorism / Counter Terrorism Implications - Indicators

- ❑ Air Traffic Control System (ATC) Vulnerable to Cyber Terrorism
 - ❑ President Obama created a White House Office of Cyber Security on May 29, 2009
 - ❑ He said the U.S. has for too long failed to adequately protect the security of its computer networks
 - ❑ He called cyber threats one of the most serious economic and military dangers the nation faces
 - ❑ Satellite-based ATC System heavily reliant on COTS and IP-based technology
 - ❑ Creates more opportunities to hack into FAA systems

Cyber Terrorism / Counter Terrorism Implications - Indicators

- ❑ Air Traffic Control System (ATC) Vulnerable to Cyber Terrorism
 - ❑ Officials identified 763 high risk vulnerabilities that could give immediate access into an FAA computer system
 - ❑ Insufficient monitoring coverage of ATC creates another weakness for the FAA
 - ❑ Hackers gained access to FAA Systems causing a partial shutdown of ATC Systems in Alaska in close proximity to the University of Alaska, one of six UAS test sites

Cyber Terrorism / Counter Terrorism Implications - Indicators

Smart Skies Project

- ❑ Three-year, \$10M joint research project
 - ❑ Australian Research Centre for Aerospace Automation
 - ❑ Boeing Research & Technology
- ❑ Objective of Smart Skies: Develop and demonstrate automated separation management technologies for UAS to be in NAS, use information to develop standards and regulations for UAS in Australia and overseas
- ❑ Four research areas:
 - ❑ Mobile Aircraft Tracking System
 - ❑ Automated Electro-Optical System
 - ❑ Static Obstacle Avoidance
 - ❑ Global Automated Separation Management System

Cyber Terrorism / Counter Terrorism Implications - Indicators

Smart Skies: Mobile Aircraft Tracking System

- ❑ Research, develop & demonstrate a field-deployable surveillance system
- ❑ Designed to support UAS operations in non-segregated airspace
- ❑ Commercial off-the-shelf primary radar & tracking system
- ❑ Automatic Dependent Surveillance-Broadcast (ADS-B)
- ❑ Filtering, display & communication systems

Cyber Terrorism / Counter Terrorism Implications - Indicators

Smart Skies: Automated Electro-Optical (EO) System

- Detect and Avoid System (DAS) a.k.a. SAA
- DAS solution particularly suited to small fixed-wing UAS
- DAS required to make use of existing cost-effective sensing and processing capabilities already on-board typical UAS
- Provides sUAS with suitable detect and avoid capability, a decision aid to pilots and improves the safety of UAS operations
- To research, develop & flight test an automated SAA system for detecting & avoiding mid-on and over-taking scenarios with UAS
- Range of FOV, image processing & control law configurations explored

Cyber Terrorism / Counter Terrorism Implications - Indicators

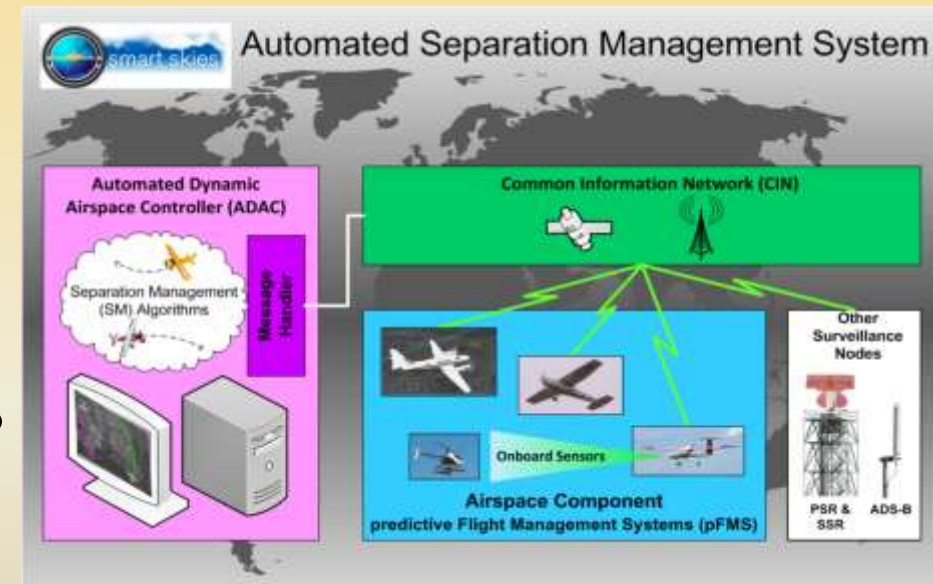
Smart Skies: Static Obstacle Avoidance (SOA)

- ❑ To research, develop & flight test an autonomous SOA system suitable for close range (<30m) Rotorcraft UAS operations at low-altitudes
- ❑ Research explored the use of a 2D scanning laser and stereo-camera sensors
- ❑ Detection of trees & autonomous operations around infrastructure

