Unmanned Aerial Insecurity

Third Party Hostile Takeovers of Unmanned Aircraft: Law, Policy, and Implications for Business

Donna A. Dulo MS, MA, MAS, MSSE, MBA, JD, PhD(c)
U.S. Naval Postgraduate School
Embry-Riddle Aeronautical University Worldwide
President, Unmanned Aircraft Safety & Security Society, Inc.
Introduction
IA Fundamentals
UAS as a System of Systems
UAS Hostile Takeover Threats
Tort Liability & Criminal Culpability
Critical Infrastructure Protection
Discussion
UAS integration into the national airspace opens up a variety of legal issues that must be addressed in light of both UAS airframe and payload technologies.

Legal Issues Arising with Civilian UAS Integration

- Payload & Cargo
- Specific Legal Issues
- 1st, 2nd, 4th, 5th, 10th, 14th Amendment Issues
- Safety Issues
- Privacy Torts
- Civil Liability & Criminal Culpability Issues
- Security Issues
- Product Liability, Risk, & Insurance Issues
- Administrative/Airspace Issues
Safety Issues: Collision Avoidance, Ground Safety, Operator Safety

Security Issues: Data Security, Interception Prevention, Hostile Takeover

Privacy Issues: Personal Privacy, Data Privacy

Payload Specific Issues: Hazards (Pesticides), Freight Regulations, etc.

Administrative Issues: Aircraft Registration, Operations Permits, etc.

2nd Amendment Issues: Property Protection, Livestock Protection, etc.
Complexity of Security Issues

Complexities arise as issues compound with each other or conflict with each other:

Data Security + Data Privacy = Compound Issue

Payload Issues + Safety Issues = Compound Issue

Safety versus Privacy = Compound Issue

It is vital to view UAS integration in the national airspace as a multi-issue situation.
Many facets of UAS security: Data security, physical security, personnel security, systems security, operations security.

Each area has its own discipline.

Example: Physical security = aircraft security, ground station security, hangar security, equipment security, etc.

Our focus will be UAS cyber security and information assurance areas and the threat of hostile takeover.
Cascading Legal Effect of Security

Security cascades into other areas rapidly making it a central issue in UAS operations.

- Data Security Breach ➔ Privacy Tort ➔ Civil Liability
- Software Vulnerability ➔ Safety Issue ➔ Product Liability
- Data Integrity Issue ➔ Safety Issue ➔ Criminal Culpability
Unmanned Aircraft
Information Assurance
Fundamentals
Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542]

"A loss of confidentiality is the unauthorized disclosure of information"

UAS security measures examples: restricted access to data through encryption, employment of pilot and user authentication methodologies, anti-spoofing technologies
Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., SEC. 3542]

"A loss of integrity is the unauthorized modification or destruction of information"

UAS security measures examples: encrypted data signatures, stratified authentication to restrict access, hardened onboard data storage systems, anti-spoofing technology
Availability

"Ensuring timely and reliable access to and use of information...”
[44 U.S.C., SEC. 3542]

"A loss of availability is the disruption of access to or use of information or an information system"

UAS security measures examples: redundant ground control systems, redundant communication systems, backup navigation systems, backup data systems including real time backups
Full Spectrum UAS Information Assurance

- UAS Information Systems Protection
- Information Protection (Assurance)
- Data Protection

UAS INFORMATION SYSTEMS

{ INFORMATION }

{ DATA }

- Secrecy
- Integrity
- Authenticity

- Availability
- Confidentiality
- Integrity
- Authenticity
- Non-Repudiation

Personnel Security
Computer Security
Physical Security
Emission Security
Operations Security
Network Security
Database Security
Aircraft Security
Communications Security
Ground Station Security
Full Spectrum UAS Information Assurance

UAS Operations

Unmanned Aircraft

Information Assurance

Data Security

Information

Data

Datum

Char

Byte

Bit

Complexity

Risk
**Threats, Vulnerabilities, & Risk**

### Threat
Capabilities, intentions and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system.

### Vulnerability
Weakness in an information system, cryptographic system, security procedures, hardware, software or other components that could be exploited.

### Risk
A combination of the likelihood that a threat will occur, the likelihood that the threat will result in an adverse impact, and the severity of the resulting impact.

### Residual Risk
The portion of risk that remains after security measures have been applied.
Defense in Depth

Intruder = Vulnerability

Layers of Defense
The UAS as a System of Systems
UAS as a System of Systems

- Fixed Wing UAV
- Rotary Wing UAV
- Tilt Rotor UAV
- Lighter Than Air UAV
An unmanned aircraft is not merely an aircraft but in systems engineering terms, a “system of systems” consisting of the aircraft, the ground station, the GPS satellite constellation, the communication infrastructure (L-Band, C-Band), the launch & recovery infrastructure, the personnel, etc.

