Unmanned Aerial Systems

Information Assurance & Security

Unmanned Insecurity:
The Safety and Privacy Issues of Unmanned Aircraft Information Assurance

Donna A. Dulo MS, MA, MSCS, MAS, MBA, JD, PhD(c)

Unmanned Aircraft Safety & Security Society, Inc.

Legal Issues Arising with Civilian UAS Integration

1st, 2nd, 4th , 5th, 10th, 14th Amendment Issues

Payload & Cargo Specific Legal Issues

Safety Issues

Product Liability, Risk, & Insurance Issues

Civil Liability & Criminal Culpability Issues

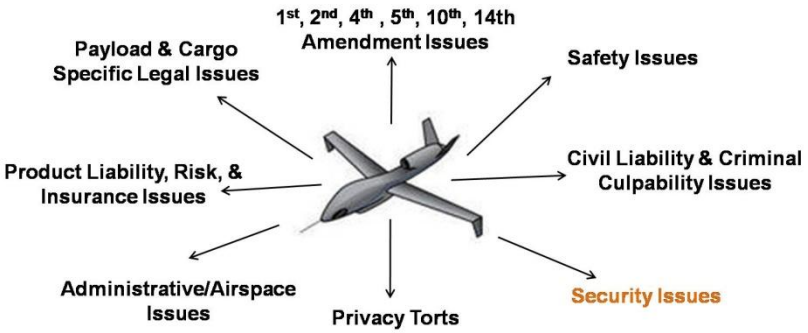
Administrative/Airspace Issues

Privacy Torts

Security Issues

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



Safety Issues: Collision Avoidance, Ground Safety, Operator Safety

Security Issues: Data Security, Interception Prevention, Hostile Takeover

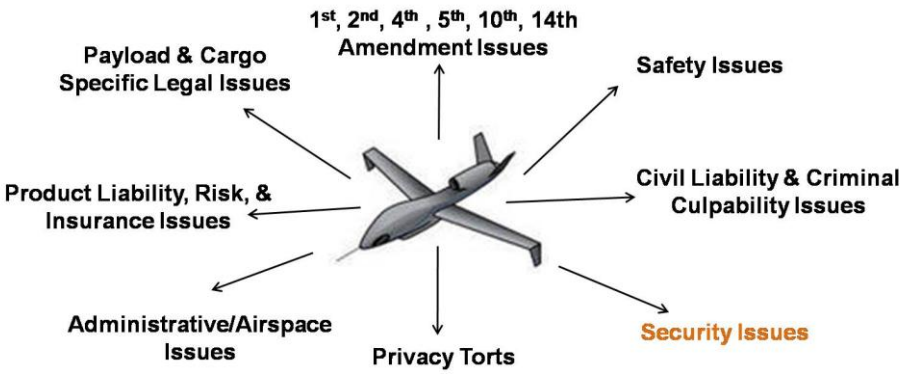
Privacy Issues: Personal Privacy, Data Privacy

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 Technical 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-legal and multi-technical issue situation.

Many Facets of Security

Many facets of UAS security: Data security, physical security, personnel security, systems security, operations security.

Information Assurance is linked to all of them.

Each area has its own discipline.

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

Our focus will be UAS data security and information assurance areas.

Cascading 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**

Information Assurance Fundamentals

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

Information Assurance Fundamentals

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

Information Assurance Fundamentals

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

UAS Information Systems Protection

- Personnel Security
- Computer Security
- Physical Security
- Emission Security
- Operations Security
- Network Security
- Database Security
- Aircraft Security
- Communications Security
- Ground Station Security

Information Protection (Assurance)

INFORMATION

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

Data Protection

DATA

Secrecy Integrity Authenticity

Full Spectrum UAS Information Assurance

Complexity

Risk

UAS Operations

Unmanned Aircraft

UAS Info Systems Security

Information

Information Assurance

Data

Datum

Data Security

Char

Byte

Bit

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.