Cyber Terrorism / Counter Terrorism Implications - Indicators

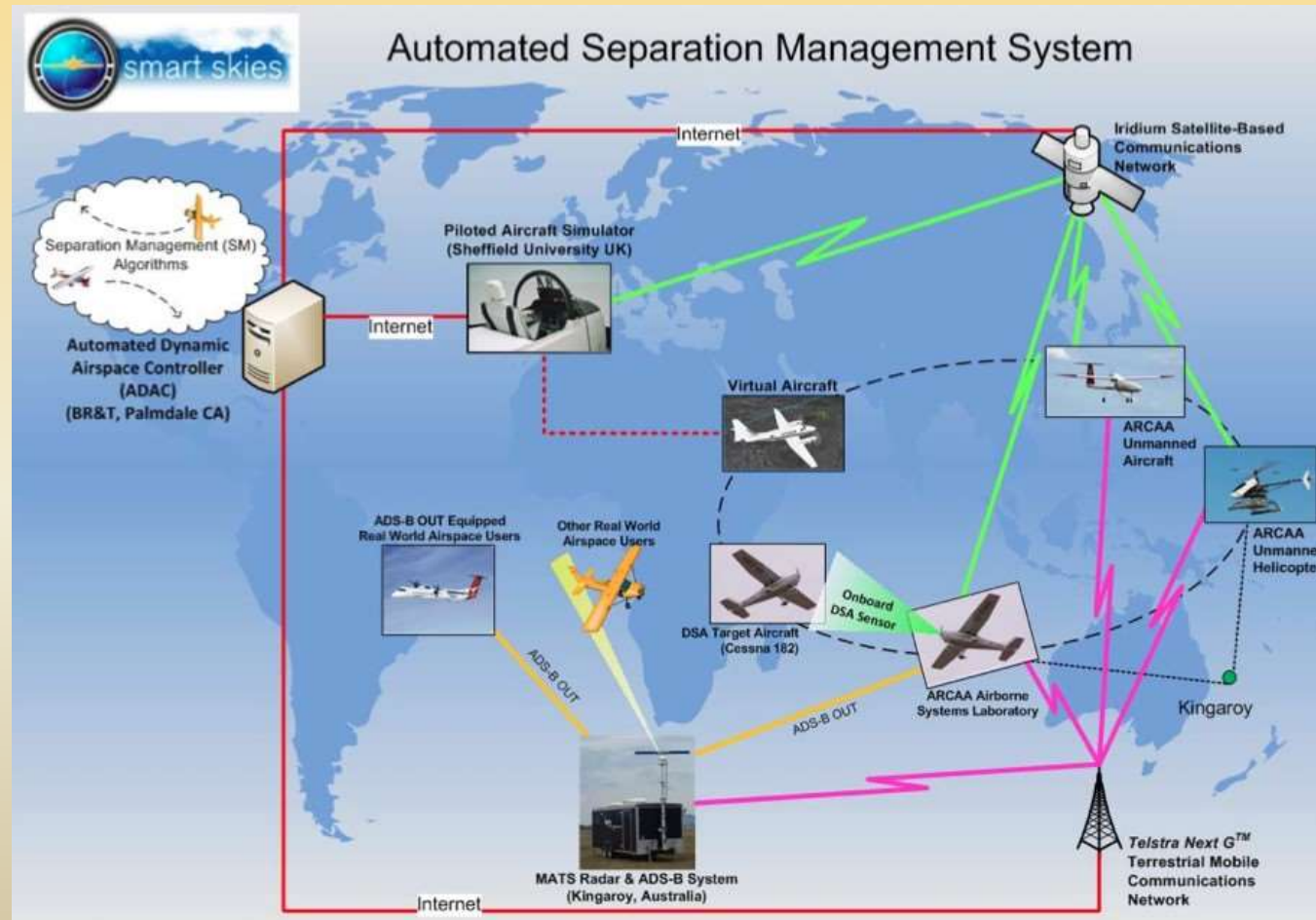
Smart Skies: Global Automated Separation Management System (ASMS)

- ❑ Service from anywhere in the world
- ❑ Automated conflict detection and resolution
- ❑ 4D separation resolution
- ❑ Multiple communications links
- ❑ Complex mix of airspace users, intent & behavior
- ❑ Separation commands fed directly into aircraft FMS



Cyber Terrorism / Counter Terrorism Implications - Indicators

Smart Skies: ASMS



Cyber Terrorism / Counter Terrorism Implications - Indicators

Low-Cost Mobile Radar Systems for sUAS SAA

- ❑ Unmanned Aircraft Systems (UAS) goals
 - ❑ Routine, regular, and safe integration of UAS into the national airspace system (NAS)
 - ❑ ‘File and Fly’: file a flight plan and fly within the same day
- ❑ Current system unacceptable
 - ❑ Time-critical applications can’t wait months for approval
 - ❑ Brushfire monitoring
- ❑ UAS demonstrated abilities
 - ❑ Fly, navigate, and perform useful missions
 - ❑ UAS cannot *see and avoid*, a human function

Cyber Terrorism / Counter Terrorism Implications - Indicators

Mobile Aircraft Tracking System (MATS)

- Mobile
- Network-enabled
- Surveillance system
- Detects other airspace users
 - Ground-based primary surveillance radar (PSR)
 - Supplemented with Automatic Dependent Surveillance – Broadcast (ADS-B)
 - Aircraft with ADS-B independently co-located with ADS-B receiver

Cyber Terrorism / Counter Terrorism Implications - Indicators

Mobile Aircraft Tracking System (MATS)

- ❑ Provides information to UAS pilot
 - ❑ Enables ground-based sense and avoid (GBSAA) capability
 - ❑ UAS pilot is in the control loop
- ❑ Enables automated SAA for UAS operations
- ❑ Acts as an aircraft sensor
 - ❑ Part of the larger aircraft tracking and control network
- ❑ Integrated component of Smart Skies Project
 - ❑ Initial demonstrations
 - ❑ Characterization trials

Cyber Terrorism / Counter Terrorism Implications - Indicators

Mobile Aircraft Tracking System (MATS)

- ❑ Smart Skies explored development of technologies
 - ❑ Support greater use of NAS by manned and unmanned aircraft
 - ❑ Aircraft accurately logged position and altitude during experiments
 - ❑ Served as a valuable calibration target for MATS
 - ❑ Opportunity to flight test several radar-based SAA scenarios with results
 - ❑ Showed examples of radar tracking variety of manned and unmanned aircraft
 - ❑ MATS showed location and movement of storms
 - ❑ GBSAA enables a pathway for UAS operations in the NAS

