UAS FORENSICS FRAMEWORK (UAS FFWK)

Presented by: Nagi Mei, DSc

September 23, 2020

About Me

Over 14 years of experience in IT and security management

CISM, Sec+, PMP, PMI-ACP, SSM, CSM, ITILv3

DSc Cybersecurity, MBA, MS ITS, BS IS – Digital Forensics

Dissertation: An Approach To Unmanned Aircraft Systems Forensics Framework

Articles: Mitigating Implanted Medical Device Cybersecurity Risks & An Integrated Framework for Sensing Radio Frequency Spectrum Attacks on Medical Delivery Drones

Passionate about learning, team building, and problem solving

Introduction

- Increase of drone usage in public areas, a framework needed to analyze recovered unauthorized consumer drones trespassing into the National Airspace System (NAS)
- Private industry uses drones for recreational and legal activities
- Threat actors can weaponize drones to attack government facilities, transport contraband into prisons, and harm private citizens
- Criminals can use drones to deliver drugs, invade privacy, and perform terrorist acts
- Customized drones can increase the complexity of forensic analysis – need a systematic framework
- Review of evidence collection techniques in forensic analysis to produce admissible evidence for the cybercrime

FAA Drone Sightings [1]

Year	# by State
2014	43
2015	1,210
2016	1,760
2017	2,121
2018	2,308
2019	2,152
2020	781
Total	10,375

Unauthorized Drone Operations

- FAA published reports of drone sights, starting in November 2014
- Reported drone sightings of 100+ per month since May 2015
- 781 drone sightings from January 2020 to June 2020
- Drone sightings are the reported cases – could be many more unreported cases
- Per DHS, the number of drones used in U.S. will increase from 158,000 in 2018 to 451,000 by 2022
- Incorrect usage of the drones might result in dangerous and life-threatening accidents
- Licensed or unlicensed remote pilot can be
  - a clueless drone operator unknowingly fly an aircraft into a restricted area
  - a careless drone operator with an understanding of the regulations but still operate recklessly
  - a criminal drone operator is posing a malicious threat to public safety

[1] https://www.faa.gov/uas/resources/public_records/uas_sightings_report/

An Approach To Unmanned Aircraft Systems Forensics Framework

Reasons for the Study

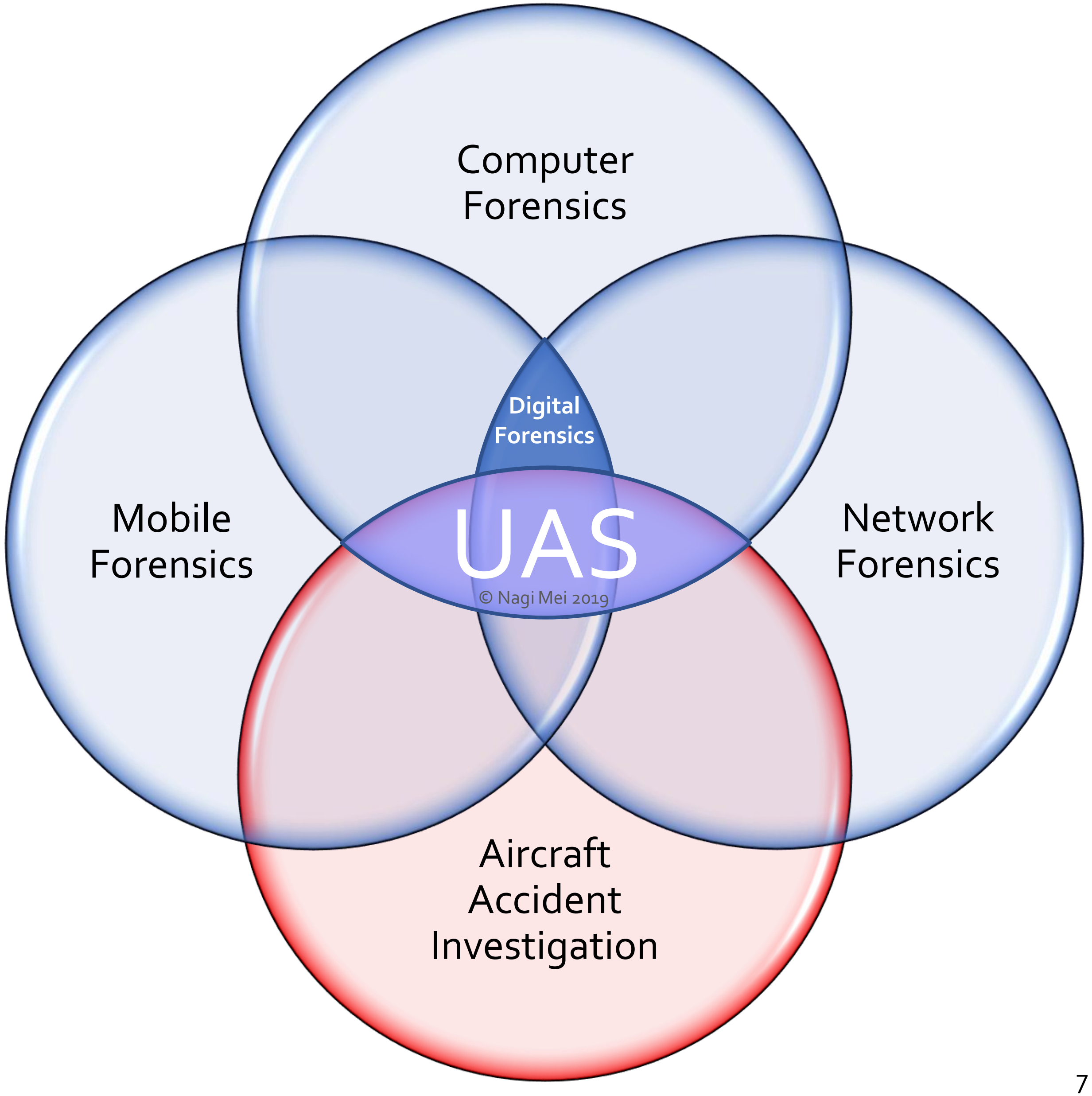
- Forensic investigators did not have a standard UAS forensics framework
- Without a standard framework, investigators might perform different overlapping types of forensic examinations
- Identify and evaluate frameworks, tools, and regulations investigators use to perform UAS forensics
- Identify common criteria in UAS forensics guidelines to determine if a single framework is needed for UAS forensic examiners
- Few studies exist on the need for a standard UAS framework and FAA UAS Regulations and Policies
- Absence of policies for integrating UAS into the NAS left law enforcement without a standard process for handling drone violations
- Knowledge of federal and state regulations will help support the credibility and admissibility of evidence in the courts
- Benefit society as research may contribute diligent forensic investigations in the justice system