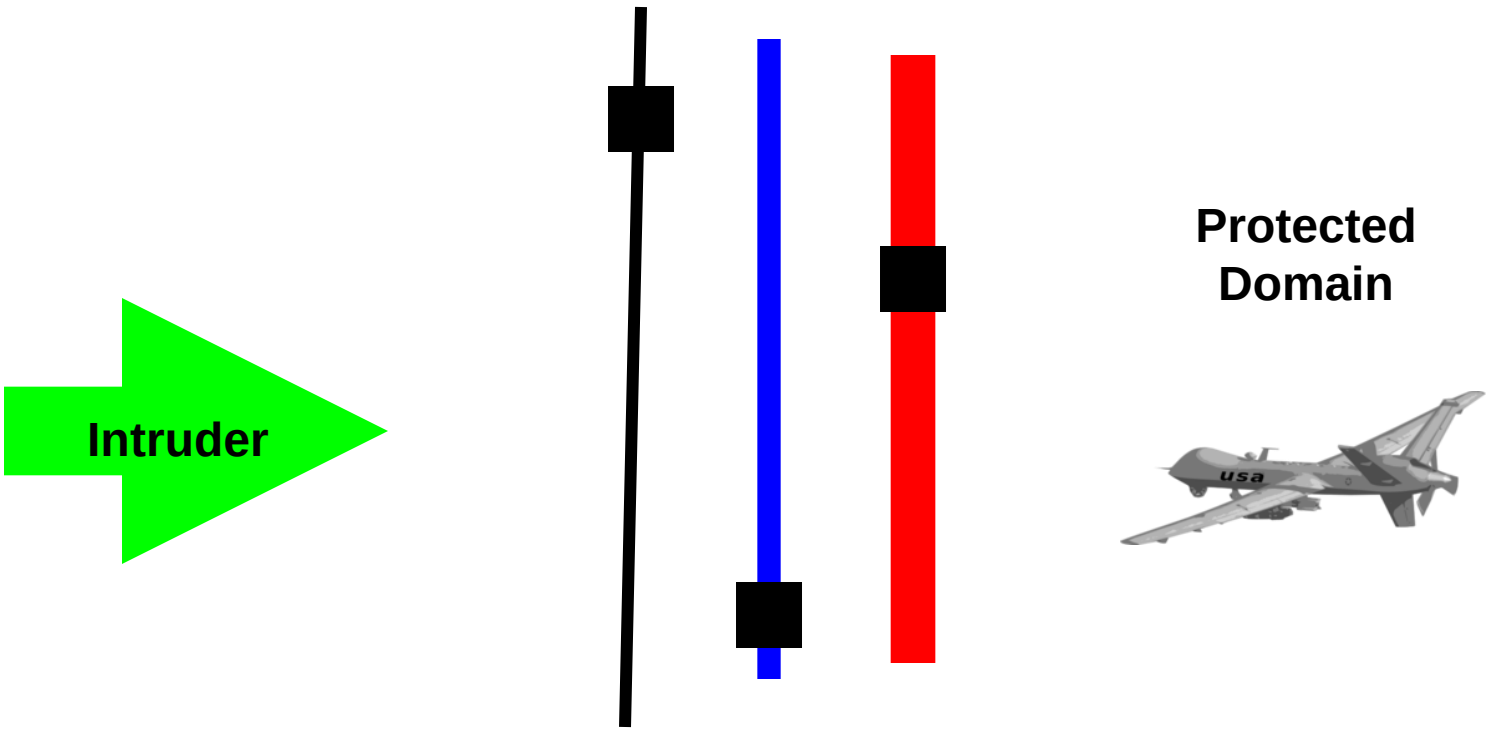
RISK

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



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

UAS as a System of Systems

An UAS 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.

The following technical diagrams demonstrate the critical need for information assurance and system security in complex UAS operations.

Information Assurance Threats to UAS

UAS Information Assurance Threats

As can be seen UAS operations have computational and communicational complexity giving rise to increasing risk to information assurance threats.

Attacks can occur in:

- **Embedded UAS Systems**
- **Software**
- **Hardware**
- **Combination of the Above**

Embedded Systems Threats

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 Threats

Cyber attack acts impede the physical processing of the controllers; this is what makes it 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

Embedded Systems Threats

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!

Viruses and Malware

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

Software Exploits

In 2011 Iran captured a US RQ-170 Sentinel stealth drone

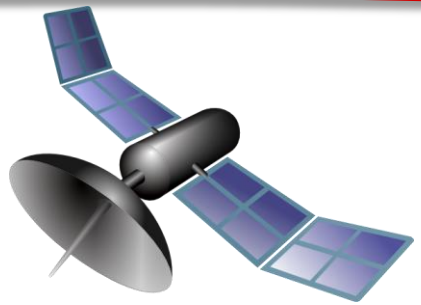
Iran claims it exploited a vulnerability in the software and caused the system logic to allow access to flight controls

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

GPS Spoofing



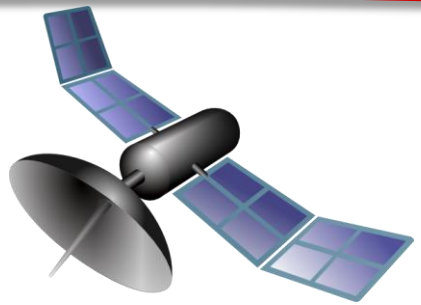
GPS civilian signals are open standard, free accessibility signals

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

This vulnerability was demonstrated by Professor Todd Humphreys of University of Texas at Austin & he testified to Congress on this vulnerability

The demonstration proved that a UAS could 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

UAS Information Assurance Threats

Overall, research and awareness is key in the developing realm of UAS information assurance and security

Information assurance starts from manufacturing and ends with daily operational security and awareness

Legal, information assurance, and aviation professionals need to push forward on the area of information assurance in the future to ensure it stays in the forefront of UAS operations

Continuing education and training in IA and security are vital to maintain UAS security

U.S. Critical Infrastructure Protection

UAS and Aviation 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

UAS and Aviation Critical Infrastructure Protection

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.**

UAS and Aviation Critical Infrastructure Protection

The PPD-21 places a significant emphasis on research and development of security for critical infrastructure, particularly the cyber infrastructure through :

- **Promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;**

- **Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;**

- **Facilitating initiatives to incentivize cyber security investments and the adoption of critical infrastructure design features that strengthen all hazards security and resilience; and**

- **Prioritizing efforts to support the strategic guidance issues by the Secretary of Homeland Security.**

UAS and Aviation Critical Infrastructure Protection

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.