Cyber Terrorism / Counter Terrorism Implications - Indicators

Airspace and Radio Carriage

- Controlled airspace
 - ATC provides separation services
 - High-speed jets and turbo-prop aircraft in Class A airspace
 - No speed restrictions
 - Visual flight rules (VFR) not permitted
- Non-controlled airspace
 - VFR and Instrument flight rules (IFR) permitted
 - Speeds generally restricted to 250 knots below 10,000' above mean sea level (AMSL)
 - Continuous two-way communication with ATC required on IFR flights

Cyber Terrorism / Counter Terrorism Implications - Indicators

Airspace and Radio Carriage

- Class G airspace in Australia
 - Non-controlled airspace
 - Limited radio carriage requirements
 - VFR flights above 5000' AMSL
 - At aerodromes [small airports] requiring the carriage and use of radio
 - UAS operating problems
 - Location and intent of other airspace users are unknown
 - No see and avoid defense against midair collisions

Cyber Terrorism / Counter Terrorism Implications - Indicators

See and Avoid

- Aircraft regulations require pilots to see and avoid
 - Aircraft and other objects
 - Flying in visual meteorological conditions
 - Aids collision prevention
 - Far from reliable
 - Uncertain method of traffic separation

Cyber Terrorism / Counter Terrorism Implications - Indicators

Midair Collisions

- Between manned aircraft
 - Rare involving large commercial aircraft
 - Greater risk in General aviation (GA)
 - At relatively low closing speeds
 - From the rear, above, or quartering angle
 - Low altitude
 - On approach and landing
 - Less frequently on take-off and climb-out

Cyber Terrorism / Counter Terrorism Implications - Indicators

Midair Collisions

- ❑ Probable causes in 94% of collisions
 - ❑ Failure to see and avoid
 - ❑ Inadequate visual lookout
 - ❑ Failure to maintain visual and physical clearance
- ❑ SAA performance compared to human pilot
 - ❑ Failure rate of 10^{-2} to 10^{-3} per flight hour per regulation
 - ❑ Between 1 per 100 to 1 per 1000 PFH
 - ❑ Does not need to be a flight critical system
 - ❑ Failure rate of less than 10^{-7} PFH
 - ❑ < 1 per 10,000,000 PFH

Cyber Terrorism / Counter Terrorism Implications - Indicators

UAS Operating Environment

- Initial operations away from populous areas
- Typical environment
 - Non-towered small airport in Class G airspace
 - Could include other aircraft operating for pleasure or training
 - Only some aircraft will carry transponders or provide VHF radio reports
 - Higher risk of midair collision
- Must carefully consider SAA system FOV because midair collisions do not tend to be head-on

Cyber Terrorism / Counter Terrorism Implications - Indicators

A Layered Approach to Avoiding Collisions

- ❑ Separation management provided by:
 - ❑ ATC
 - ❑ VHF-radio location and intention reports
 - ❑ Intended to keep aircraft separated by safe distance
 - ❑ Aim of SAA self-separation function is safe clearance
- ❑ Collision avoidance layer activated on self-separation failure
 - ❑ Aim is to escape dangerous situations
 - ❑ Stated goal is ‘don’t scrape paint’
- ❑ SAA collision avoidance involves last-minute maneuvering

Cyber Terrorism / Counter Terrorism Implications - Indicators

A Layered Approach to Avoiding Collisions

- Must acquire intruding aircraft in time to perform SAA sub functions
 - Detect
 - Track
 - Evaluate
 - Prioritize
 - Declare Threat
 - Determine Action
 - Command
 - Execute

Cyber Terrorism / Counter Terrorism Implications - Indicators

A Layered Approach to Avoiding Collisions

- ❑ Sensor acquisition range affects severity of evasive maneuvers
 - ❑ More sensitive detection equipment
 - ❑ Detect at longer range
 - ❑ Reduces severity of evasive maneuvers
 - ❑ Less sensitive detection equipment
 - ❑ Detect at shorter range
 - ❑ Increases severity of evasive maneuvers

Cyber Terrorism / Counter Terrorism Implications - Indicators

A Layered Approach to Avoiding Collisions

- Detection technology trade space
 - Active SAA Systems
 - Transmit a signal to receive information about other aircraft
 - Passive SAA Systems
 - Do not transmit a signal
 - Use sensor measurements to detect other aircraft
- Cooperative aircraft use electronic transponder for identification
- Non-cooperative aircraft have no on-board means for identification
 - No transponder
 - Transponder not functional from malfunction or deliberate action

Cyber Terrorism / Counter Terrorism Implications - Indicators

A Layered Approach to Avoiding Collisions

- Cooperative SAA solution is ideal
 - FAA recommended for every non-cooperative aircraft
 - Be installed and operate with electronic means of identification
 - Short-range
 - Low-power
 - Lightweight
- Alternative recommendation
 - Spend approximately US\$58 million
 - Equip remaining U.S. fleet of aircraft
 - ADS-B OUT (transmit only)

Cyber Terrorism / Counter Terrorism Implications - Indicators

UA Operating Volume

- ❑ Detection and tracking volume aims
 - ❑ Provide a minimum level of detection and tracking performance
 - ❑ Covers aircraft with a minimum radar cross section (RCS)
 - ❑ RCS measures how well radar can detect an object
 - ❑ Targets with a larger RCS can be detected at longer ranges
- ❑ Surveillance volume describes the effective limits of a surveillance system
 - ❑ Aircraft with low RCS may not be detected between surveillance volume and detection and tracking volume
- ❑ Radar system performance characteristics set airspace volume dimensions
- ❑ Speed of aircraft and range to the UA sets warning time for the SAA timeline