Terminology

- Drone – small UAV, weighing under 55 pounds
- Unmanned Aircraft System (UAS) – drone, remote pilot, control mechanism, and media storage
- Digital forensics – investigative review of computers, network devices, and storage devices
- Digital/multimedia Evidence – most drones have a camera with audio and video capabilities
- Expert testimony – SME as witness testimony based on valid scientific reasoning
- Forensic investigation – systematic and legal analysis of evidence
- Model Aircraft – clearly "invented, used, or designed" and capable of flying for recreational purpose within the hobbyist's visual line-of-sight
- National Airspace System (NAS) – Controlled Airspace, Uncontrolled Airspace, Special Use Airspace, and Other Airspace Areas
- Remote Pilot in Command or Remote Pilot – drone operator responsible for the operation of the UAS
- Small UAS Rule (FAA Part 107) – drone flown during daylight under 100 mph and below 400 feet; must be within the visual line of sight, yield to manned aircraft, and not fly highly populated areas

UAS Forensics

- Digital Forensics
  - Computer Forensics
  - Mobile Forensics
  - Networks Forensics
- Aircraft Accident Investigation



An Approach To Unmanned Aircraft Systems Forensics Framework

Scope of Research

- Identify common frameworks used for UAS forensics and aircraft accident investigations
- Consumer drones, not large military drones
- Target population was computer, network, mobile, and aircraft accident investigators who have conducted UAS forensics in the U.S. and its territories
- Local law enforcement procedure for reporting unauthorized drone use

Drones in Historical Use

- 1850s - 1944
  - Earlier UAVs were developed for military use in hazardous environments where human could not operate
- 1946 - 1990s
  - Used for gathering weather data, reconnaissance, and simulate a combat aircraft
- 1990s - 2010s
  - Large-scale UAV became less known to non-government individuals after 1990
  - Small-scale drones gained popularity in the consumer and commercial markets in the early 2010s

Drones for Government Use

- Surveillance and reconnaissance patrol
- Military weapon
- Counter-UAS
- Law enforcement
- Search and rescue emergency response
- Ad hoc wireless communications

Drones for Commercial Use

- Merchandise delivery
  - Amazon Prime Air
  - Medical supplies
- Agriculture assessment
  - Crop dusting
  - Capturing images of the fields
- Structural monitoring
  - Detect structural faults in buildings, railway tunnels, and bridges

