Chapter 12: UAS System Deployment and Information Dominance (ID)

Student Learning Objectives – The student will be introduced to the concepts of Information Dominance (ID), Information Superiority (IS), Offensive Information Operations (OIO), Network-Centric Operations (NCO) and deployment objectives for the US Coast Guard in areas of operation using unmanned air and sea vehicles. This chapter will hone in on the *Information Dominance (ID) goal* that UAS/UAV systems present opportunities for excellence in Offensive Information Operations (OIO), and Network – Centric Operations (NCO).

UAS in Military and Commercial Service

At first glance most developed UASs are applicable to both military and civilian deployment. The military forces use UAS in dull, dirty, dangerous (DDD) roles in which human pilots would be at risk. These roles have expanded far beyond the DDD boundary. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010) The reason civilian UASs have not outnumbered military UAS (in the CONUS) is because of the restrictions in the civilian market.

Civilian uses require operations in open airspace, rather than on a battlefield or within a military enclosure. Regulating authorities have not yet accepted their general operation. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010) FAA is in charge of protecting the National Airspace (NAS). The FAA regulations regarding UAS seem to center on preventing injury to persons and damage to property due to failures of the UAS and preventing injury or damage caused by collisions between UAS and other airborne vehicles. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010) In the former case, FAA has made effective regulations to assure the airworthiness of the systems and meeting these requirements to insure protection of persons and property. If there are drawbacks, they are cost and bureaucracy.

UAS collisions in the NAS is another thing entirely. Authorities are still searching for a completely reliable method of sensing the presence of another airplane vehicle and avoiding collision with it. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010) This requirement is true in open airspace and in dedicated UAS space. Cost of the SAA and product support may also be inhibiting the civilian UAS market. Both UAS markets are subject to the principles of Information Dominance (ID) because UAS / UAV systems are an essential component of the collection technologies used. As an intermediate step to full commercialization, FAA may require a Part 107 waiver process in controlled airspace. (FAA, 2018)

Information Dominance (ID)

"Information warfare (IW) -based technologies are categorized by their information operations roles and by three distinct levels of technology maturity:

- *Core Technologies* – current state-of-the-art, essential technologies necessary to sustain the present level of information.

- *Enabling technologies* –concerned with the next generation of IW capabilities. They represent a significant enhancement in operations. [Tactical level changes]
- *Emerging technologies* – far on the horizon applications where feasibility is demonstrated. These are so call Black Swan events which involve radical improvements in capability and approach to information operation." [Strategic level changes]
  (Waltz, 1998) 1972 RSA changes to public –key cryptography represented a Black Swan (Taleb, 2010) event in the crypto – world. (Rivest, 1978)

Numerous DOD technology studies have evaluated the potential developments that may impact Information Warfare with respect to UAS / UAV / UUV systems. A few samples:

Unmanned Systems Integrated Roadmap Fy2011-2036 covers interoperability, autonomy, airspace integration, and manned-unmanned teaming (MUM) (Army, 2013)

The Navy Unmanned Undersea Vehicle: (UUV) Master Plan covers the important mission categories for use of UUVs. These include ISR, mine countermeasures (MCM), Anti-submarine warfare (ASW), Inspection and Identification (ID), Oceanography, communications / navigation network node (CN3), payload delivery, information operations (IO) time critical strike (TCS), barrio patrol and sea base support. (Navy, 2004)

Joint Publication JP 6-01, Joint Electromagnetic Spectrum Management Operations covers the entire spectrum of offensive and defensive electromagnetic spectrum operations for all levels of defense activities. (Army-M, 2012)

US department of Homeland Security Cybersecurity Strategy- a fascinating document that covers risk identification, vulnerability reduction, threat reduction, consequence mitigation and enabling cybersecurity outcomes. (DHS, 2018)

The U.S. Navy's Plan for Information Dominance – a broad ranging document about US Navy policies to gain ID and to use information as a weapon. (NavyID, 2010)

The Military Critical Technologies List Part II: Weapons of Mass Destruction Technologies. An older document that enumerates critical technologies for directed energy weapons (DEW) and information warfare. (DoD-IW, 1998)

"*Information Dominance* as defined by the US Navy is the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects." (Google, 2018) There are other definitions:

"Information Dominance - the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary." (Army6, 1996)

"Information Dominance - A condition that results from the use of offensive and defensive information operations to build a comprehensive knowledge advantage at a time, place, and on decision issues critical to mission success." (Griffith, 1997)

"Information Superiority - the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." (Chiefs, 2014)

The definitions above have conceptual similarities. The author actual prefers the Information Superiority approach which involves technologies for collecting data, processing that data into knowledge and disseminating that knowledge to live respondents. Table 12-1 is a condensed form of (Waltz, 1998) Table 10.1 pages 362-363 specific to IW/ID. Table 12-1 is essentially a top-level matrix for Information Warfare based on enabling and emerging core technologies. Recognize that the prime goal of the broader purview of Information Warfare is Information Dominance and by inclusion Information Superiority (IS)

Table 12-1 General Technology Categories for Information Warfare

Information Warfare

Core - Sustainable

Attack

- Electronic attack based on brute force
- And precision jamming, deception
- Semi-automated network attack
- Dynamic Malicious codes