Cyber Terrorism / Counter Terrorism Implications - Indicators

Situation Awareness

- Be aware of what is happening in the immediate vicinity
- Understand what that information means
 - Effects present and future decision-making
- Persons cannot be given situation awareness
- GBSAA systems provide information to UAS pilots
 - Enhance situation awareness of the pilot
- Maintaining a high-level of situation awareness is essential for effective decision-making, a key ingredient of SAA, especially while UAS pilots remain in direct control of the UA

Cyber Terrorism / Counter Terrorism Implications - Indicators

SAA Summary

Unmanned aircraft require sense and avoid (SAA) for greater operational freedom in the NAS

- Support for UAS available from:
 - Low-cost mobile radar
 - ADS-B receiver
 - GBSAA
 - MATS – Smart Skies
 - Non-segregated airspace within NAS
 - Predetermined flight plans
 - Specially equipped aircraft included with other aircraft of varying shapes/sizes

Cyber Terrorism / Counter Terrorism Implications - Indicators

SAA Summary

Local terrain influences GBSAA performance

- Must position system to achieve desired surveillance coverage
- Weather influences operating environment
 - Radars monitor rainfall and track storms
- Military UAS flights in the NAS
 - Training
 - Research and Development
 - Testing
 - U.S. DoD incremental NAS access strategy
 - Starts with line-of-sight operations
 - GBSAA supports terminal area operations and UA transiting airspace
 - Makes a case for 'file and fly' UAS operations

Cyber Terrorism / Counter Terrorism Implications - Judgments

- ❑ Schrodinger's Cat, when observed, will be found dead or alive
 - ❑ Outcomes are inevitable regardless of observation
 - ❑ The cat will eventually be found dead whether observed or not
- ❑ The FAA has no public policy to deal with inevitable UAS/piloted aircraft collision
 - ❑ Attacks or accidents have specific public policy responses
 - ❑ Because a collision has yet to be observed does not justify the absence of a public policy or absolve the FAA from responsibility to create one
- ❑ The FAA must have an official public policy for UAS in the NAS, so it's prepared to mitigate the risk of a UAS collision with a piloted aircraft, whether by attack or accident

Cyber Terrorism / Counter Terrorism Implications - Judgments

- ❑ UAS surveillance must protect U.S. citizen Rights to Privacy regardless of the altitude, surveillance method, intent or objective
- ❑ UAS public policy must include privacy rights oversight authority
- ❑ UAS public policy must be adaptable to accommodate rapidly changing technology
- ❑ FAA must implement UAS tracking to assist civilian and military law enforcement investigations

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

- ❑ **FAA must treat UAS as one of many Critical Infrastructures in the U.S.**
- ❑ **Add robust cybersecurity regulations, policy, and guidance**
 - ❑ **Strengthen security related certification criteria**
 - ❑ **Standardize and harmonize between domestic and international regulatory authorities**
- ❑ **The FAA must have an official public policy for UAS in the NAS, so it's prepared to mitigate the risk of a UAS collision with a piloted aircraft, whether by attack or accident**

Cyber Terrorism / Counter Terrorism Implications - Recommendations

U.S. must classify formerly open source information on its UAS performance.

- ❑ The U.S. must safeguard privacy and constitutional freedoms while increasing surveillance via UAS, to protect critical infrastructures.
- ❑ The FAA must create a dynamic and scalable UAS public policy that incorporates UAS training as a top priority, and include safety assessment, regulation, and countermeasures for preventing collisions.

Cyber Terrorism / Counter Terrorism Implications - Recommendations

- ❑ SAA for UAS must have top priority in Critical Infrastructure public policy
 - ❑ Include comprehensive rules to enable and support ‘file and fly’
 - ❑ Implement public policy before a manned aircraft collides with a UAS in the NAS
- ❑ FAA must follow best practices of the Smart Skies Project
 - ❑ Must include ways and means for training UAS operators to
 - ❑ Avoid midair collisions
 - ❑ Demonstrate proficiency in collision avoidance
 - ❑ Must require all UAS to have active detection technology installed
 - ❑ Must require orientation of UAS operators to local GBSAA installations

Cyber Terrorism / Counter Terrorism Implications - Recommendations

Implement Smart Skies technology for UAS

- ❑ Automated Electro-Optical (EO) mid-air collision avoidance system to provide UAS with SAA capability
- ❑ Automated static obstacle avoidance (SOA) system to support safe operation of unmanned rotorcraft at low altitudes and in unknown environments
- ❑ Mobile ground-based air traffic surveillance system (MATS) to provide UAS operators with information about local air traffic environment
- ❑ Global Automated Separation Management System (ASMS) to manage complex air traffic scenarios involving manned and unmanned aircraft

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Automated Electro-Optical (EO) System
 - ❑ Detect and Avoid System (DAS) a.k.a. Sense and Avoid (SAA)
 - ❑ DAS solution particularly suited to small fixed-wing UAS
 - ❑ DAS required to make use of existing cost-effective sensing and processing capabilities already on-board a typical UAS
 - ❑ Aware of size, weight, power, and cost-constraints of sUAS platforms
- ❑ Provides sUAS with suitable detect and avoid capability, a decision aid to pilots, and improves the safety of manned and unmanned aviation operations

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- Automated static obstacle avoidance (SOA) system to support safe operation of unmanned rotorcraft at low altitudes and in unknown environments
 - Be suitable for use in unknown outdoor environments
 - Use sensors appropriate for weight, cost, and power consumption of mini unmanned helicopters
 - Enable inspection of remote pieces of infrastructure Beyond the Visual Light Of Sight (BYLOS) of the aircraft controller
 - Be robust through intermittent communications
 - Capable of avoiding common obstacles including trees and structures and capture imagery of inspection target
- Uses lightweight COTS sensors, simple perception methods, and reactive behaviors to achieve autonomous obstacle avoidance