Drones Misused by Criminals and Careless Consumers

- Invasion of privacy
  - DHS considered a drone used for surveillance as intentional disruption or invasion of privacy on other individuals
- Contraband transport
  - Illegal uses of the drone were to transport contraband into prisons by an accomplice
- Counter-surveillance of legal authorities
  - Illegal uses of drones and counter-surveilling of police activity by drug criminals have also been observed
- Weaponized drones
  - A weaponized drone is capable of dispersing chemical material and transporting explosive payloads
  - Criminals, terrorists, or lone actors can use drones to carry out malicious acts with specific intentions

An Approach To Unmanned Aircraft Systems Forensics Framework

Rules & Regulations Related to UAS

- Federal Laws for UAS
  - FAA Modernization and Reform Act of 2012, 49 U.S.C. § 40101
  - FAA Extension, Safety, and Security Act of 2016, 49 U.S.C. §40101
  - FAA Reauthorization Act of 2018, 49 U.S.C. §§44801-44810
  - Transportation, 49 U.S.C. §§ 46307. National Defense Airspace
  - Transportation, 49 U.S.C. § 46306. Registration violations involving aircraft not providing air transportation
  - Preventing Emerging Threats Act of 2018, 6 U.S.C. § 210G. Protection of certain facilities and assets from unmanned aircraft
- Federal Rule of Evidence 702
  - The U.S. FRE Rule 702 necessitated the courts to assess the reliability and validity of scientific expert testimony

Notable FAA UAS Regulations

- Part 107 Small Unmanned Aircraft Systems (2018)
  - Subpart A – General 14 C.F.R. §§107.3-107.9

    The definitions of the UAS team include remote pilot in command, visual observer, and any person controlling the flight; the civil penalty for altering records and reports for fraudulent purposes; the remote pilot must provide UAS certificate with small UAS rating to authorities upon request; and mandatory report accidents causing serious injury or property damage greater $500.
  - Subpart B – Operating Rules §§107.11-107.51

    The drone operator must hold a remote pilot certificate to fly commercial, fly in safe conditions, have no physical or mental condition which would interfere with safe operations. The operator cannot fly recklessly to endanger people or property, operate from a moving vehicle or aircraft, fly under the influence of alcohol or drugs, or fly at night. The operator must maintain visual line of sight, not load hazardous material in the drone, and yield to manned aircraft. The operator cannot fly over people, in or near restricted areas and airports unless authorized by Air Traffic Control (ATC), and must conduct a preflight inspection. The drone must fly under 100 miles per hour and under 400 feet above ground level (AGL) and maintain a visual line of sight from under three statute miles. The drone must stay under 500 feet below clouds and 2,000 feet horizontally from clouds.
  - Subpart C – Remote Pilot Certification §§107.53-107.79

    The section pertains to qualifications to obtain the Part 107 remote pilot certification in a small UAS rating. The applicant must be at least 16 years of age and demonstrate aeronautical knowledge.
  - Subpart D – Waivers §§107.200-107.205

    The remote pilot may request waivers to fly the drone from a moving vehicle or aircraft, fly at night, operate a swarm of network drones, fly over people, or fly in dedicated airspace.

https://www.congress.gov/bill/115th-congress/house-bill/302

An Approach To Unmanned Aircraft Systems Forensics Framework

Standards and Guidelines

- FAA formed the Drone Advisory Committee (DAC) [1]
- NIST maintained repository in Computer Forensic Reference datasets (CFReDS)
- ISO formed a Technical Committee in 2014 under ISO/TC 20/SC 16
- Organizations headed in the right direction but need more standards and guidelines development

[1] https://www.federalregister.gov/documents/2020/09/11/2020-20082/drone-advisory-committee-dac-notice-of-public-meeting

Models and Frameworks

- Investigative Models
  - Aircraft Accident Investigations (NTSB)
  - Competence framework for aircraft accident investigators
- Drone Forensics Framework and Models
  - Drone Forensic Framework
  - DRone Open source Parser (DROP)
  - UAV Forensic Investigation Process
- Digital Forensics Models
  - Digital Forensics Investigation Models
  - Cyber Forensic Investigation Process Model
  - Framework for Digital/Multimedia Evidence

Study Participants

- In the aircraft accident investigation and digital forensics community
- Forensics examiners who has conducted forensics on drones
- Conducted via survey online
- 63 initial participants
  - 16 did not finish survey
  - 32 did not qualify
  - 15 finish survey