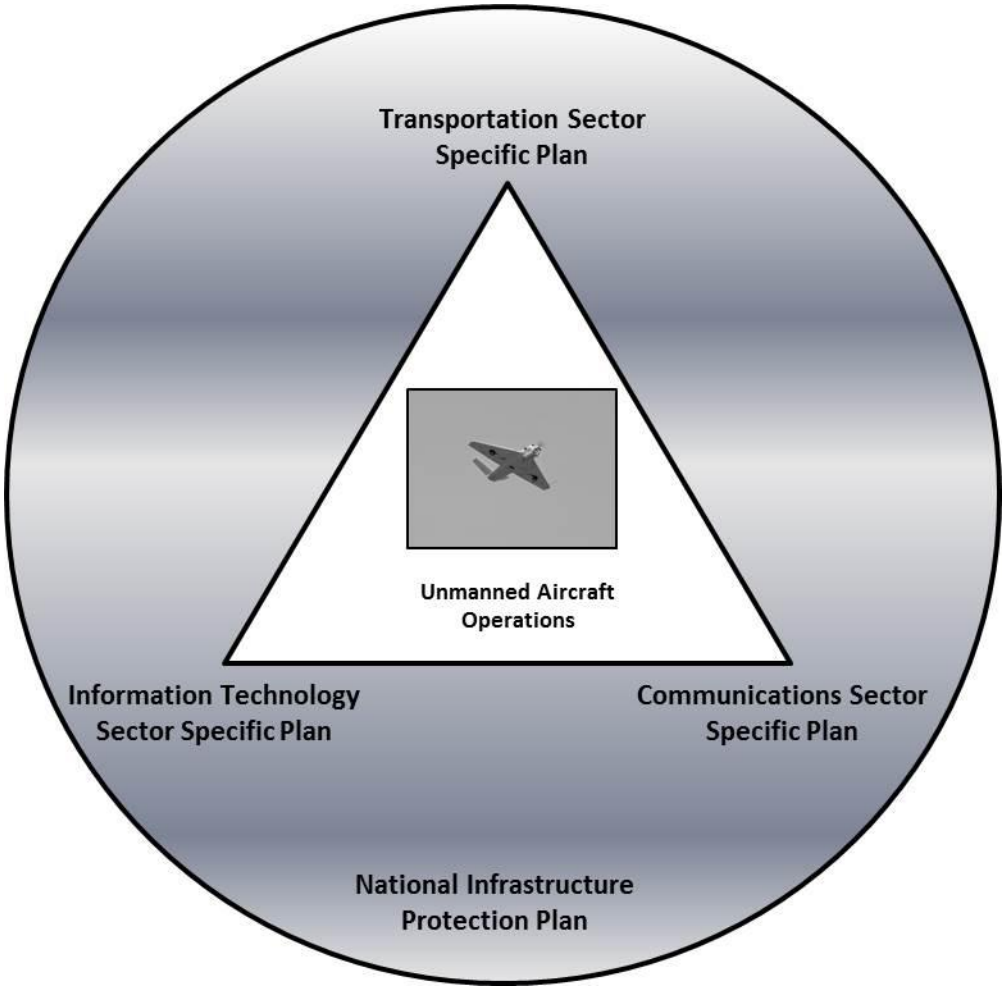
The critical infrastructure area of "Transportation Systems" is a distinct area and is assigned to both the Department of Transportation and the Department of Homeland Security

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

It is wise to keep an eye on the critical infrastructure developments at the federal level in this arena to see the trends in the security aspects of UAS implementation and integration into the national airspace

UAS in the Critical National Infrastructure



Conclusion

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

The White House. (May 22, 1998) Presidential Directive PDD/NSC-63. Critical Infrastructure Protection. Washington, DC.

42 USC Section 5195c. (October, 2001). Critical Infrastructures Act of 2001.

The White House. (February, 2003). National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Washington, DC.

The White House. (February 12, 2013). Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Washington, DC.

Comision De Investigacion De Accidentes E Incedentes De Aviacion Civil. "Accident Involving Aircraft MD DC-9-82 (MD-82) Registration EC-HFP, Operated by Spanair at Madrid Barajas Airport on 20 August 2008". Interim Report A-032/2008, August 4, 2009.

Hamilton, J. (2011). Practical Aviation Law 5th Edition. Newcastle: ASA Publishing.

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