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Mobile ground-based air traffic surveillance (MATS) system to provide UAS operators with information about local air traffic environment
 - ❑ Use low-cost and portable primary surveillance radar (PSR) that supports UAS operations at any location
 - ❑ Supplemented with other surveillance systems
 - ❑ Automatic Dependent Surveillance – Broadcast (ADS-B) to enhance the airspace picture provided to the UAS pilot, who uses MATS sensor information to keep the UAS well clear of other aircraft
 - ❑ Ability to sense and avoid satisfies a key requirement for flying UAS in the NAS
- ❑ Can assist UAS operations and provide information about local airspace users to UAS pilots to keep UAS clear of other aircraft

Cyber Terrorism / Counter Terrorism Implications

- Recommendations

Implement Smart Skies technology for UAS

- ❑ Global Automated Separation Management System (ASMS) to manage complex air traffic scenarios involving manned and unmanned aircraft
 - ❑ Provides air traffic separation services for complex Air Traffic Management (ATM) scenarios
 - ❑ Involving a mix of manned and unmanned aircraft from any country
 - ❑ Improve the efficiency and flexibility of ATM for future airspace environments
 - ❑ Scenarios involve large numbers and diverse mix of cooperative and uncooperative airspace users
- ❑ Remotely located computing, commercial data links, and aircraft-based flight management systems provide separation services for complex ATM scenarios, reduce the workload of air traffic controllers, improve efficient use of airspace, and maintain and improve current safety levels

Glossary

- ❑ Aircraft Hull Insurance -- An insurance policy providing coverage to owners and operators of an aircraft in event that it is damaged or destroyed.
- ❑ Cyber Terrorism -- Any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents
- ❑ SCADA -- System Control And Data Acquisition
- ❑ Schrodinger's Cat -- Thought experiment

Glossary

- ❑ ADAC --Automated Dynamic Airspace Controller
- ❑ ADS - B --Automatic Dependent Surveillance - Broadcast
- ❑ ARCAA--Australian Research Centre for Aerospace Automation
- ❑ ASL --Airborne Systems Laboratory
- ❑ ASMS --Automated Separation Management System
- ❑ ATM --Air Traffic Management
- ❑ BR & T --Boeing Research & Technology
- ❑ BVLOS --Beyond the Visual Line Of Sight
- ❑ CIN --Common Information Network
- ❑ CPA --Closest Point of Approach

Glossary

- ❑ CPA --Conventionally-Piloted Aviation
- ❑ CSIRO --Commonwealth Scientific and Industrial Research Organization
- ❑ DAS --Detect and Avoid System
- ❑ EO --Electro-Optical
- ❑ FAR --False Alarm Rate
- ❑ FOV --Field of View
- ❑ GA --General Aviation
- ❑ GBSAA -- Ground-Based Sense And Avoid
- ❑ IR --Infrared
- ❑ MATS --Mobile Aircraft Tracking System
- ❑ MOC --Mobile Operations Center

Glossary

- ❑ NAS --National Airspace System
- ❑ pFMS --Predictive Flight Management Systems
- ❑ QUT --Queensland University and Industrial
- ❑ RCS --Radar-Cross Section
- ❑ SOA --Static Obstacle Avoidance
- ❑ SME --Subject Matter Experts
- ❑ UAS --Unmanned Aerial System
- ❑ UUV --Unmanned Underwater Vehicle
- ❑ VMC --Visual Meteorological Conditions

Primary References

Aeronautical Decision Making (2015) (PDF) Professor Handout.

Angelov, P. (2012). Sense and avoid in UAS research and applications. Hoboken, N.J.: Wiley.

Christensen, R. (1997). *Effect of technology integration education on the attitudes of teachers and their students*. Doctoral dissertation, Univ. of North Texas. Based on Russell, A. L. (1995) Stages in learning new technology. *Computers in Education*, 25(4), 173-178.

Clothier, R.A., Frousheger, D., Wilson, M., (2010) *The Smart Skies Project: Enabling technologies for future airspace*. Australian Research Center for Aerospace Automation, Commonwealth Scientific and Industrial Research Organization, Boeing Research and Technology-Australia environments

Nichols, R.K, (Nov 28-30, 2006) *Cyber Terrorism, Critical Infrastructure, & SCADA Presentation*: Utica College, Utica NY. Defense Threat Reduction Agency Conference, Shirlington VA

Nichols, R.K. (2004, January 1). “*Trust Me, Its Encrypted*”. Lecture presented at Rutgers University, New Brunswick, NJ.

Nichols, R.K., & Lekkas, P.C., (2002) *Wireless Security: Models, Threats and Solutions*, New York: McGraw Hill.

Nichols, R.K., Ryan, D.J., & Ryan, J.C.H., (2001) *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*, McGraw-Hill.

Nichols, R.K. (2009, April 16). *Terrorism – The Mutating Threat CYBERSECURITY – A Future in Crisis?* Lecture presented at NYSETA Plenary in SUNYIT, Utica, NY.

Norris, A. (2013). *Legal Issues Relating to Unmanned Maritime Systems Monograph*. Retrieved November 23, 2015.

Parker, D.B, (1991) *Proceedings of the 14th National Computer Security Conference*.

Primary References

Petersen, J. (2001). *Understanding surveillance technologies: Spy devices, their origins & applications*. Boca Raton, FL: CRC Press.