Survey, Response Rate by Partial, Disqualified, and Complete

	Response Rate	
Participation Response	Frequency	Percent
Partial Responses	16	25.4%
Disqualified Responses	32	50.8%
Complete Responses	15	23.8%
Total	63	100.0%

Demographics

- Location, top three primary locations where UAS investigations were conducted
  - Ohio (13.3%)
  - Texas (13.3%)
  - Undisclosed U.S. territories (13.3%)
- Education
  - Associate degree (6.7%)
  - Bachelor's degree (20%)
  - Master's degree (53.3%)
  - Doctorate (20%)
  - No participants less than an Associate degree

- Organization Type:
  - U.S government (40%)
  - Publicly held company (6.7%)
  - Private company or self-employed (46.7%)
  - Academic institution (6.7%)
- Experience
  - 1 to 4 years (13.3%)
  - 5 to 8 years (13.3%)
  - 9 to 12 years (6.7%)
  - Over 12 years (66.7%)
  - No participants with less than 1 year

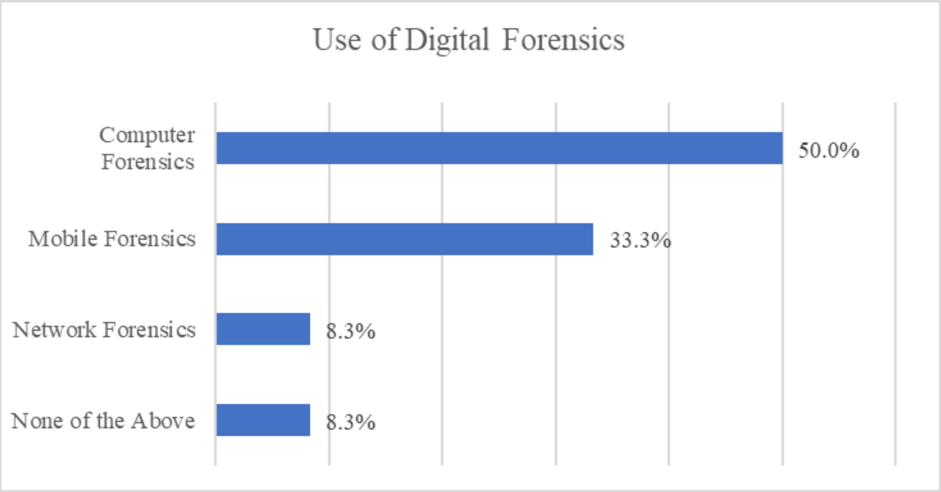
Certifications

- FAA Part 107 Remote Pilot certification:
  - Certified (40%)
  - Not certified (60%)
- Investigation certifications:
  - AccessData Certified Examiner (16.7%)
  - Certified Computer Examiner (6.7%)
  - EnCase Certified Examiner (16.7%)
  - Private investigator license (16.7%)

Findings – 1

UAS forensics investigations and the use of digital forensics (computer, network, and mobile forensics) frameworks

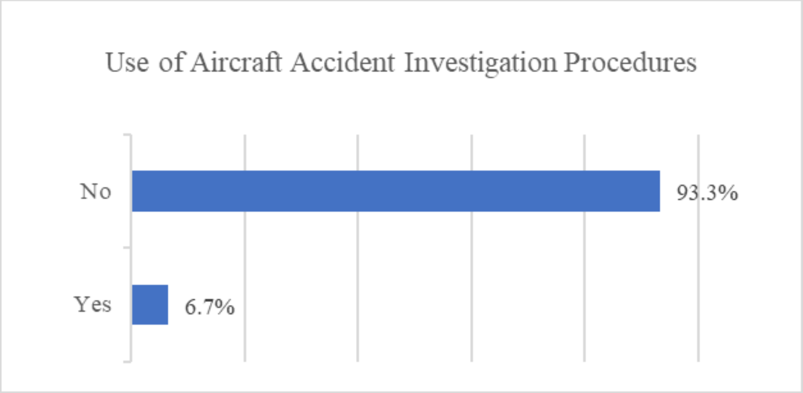
- Have you used any of the following forensic disciplines to analyze a drone, UAV, UAS, or model airplane?