All aspects of these systems must be secured and maintain information assurance, as data is constantly transmitted in the form of information and commands.
Hostile Takeover Cyber Threats to UAS
As can be seen UAS operations have computational and communicational complexity giving rise to increasing risk to information assurance threats.

Attacks can occur in aircraft and ground station:

- Embedded Systems
- Software
- Hardware
- Network Components
- Combination of the Above (Blended Threats)
The Hostile Takeover Threat Spectrum

- Embedded Systems Threats
  - Wireless Hack Threats
  - GPS Spoofing
  - Signal Jamming
- Malware/Viruses/Worms
Embedded security is a major concern for UAS (as well as manned aircraft and satellite systems)

Embedded systems tend to have generic hardware & software, which in many cases do not have a development process with mandatory security protocols (Example: Computer chips from China)

This can result in built in vulnerabilities in the chips (integrated circuit hardware) and the software that drives the chips.

The interconnectivity of the system of systems makes these vulnerabilities pervasive throughout the entire system. (Example: A virus in a UAS chip can spread to the ground station or a networked UAS)
Embedded systems such as Integrated Circuits (IC) or Programmable Logic Controllers (PLC) can inflict physical as well as informational damage. (Think Stuxnet)

Controllers are real time computer chips that have the potential to manipulate electrical outputs based on the programming conditions within the controller or integrated circuit.

The chips or controllers are connected to electrical devices such as pumps, motors, sensors, or other electromotive devices which have a specific electrical purpose controlled by the chip or circuit.

Through computational logic, the laws of physics, as well as the laws of information technology, enable the fusion and functionality of the controller, the computational logic, the software, and the UAS electronics to operate in a viable manner.
Cyber attack acts impede the physical processing of the controllers; this is what makes them dangerous and deadly.

Malicious manipulations of the controllers can lead to logic issues resulting in software corruption or in the worst case scenario physical damage to the hardware of the system due to erroneous electrical impulses in the physical manifestations of the logic carried out in the electronics attached to the controllers.

The result = damage to the UAS = catastrophic failure or malicious control of the UAS from rearranged logic signals
Case Study

The Actel ProASIC chip in the new Boeing 787 had a backdoor that could allow chip to be taken over via Internet

A person using the entertainment system in the passenger cabin could take over the avionics and control the aircraft!
Combating Embedded Systems Threats


Development Based Tools: Formal Methods Based Specifications and Tools during Requirements & Development, Testing, Verification & Validation

Vulnerability Assessment Tools and Techniques by Vendors and UAS Systems Manufacturers

Strategic Countermeasures and Fault Tolerance Mechanisms Introduced by Vendors, Manufacturers and Operators

Error Detection & Handling in the Software
Viruses and Malware

Viruses, Worms and other forms of software based malware are critical threats for UAS systems: aircraft and ground stations

Viruses hit the US military drone fleet in 2011 including the Predator and Reaper drones through ground station viruses

The keystrokes of operators were logged and sent to outside (potentially enemy) sources

Despite repeated efforts, the viruses kept coming back onto the systems

Key Logging Malware the central cause of the incident
In 2011 Iran captured a US RQ-170 Sentinel stealth drone

Iran claims it exploited a vulnerability in the software and caused the system logic to allow access to flight controls

In 2009 Shiite militants in Iraq were found to have downloaded live unencrypted video streams from American predator drones

These videos were captured through software exploits of the system

The equipment used by the militants was valued at less than $100
Combating Malware & Software Exploits

Hardening software systems

Advanced Malware Protection Systems

Advanced Encryption on all live data streams

Ground station malware protection systems

Network based intrusion detection and firewalls

Policies and procedures

Personnel security
GPS civilian signals are open standard, free accessibility signals, with no form of authentication, and are unencrypted!

Transparency and predictability have created a major weakness – the ability to be spoofed which means it can be replicated easily

A UAS can thus be hijacked and crashed by spoofing its live GPS signal
Types of GPS Spoofing

Live Satellite Signal Spoofing: user a GPS signal generator, like a fake satellite, to synthesize a navigationally consistent signal set and overlay and substitute them for the actual satellite signals

Software Code Spoofing: The receiver is actually uploaded with malware which makes it appear as functioning normally but the location of the UAS is altered

Differential Corrections Spoofing: the digital corrections signal is actually spoofed. DCS enhances GPS accuracy to 1 meter so this is a limited attack
GPS spoofing countermeasures are still being researched as they are complex and costly

Fix the satellite vulnerability (Air Force is looking at anti-spoofing module)

Monitor absolute and relative strength of GPS signal in the UAS

Check time intervals and do time comparisons

Monitor satellite signal strength

Monitor satellite ID codes and number of satellite signals received from the constellation
Jamming is a major issue with the cyber-physical aspects of unmanned aircraft.