Mumm, H. (2015). *Applying Complexity Leadership Theory to Drone Airspace Integration*. Melbourne, Florida: Motivational Press

Mumm, H. (2015, December 4). *Managing the Integration and Harmonization of the National Airspace for Unmanned and Manned Systems*. Lecture presented at DuPont Summit in The Historic Whittemore House, Washington D.C.

Nestler, V. (2015, October 15). *The Age of Drones and Cybersecurity*. Lecture presented at Centers of Academic Excellence TECH TALK in Capitol Technology University, San Bernardino, CA.

Secondary References

- 45 years ago: First message sent over the Internet. (2014, October 29). Retrieved December 3, 2015, from <http://www.cbsnews.com/news/first-message-sent-over-the-internet-45-years-ago/>
- 1950s & 1960s. (n.d.). Retrieved December 5, 2015, from <https://sites.google.com/site/uavuni/1950s-1960s>
- Advanced Drone Detection Technology. (2015). Retrieved December 3, 2015, from <http://www.dronedetector.com/>
- Aircraft Hull Insurance. (2012). Retrieved November 29, 2015, from <http://financial-dictionary.thefreedictionary.com/>
- Air Informatics® LLC . (2015). Retrieved October 25, 2015 from http://www.airinformatics.com/e-Enabled_Definition.html/
- Amazon's Drone Highway Concept. (2015, September 23). Retrieved December 3, 2015, from <https://www.workinghomeguide.com/23979/amazons-drone-highway-concept>
- Arthur, C. (Ed.). (2009, December 17). SkyGrabber: The \$26 software used by insurgents to hack into US drones. Retrieved December 5, 2015, from <http://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked>

Secondary References

- B, W. (2009, June 8). Air Traffic Control System Vulnerable to Cyber Terrorism. Retrieved December 2, 2015, from <https://www.globaldatavault.com/blog/air-traffic-control-system-vulnerable-to-cyber-terrorism/>
- Bonggay, C. (2015, March 4). Commercial Drone Rules Around the World PrecisionHawk. Retrieved November 17, 2015, from <http://media.precisionhawk.com/topic/commercial-drones-faa/>
- Calvo, K. (2015, October 29). So You Want to Keep Track of All Your Drone Flights? Retrieved November 3, 2015, from <http://voices.nationalgeographic.com/2015/10/29/so-you-want-to-keep-track-of-all-your-drone-flights/>
- Carpenter, R., & Anderson, A. (2006). The death of Schrödinger's cat and of consciousness based quantum wave-function collapse. *Annales De La Fondation Louis De Brogli*, 31(1), 45-52. Retrieved December 2, 2015, from <http://web.archive.org/web/20061130173850/http://www.ensmp.fr/aflb/AFLB-311/aflb311m387.pdf>
- CARAC Activity Details. (2015). Retrieved November 9, 2015, from <http://wwwapps.tc.gc.ca/Saf-Sec-Sur/2/NPA-APM/actr.aspx?id=17&aType=1&lang=eng>
- Castillo, A. (2015, November 10). A DMV for Drones? Inside the FAA's Clumsy Push to Regulate Flying Computers. Retrieved November 22, 2015, from <https://reason.com/archives/2015/11/10/faa-versus-drones>
- Chesson, J. (n.d.). Cyber Crime. Retrieved December 3, 2015, from http://www.powershow.com/view/20b54-OGU4Z/Cyber_Crime_powerpoint_ppt_presentation
- Chicago Protects Critical Infrastructure and Services with Security Connected. (2014). Retrieved December 2, 2015, from <http://www.mcafee.com/us/case-studies/cs-city-of-chicago.aspx>

Secondary References

Chinese drone manufacturer DJI building outpost and hiring in Palo Alto - Silicon Valley Business Journal. (2015, October 30). Retrieved October 31, 2015, from <http://www.bizjournals.com/sanjose/blog/techflash/2015/10/chinese-drone-manufacturer-dji-is-building-a.html>

Cyber Threats. (2015). Retrieved December 2, 2015, from <http://thefc2.org/news/cyberthreatvectors.aspx>

Definition of Black Swan Theory. (2015). Retrieved December 2, 2015, from <http://www.davemanuel.com/investor-dictionary/black-swan-theory/>

DJI: The World Leader in Camera Drones/Quadcopters for Aerial Photography. (2015). Retrieved December 1, 2015, from <http://www.dji.com/>

Drones vs. Radio-Controlled Aircraft: A Look at the Differences between the Two. (2015). Retrieved November 3, 2015, from <https://rcflightline.com/drones-vs-radio-controlled-aircraft-a-look-at-the-differences-between-the-two/>

Dussault, J. (2014, March 14). 7 commercial uses for drones. Retrieved December 1, 2015, from <http://www.boston.com/business/2014/03/14/commercial-uses-for-drones/dscS47PsQdPneIB2UQeY0M/singlepage.html>

Edwards, D. (2015). Flying-Swimmer (Flimmer) UAV/UUV. Retrieved December 1, 2015, from <http://www.nrl.navy.mil/lasr/content/flying-swimmer-flimmer-uavuuv>

Federal Aviation Administration. (2015, November 1). Retrieved November 30, 2015, from <https://www.faa.gov/>

Secondary References

Facts. (2015). Retrieved November 1, 2015, from <http://knowbeforeyoufly.org/ - Facts/>

Federal Register. (2015, February 3). Retrieved October 25, 2015 from <http://www.gpo.gov/fdsys/pkg/FR-2015-02-03/html/2015-01918.html>

Ferranti, M. (2015, October 19). US to require registration process for drones. Retrieved October 31, 2015, from <http://www.cio.com/article/2994818/us-to-require-registration-process-for-drones.html>