Findings – 2

UAS forensics investigations and the use of aircraft accident investigations procedures

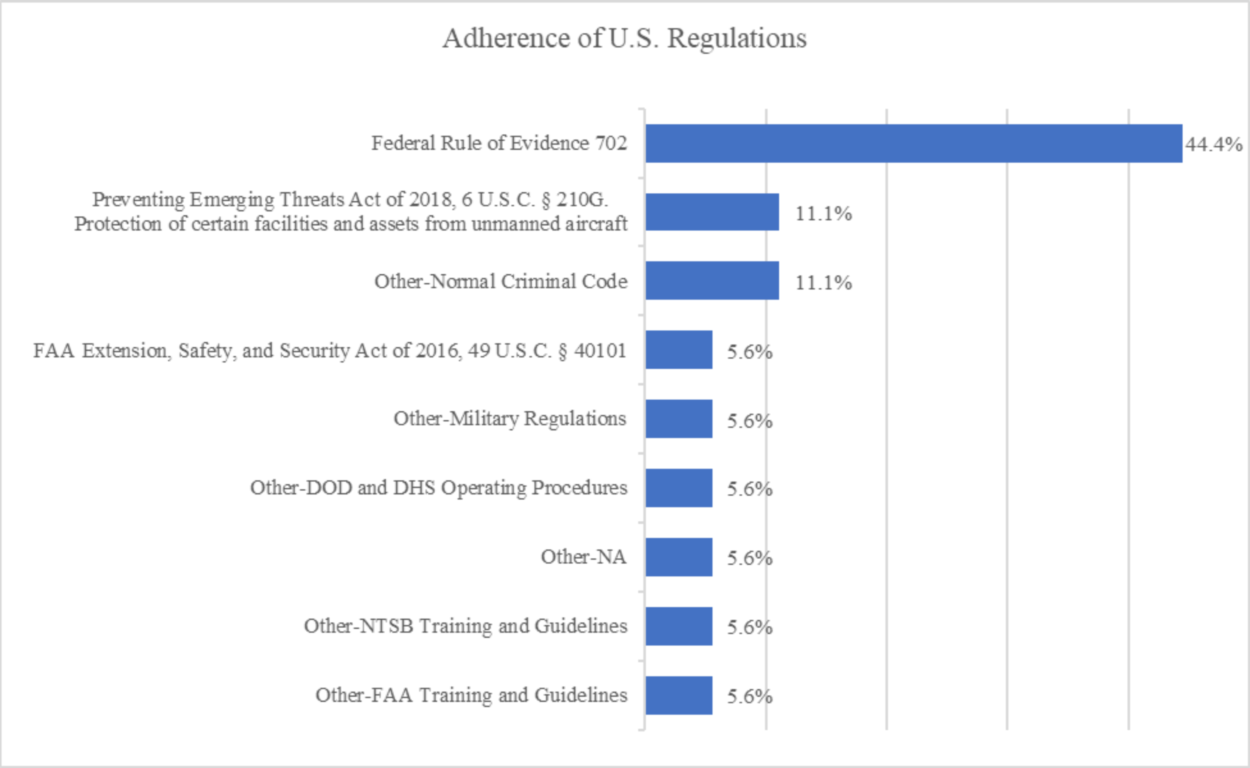
- Have you conducted or reported an aircraft accident investigations to NTSB regarding a drone-related investigation?