Jamming signals can block:

1. GPS Signals
2. Communication Signals
3. Command & Control Signals
4. Anti-Collision System Signals
Signal Jamming

Case Study

In 2012 the South Korean military lost direct control of its S-100 Reconnaissance Drone

The drone crashed into the ground station killing one and injuring several

The loss of control is attributed in part to North Korean jamming signals
Countering Signal Jamming

High Performance GAJT (GPS Anti-Jamming Technology)

Communication systems anti-jamming technology

ECCM (Electronic Counter-Counter Measures)

Multiple signal channels

Polarization to filter out unwanted signals
Wireless Hacks

Unmanned aircraft are aircraft on a wireless tether

Network exploits and hacks are possible, resulting in a takeover of the aircraft

- Packet injection
- Re-authentication
- Script code injection (Example: Javascript)
- Malicious Freeware
Preventing wireless hacks is difficult but basic network security principles apply as a first layer of defense.

In ground station as well as on the aircraft:

- Anti-injection code
- Strong Encryption
- Defense in Depth
Implications

Embedded Systems Threats

- Wireless Hack Threats
- Malware/Viruses/Worms
- GPS Spoofing
- Signal Jamming
Criminal Culpability and Civil Liability
Criminal Culpability and Civil Liability

Will failure to provide security in a UAS which results in an accident result in a crime or a tort or both?

Case Study

SabreTech Inc was charged with 110 counts of murder and 110 counts of manslaughter due to the improperly packed oxygen canisters that caused a ValueJet DC-9 to crash in the Everglades in 1996.

Extensive civil action and FAA enforcement also resulted.

This was the first time a US aviation company was convicted of criminal charges arising out of a crash.
Negligence and Liability: negligence is the most common tort in manned aircraft litigation, will it become so in unmanned litigation?

Negligence is failing to do an act that a reasonably careful person would do to protect others from harm. The elements of negligence are:

1. a duty to be reasonably careful
2. a failure to be reasonably careful
3. which is the proximate cause of
4. injury to another person or their property

Would someone be negligent for failing to provide security where the failure results in a catastrophic failure of the UAS resulting in damage or injury?
Where the plaintiff can prove that an accident resulted from a violation of a Federal Aviation Regulation that is intended to prevent such accidents, the violation constitutes negligence as a matter of law.

The problem is that there are no Federal Aviation regulations on information Assurance!

Res Ipsa Loquitur (the facts speak for themselves) may be relied upon if the UAS was under the exclusive control of the defendant and the accident was not the fault of the plaintiff and the accident was not something that normally happens unless the defendant was negligent

Strict liability for defective product?

Strict liability for ultra hazardous activity?
U.S. Critical Infrastructure Protection
The critical infrastructures of the United States have only been recently, in the past decade and a half, been recognized as a target for cyber attacks.

However, during this time the government has acted, albeit slowly to ensure that the national critical infrastructure is adequately protected as a national security measure.

In this section we will briefly discusses the acts and directives meant to protect the nation's critical infrastructure from cyber attacks, focusing on the aviation sector.

Understanding the US critical infrastructure protection directives is critical in UAS security and information assurance implementation.
The **Presidential Policy Directive PPD-21** that President Obama signed on February 12, 2013 entitled "Critical Infrastructure Security and Resilience" advanced a "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructures".

This directive seeks three specific strategic imperatives that will drive the Federal approach to strengthen the security of the critical infrastructure:

- Refine and clarify functional relationships across the Federal government to advance the national unity of effort to strengthen the critical infrastructure security and resilience;

- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and

- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.
Note the increased emphasis on cyber security as compared to the earlier laws and directives concerning critical infrastructure.

The PDD-21 also develops 16 critical infrastructure sectors and assigns oversight of these sectors to a Federal Agency.

The critical infrastructure area of “Transportation Systems” is a distinct area and is assigned to both the Department of Transportation and the Department of Homeland Security.

This has significant implications for UAS security development, implementation and enforcement.

Thus the DHS, DOT as well as the FAA will have a significant set of inputs into UAS security issues, regulations, and matters in general.
UAS in the Critical National Infrastructure
UAS security is an emerging field as is UAS technology and UAS law

Security must be placed high in importance with safety and privacy

Information Assurance and Security professionals must be kept in the loop along with legal and aviation professionals

New information assurance and security technology must be followed carefully and merged into the UAS arena

Security affects all areas of UAS operations and as such must be treated as a compound issue

Security is everyone’s responsibility
Questions?
References


Humphries, T. (July 18, 2012). Statement on the Vulnerability of Civil UAV and Other Systems to Civil GPS Spoofing