Foxx, A. (2015, October 19). Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS. Retrieved October 31, 2015, from <https://www.federalregister.gov/articles/2015/10/22/2015-26874/clarification-of-the-applicability-of-aircraft-registration-requirements-for-unmanned-aircraft>

Geofencing... What is it and How does it Work? (2014). Retrieved December 3, 2015, from <http://socialbrothers.net/2014/03/18/geofencing-what-is-it-and-how-does-it-work/>

Gorman, S., Dreazen, Y., & Cole, A. (2009, December 17). Insurgents Hack U.S. Drones. Retrieved December 2, 2015, from <http://www.wsj.com/articles/SB126102247889095011>

Hackers. (2015, March 10). Retrieved December 3, 2015, from http://csrc.nist.gov/publications/nistir/threats/subsection3_4_2.html

Secondary References

- Hernandez, A. (2015, October 2). UAV. Retrieved November 17, 2015, from <http://www.slideshare.net/AnthonyHernandezMPAB/uav-53447022>
- Huerta, M. (2013). *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*. Retrieved November 17, 2015, from http://www.faa.gov/uas/legislative_programs/uas_roadmap/media/UAS_Roadmap_2013.pdf
- Howard, C. (2015, May 21). Team of military pilots enter consumer drone market, launch UAV control software. Retrieved November 16, 2015, from <http://www.intelligent-aerospace.com/articles/2015/05/team-of-military-pilots-enter-consumer-drone-market-launch-uav-control-software.html>
- Information Security Office Shared Services. (2015). Retrieved December 2, 2015, from http://www.cityofchicago.org/city/en/depts/doi/provdrs/security_and_datamanagement/svcs/information-security-office-shared-services.html
- Insurance Coverage for Unmanned Aerial Vehicles - UAV. (2015). Retrieved November 9, 2015, from <http://www.transportrisk.com/uavrcfilm.html>
- Iran starts cloning of American spy drone. (2012, April 22). Retrieved December 3, 2015, from <https://www.rt.com/news/iran-spy-drone-copy-667/>
- James, L. (2014, February 8). How do Beacon and Geo-Fencing Actually Work? Retrieved December 3, 2015, from <http://www.mobiledonky.com/blog/how-do-beacon-and-geo-fencing-actually-work>
- Jansen, B. (2014, June 5). Drones will be revolutionary, but hurdles remain. Retrieved December 1, 2015, from <http://www.usatoday.com/story/money/business/2014/06/05/drones-national-research-council-faa-clarke-lauber/10002007/>

Secondary References

Jenkins, D., & Vasigh, B. (2013, March 1). The economic impact of unmanned aircraft systems integration in the united states. Retrieved November 9, 2015, from https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic_Report_2013_Full.pdf

Kargo, D. (2012). Dad's Toys. Retrieved December 5, 2015, from <https://www.pinterest.com/pin/203365739393483039/>

Karp, A. (2015, October 1). FAA warns of 'a million drones under people's Christmas trees'. Retrieved October 31, 2015, from <http://www.suasnews.com/2015/09/38847/faa-warns-of-a-million-drones-under-peoples-christmas-trees/>

Keller, J. (2014, July 24). U.S. spending on unmanned aerial vehicles (UAVs) to reach \$15 billion by 2020, market researcher says. Retrieved December 1, 2015, from <http://www.militaryaerospace.com/articles/2014/07/igi-uav-forecast.html>

Koebler, J. (2015, October 19). 8 Questions Raised by the FAA's Decision to Register Every Drone in the US. Retrieved November 22, 2015, from <http://motherboard.vice.com/read/8-questions-raised-by-the-faas-decision-to-register-every-drone-in-the-us>

Lerner, M. (2014, August 5). The Chilling Effect of Domestic Spying (T. DeWeese, Ed.). Retrieved December 2, 2015, from <http://americanpolicy.org/2014/08/05/the-chilling-effect-of-domestic-spying/>

Lewis, J., & Caplan, L. (2015, July 28). *Drones to satellites: should commercial aerial data collection regulations differ by altitude?* Retrieved November 16, 2015, from <http://search.proquest.com.er.lib.k-state.edu/docview/1699245726?accountid=11789>

Mahoney, D. (2015, November 10). Aviation insurer offers ground rules for drones. Retrieved November 17, 2015, from <http://www.businessinsurance.com/article/20151110/NEWS06/151119989/aviation-insurer-offers-ground-rules-for-drones-faa-federal-aviation?tags=|71|76|80|83|329|302>

Merriam-Webster Dictionary. <http://www.merriam-webster.com/dictionary/cybersecurity/>

MIMO Radar. (2015). Retrieved December 3, 2015, from http://www.androcs.com/mimo_radar.html

Secondary References

- Mulrine, A. (2015, July 28). Robots in war: Ethical concern, or a help for social ills? Retrieved November 23, 2015, from <http://www.csmonitor.com/USA/Military/2015/0728/Robots-in-war-Ethical-concern-or-a-help-for-social-ills>
- Murphy, M. (2015, November 5). The future of drones is apps. Retrieved November 9, 2015, from <http://qz.com/540559/the-future-of-drones-is-apps/>
- New 50" Mini Telemaster RC Plane Kit Remote Control R/C Airplane 50in Balsa. (2015). Retrieved December 5, 2015, from <http://www.ebay.com/itm/New-50-Mini-Telemaster-RC-Plane-Kit-Remote-Control-R-C-Airplane-50in-Balsa-/181948366992>
- Palermo, E. (2014, July 29). Drones Could Grow to \$11 Billion Industry by 2024. Retrieved December 1, 2015, from <http://www.livescience.com/47071-drone-industry-spending-report.html>
- Perlman, A. (2015, November 22). DJI Introduces New Geofencing System for Its Drones. Retrieved December 3, 2015, from <http://uavcoach.com/dji-introduces-new-geofencing-system/>
- Peterson, S. (2011, December 9). Downed US drone: How Iran caught the 'beast' Retrieved December 3, 2015, from <http://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast>
- Pomerleau, M. (2015, October 28). How to do air traffic control for drones. Retrieved November 3, 2015, from <https://gcn.com/articles/2015/10/28/latas-drone-control.aspx>
- Reagan, J. (2014, December 15). 11 States Enacted New Drone Laws in 2014. Retrieved November 17, 2015, from <http://dronelife.com/2014/12/15/11-states-enacted-new-drone-laws-2014/>