Findings – 3

UAS forensics investigations and U.S. Federal Regulations

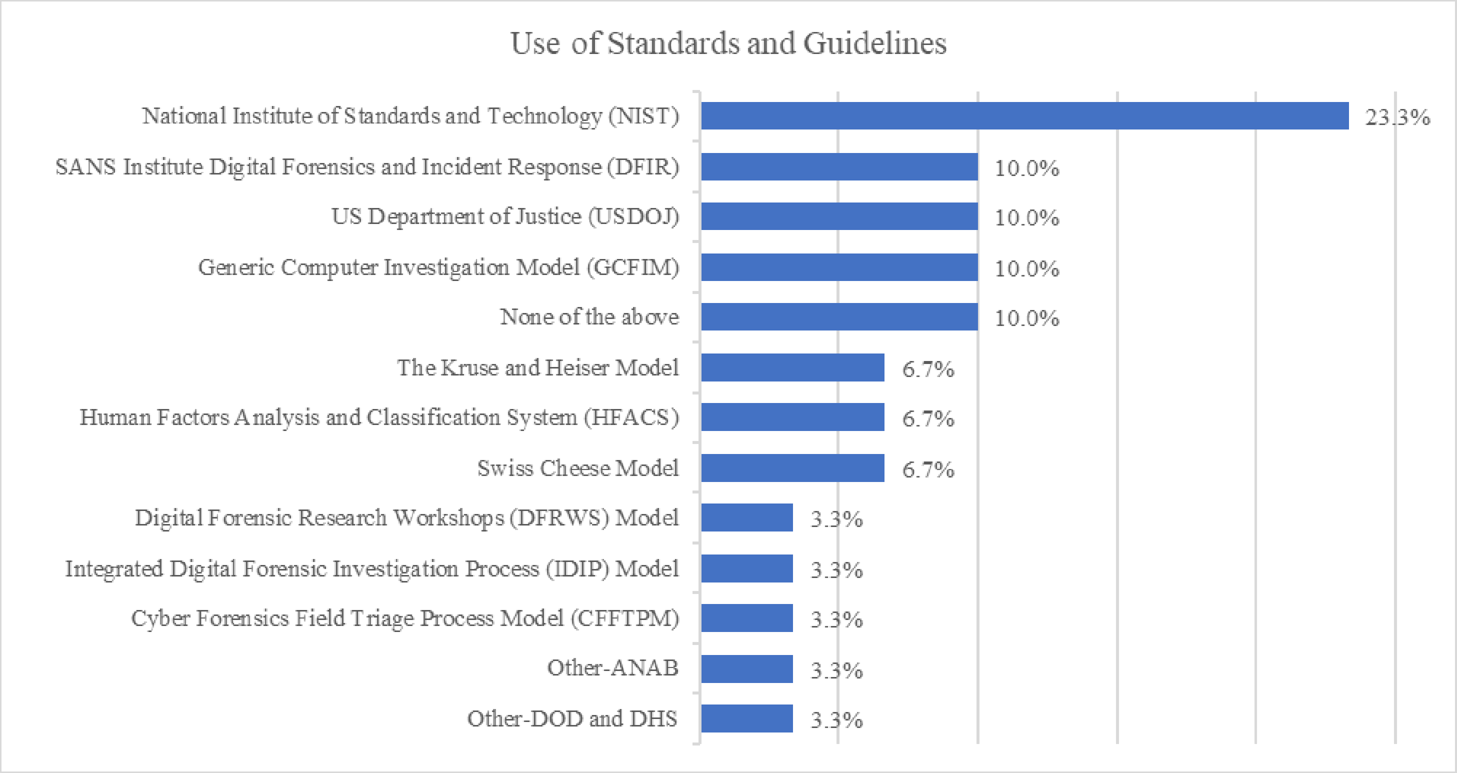
- What U.S. federal regulations guides your UAS forensic investigation or examinations?



Findings – 4

UAS forensics investigations and standards and guidelines

- What set of standards and/or guidelines do you use to conduct UAS forensic investigation or examinations?

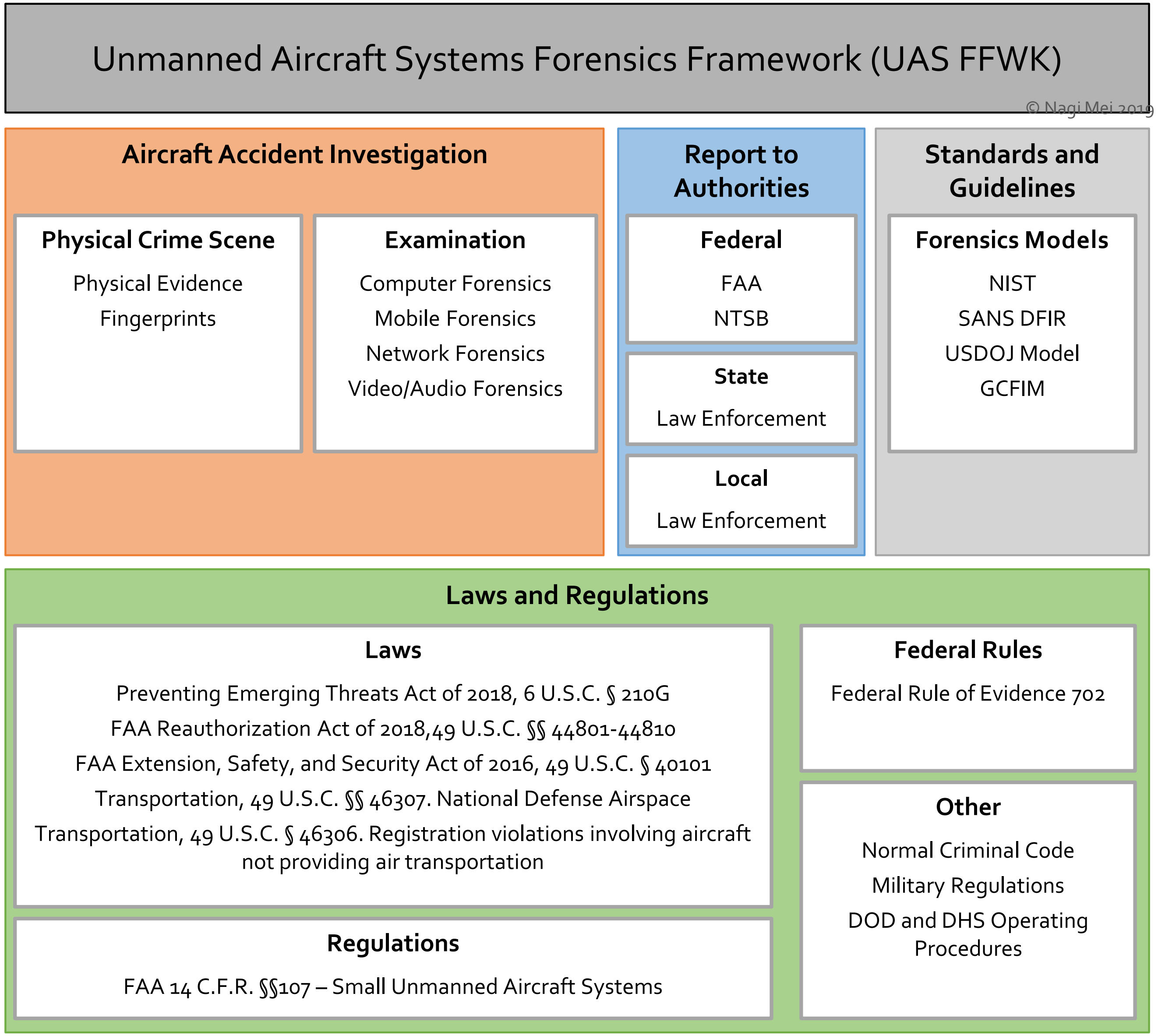


Limitations

- Access to professionals who have conducted UAS forensics was limited
- The survey may have reached the population of aircraft accident and digital forensic investigators, but not the target population of UAS forensics investigators
- Several of the participants who responded were disqualified because they either have not conducted investigation or forensics on a drone
- Despite the quality of the survey respondents, the study results suggested limited available or qualified UAS forensic experts and a majority use multiple frameworks to conduct drone investigations

Recommendations

- Rising unauthorize drone operations demands a standard framework for accurate and time sensitive investigations
- Standards organization might consider creating a standard UAS forensics framework to minimize errors and improve evidence admissibility in the U.S. courts
- To the right is a proposed basic UAS forensics framework compiled from research results



Unmanned Aircraft Systems Forensics Framework (UAS FFWK)

Aircraft Accident Investigation

Physical Crime Scene

Physical Evidence

Fingerprints

Examination

Computer Forensics

Mobile Forensics

Network Forensics

Video/Audio Forensics

Report to Authorities

Federal

FAA

NTSB

State

Law Enforcement

Local

Law Enforcement

Standards and Guidelines

Forensics Models

NIST

SANS DFIR

USDOJ Model

GCFIM

Laws and Regulations

Laws

Preventing Emerging Threats Act of 2018, 6 U.S.C. § 210G

FAA Reauthorization Act of 2018,49 U.S.C. §§ 44801-44810

FAA Extension, Safety, and Security Act of 2016, 49 U.S.C. § 40101

Transportation, 49 U.S.C. §§ 46307. National Defense Airspace

Transportation, 49 U.S.C. § 46306. Registration violations involving aircraft not providing air transportation