Secondary References

Ribiero, J. (2014, August 20). US senator to introduce proposal for mandatory drone geofencing. Retrieved November 17, 2015, from <http://www.cio.com/article/2973586/us-senator-to-introduce-proposal-for-mandatory-drone-geofencing.html>

Sifton, J. (2012, February 7). A Brief History of Drones. Retrieved December 1, 2015, from [http://www.thenation.com/article/brief-history-drones/Sense and Avoid for Unmanned Aerial Vehicles](http://www.thenation.com/article/brief-history-drones/Sense-and-Avoid-for-Unmanned-Aerial-Vehicles). (n.d.). Retrieved December 1, 2015, from <http://www.frc.ri.cmu.edu/projects/senseavoid/technology.html>

September 11th Flights. (2008, May 21). Retrieved December 2, 2015, from <http://911research.wtc7.net/planes/sept11.html>

SkyGrabber is offline satellite internet downloader. (2008). Retrieved December 2, 2015, from <http://www.skygrabber.com/en/skygrabber.php>

Shukla, M., Chen, Z., & Lu, C. (2015). Distributed Drone Flight Path Builder System. Retrieved November 1, 2015, from <http://europa.nvc.cs.vt.edu/~ctlv/Publication/2015/GISTAM-2015-Proceedings.pdf>

Skaves, P. (2015, April 1). Retrieved October 25, 2015 from http://www.cabaa.com/documents/FAA_Aircraft_System_Information_Security_Protection_Overview_4-1-2015_Jim_Skaves.pdf

Snow, C. (2014, February 6). The Yellow Brick Road of FAA Drone Regulations. Retrieved November 17, 2015, from <http://droneanalyst.com/2014/02/06/the-yellow-brick-road-of-faa-regulations/>

Tesla, C. (2014, June 17). The past and the future of drones. Retrieved November 17, 2015, from <http://www.tumotech.com/2014/06/17/the-past-and-the-future-of-drones/>

Secondary References

The Drones Report: Market forecasts, regulatory barriers, top vendors, and leading commercial applications. (2015, May 27). Retrieved December 3, 2015, from <http://www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2>

Timeline for Domestic Drone Integration. (2012, June 13). Retrieved November 28, 2015, from <https://www.eff.org/document/timeline-domestic-drone-integration>

The Drones Danger. (2015, August 19). Retrieved November 22, 2015, from <http://www.askthepilot.com/the-drone-danger/>

Tomiuc, E. (2012, January 31). Drones – Who Makes Them And Who Has Them? Retrieved December 1, 2015, from http://www.rferl.org/content/drones_who_makes_them_and_who_has_them/24469168.html

Tomkins, R. (2014, May 13). Frost & Sullivan forecasts five-year rise in spending for UAVs. Retrieved December 1, 2015, from http://www.upi.com/Business_News/Security-Industry/2014/05/13/Frost-Sullivan-forecasts-five-year-rise-in-spending-for-UAVs/5631400008680/

UAS / UAV Research and Advisors - Drone Analyst. (2015). Retrieved November 9, 2015, from <http://droneanalyst.com/>

UAV Protect. (2014, December 23). Retrieved December 3, 2015, from <http://www.uav-protect.com/>

UAV Tracking Systems | UAV Tracking & Recovery by Marshall. (2015). Retrieved December 3, 2015, from <http://www.unmannedsystemstechnology.com/company/marshall-radio-telemetry/>

Secondary References

Vintage RC. (2012). Retrieved December 5, 2015, from <http://www.rcuniverse.com/market/item.cfm?itemid=813625>

Wallace, R. (2015, June 16). SciTech Tuesday-First V-1 rockets launched June 1944. Retrieved December 5, 2015, from <http://www.nww2m.com/2015/06/scitech-tuesday-first-v-1-rockets-launched-june-1944/>

Welcome to Homeland Surveillance & Electronics LLC Unmanned Aerial Vehicle (UAV) Website! (2015, September 17). Retrieved November 2, 2015, from <http://www.hse-uav.com/>

Williams, M. (2015, July 28). Amazon proposes drone superhighways in sky. Retrieved December 3, 2015, from <http://www.pcworld.com/article/2953952/government/amazon-proposes-drone-superhighways-in-sky.html>

What is cyberterrorism? (2010, May 1). Retrieved December 3, 2015, from <http://searchsecurity.techtarget.com/definition/cyberterrorism>

What is SCADA (supervisory control and data acquisition)? (2005, September 1). Retrieved December 3, 2015, from <http://whatis.techtarget.com/definition/SCADA-supervisory-control-and-data-acquisition>

What is Schrodinger's cat? (M. Rouse, Ed.). (2014, October 1). Retrieved December 2, 2015, from <http://whatis.techtarget.com/definition/Schrodingers-cat>

Whitlock Craig Whitlock, C. (2014, January 22). Crashes mount as military flies more drones in U.S. Retrieved December 1, 2015, from <http://www.washingtonpost.com/sf/investigative/2014/06/22/crashes-mount-as-military-flies-more-drones-in-u-s/>