Regulations

FAA 14 C.F.R. §§107 – Small Unmanned Aircraft Systems

Federal Rules

Federal Rule of Evidence 702

Other

Normal Criminal Code

Military Regulations

DOD and DHS Operating Procedures

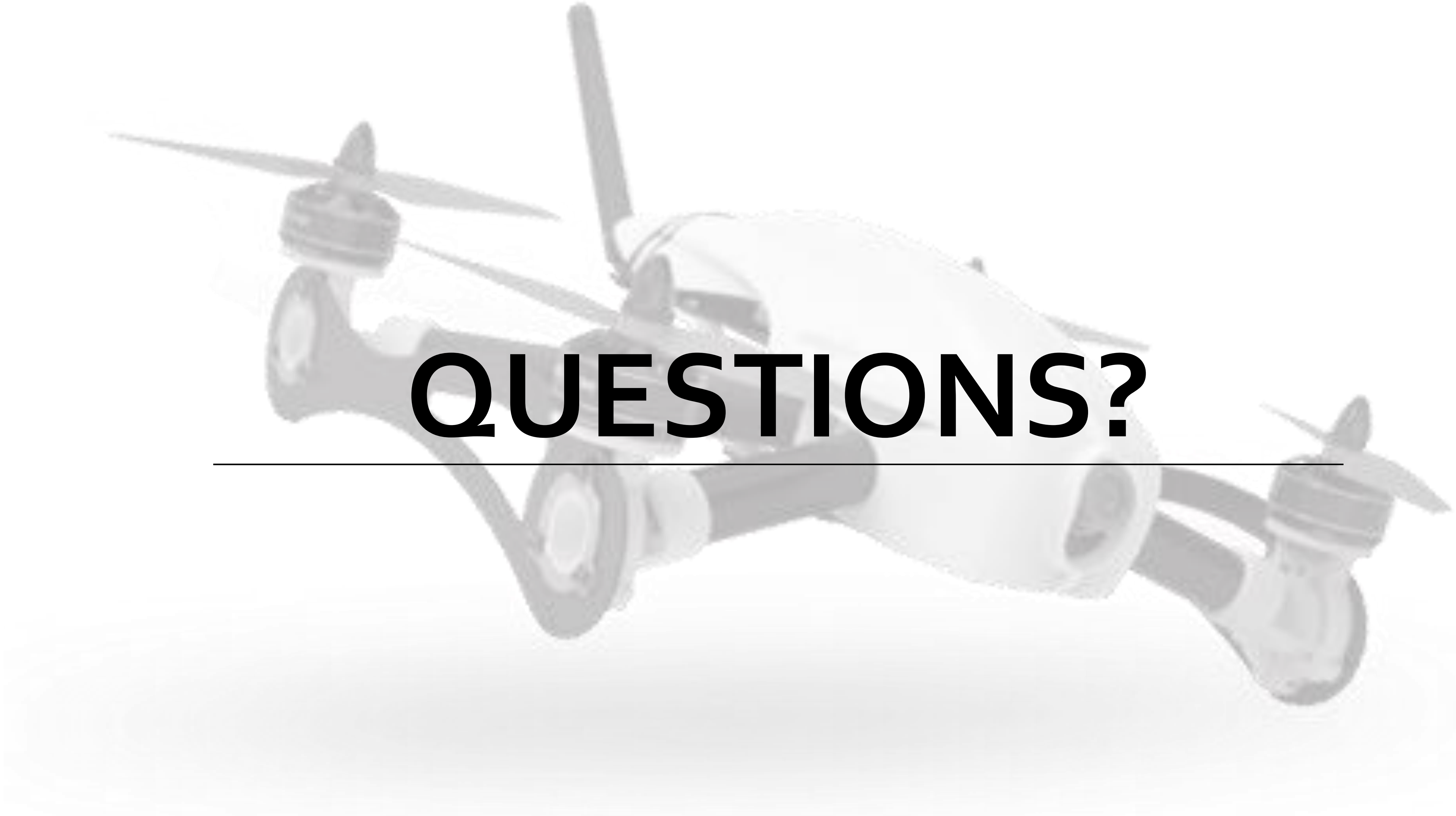
An Approach To Unmanned Aircraft Systems Forensics Framework

Recommendations for Future Research

- Many opportunities to build upon this study as drone applications continue to expand
- Additional research is needed for a standardized forensics process
- Build upon the proposed framework and existing aircraft accident investigation and digital forensics models
- Future research should include detailed processes for each area of the proposed UAS forensics framework
- UAS forensics framework might apply to unmanned vehicles (land or sea) by adapting proposed framework

Recap

- Objective was to identify the commonalities and gaps in forensics frameworks and guidelines
- Surveyed aircraft accident investigators and digital forensics investigators and their use of forensics framework to conduct forensics on a drone
- Data analysis revealed no significant relationship between the groups of respondents' drone investigations and the methods used to conduct UAS forensic investigations
- Investigators used multiple frameworks to conduct forensics on drones – UAS forensics required employing both digital forensics and aircraft accident investigations processes
- Drones have made an indelible mark in history and society – increase in drone presence, a demand for a standard UAS forensics framework is needed



QUESTIONS?

Photo by Unknown Author is licensed under CC BY-SA-NC

Resources for Flying a Drone

- Getting started for UAS https://www.faa.gov/uas/getting_started/
- Drone registration info https://www.faa.gov/uas/getting_started/register_drone/
- Register your drone https://faadronezone.faa.gov/#/
- B4UFly Mobile App https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/b4ufly/
- SkyVector for flight plan and notices https://skyvector.com/
- Commercial Drone Operator certificate https://www.faa.gov/uas/commercial_operators/
- Become a drone pilot https://www.faa.gov/uas/commercial_operators/become_a_drone_pilot/

THANK YOU

Photo by Unknown Author is licensed under CC BY-ND