Defend

- Robust cryptography, trusted computers,
- Network security authentication protocols
- Electromagnetic hardening

Enabling –Technology Jump

Attack

- Semi /fully-automated network attack
  - Dynamic adjustment
- Tactical electronic attack with DEW
- High energy chemical lasers
- Dynamic and autonomous malware/ logic
- Precision directed DEW

Defend

- Trusted network challenge response, duel /

- Authentication and response
- Multi – type authentication
- Network intrusion detection systems
- Steganography – use of SPAM
- Anti-DEW weapons
- Blockchain
- All optical networks

Information-Based Warfare

Core-Sustainable

Collect

- Airborne Reconnaissance (manned and MAME UAS)
- Space surveillance
- HUMINT
- GPS / GNSS
- EO, IR, SAR multi-spectral sensing

Process

- Data warehouse
- Data fusion
- Automatic target recognition (ATR)
- Data mining
- Text-based databases, hyperlinking

Disseminate

- Push-pull dissemination
- Data compression
- Global broadcast
- 3-D visualization

Enabling – Technology Jump

Collect

- High altitude UAS
- Unattended intelligent ground sensors
- Commercial high – resolution imaging satellites
- Integrated ground to space sensors

- Protected GNSS / tracking
- Hyperspectral, integrated aperture sensing
- Barrier penetrating sensors
- Micro UAVs
- Intelligent Level 5 SAA

Process

- High-bandwidth global broadcast
- Medium-bandwidth global communication satellite network
- Global cellular and microcellular wireless voice and data
- Virtual reality visualizations
- DNA and molecular computing storage

Disseminate

- High-bandwidth broadcast, multicast, point-cast networking
- Networks of sensors in space, air, surface operating together
- Global real-time tailored knowledge delivery

As seen in Table 12-1, information dominance technologies fall into "three general areas: collection, processing and dissemination. *Collection* includes methods of sensing physical phenomena and platforms that allow sensors to carry out their missions. These include direct and remote sensing devices along with the relays of data to user." (Waltz, 1998)

Processing (power) refers to the numbers of operations per second, information storage capacity (in bits). Technologies to increase processing power are many, subtle, overt, heterogeneous, involving hardware, software, networks, machine / human interface, autonomous, knowledge-management, indexing and beyond the scope of this work.

Dissemination technologies are communications technologies to increase bandwidth and effective use of bandwidth (compression techniques, data / knowledge organization). Enhancements to these technologies include increased storage and shortened latency times.

Unmanned aircraft systems play a significant role in the collection technologies. Collection technologies include the advanced platforms and sensors to acquire a depth of data. (Waltz, 1998)

High-Altitude Endurance (HAE) and Medium – Altitude Endurance Unmanned Air Vehicles (UAVs)

"The Global Hawk (HAE) and Predator models (MAE) introduced penetrating airborne surveillance with a broad area search capability. HAE UAVs provide long dwell times over target areas. Both the Global Hawk and the Predator series complement short – and close-range UAVs, which do not have deep

penetration capability, and satellite surveillance, which does not have revisit rates." (Waltz, 1998) Close-range UAVs support small unit operations with ranges to 30km and short-range UAVs have medium-altitude endurance (30-50 hours with 150 to 300 km range)

Both the Global Hawk and Predator sport communication relay capabilities, precision SIGINT, local precision navigation capabilities, and operate a sensor network with autonomous and cooperative behavior in hostile space. (Waltz, 1998)

Offensive Information Operations (OIO)

The names and definitions have changed since Waltz's signature work in 1998, on the subject of Information Warfare, but the operations remain the same – but more sophisticated, networked and complexity-rich. (Waltz, 1998) Our objective is to see where UAS /UAV systems fit into his various taxonomies of IW / ID. Coverage of Waltz's work, in this chapter, is only "helicopter –view" and compressed. The reader is encouraged to explore further the wealth of literature on this subject.

"Offensive operations are uninvited, unwelcome, unauthorized and detrimental to the target; therefore, the term *Attack* to refer to all of these operations." (Waltz, 1998)

"Offensive information operations are malevolent acts conducted to meet strategic, operational, or tactical objectives of authorized government bodies; legal, criminal or terrorist organizations; corporations; or individuals. The operations may be performed covertly, without notice to the target, or they may be intrusive, disruptive, and destructive. The effects on information may bring physical results that are lethal on humans." (Waltz, 1998)

President Obama used drones to great success tracking down terrorist High Value Targets (HVTs) and assassinating them. Because of his elevated use of UAVs for this purpose, he left somewhat of a legal mess in his wake. (Zenco, 2016) However, the information dominance side of the operations were an unqualified success.

Offensive information attacks have two basic functions: to capture or to affect information. Information here refers to data /information / knowledge content. ID is measured in terms of:

- "Functions – broken down into offensive measures of *capture and affect* used to effectively gain a desired degree of control of a target's information resources. Capturing information is an act of theft of a resource if captured illegally, or technical exploitation if the means are not illicit. Affecting information is an act of intrusion with intent to cause unauthorized effects, usually harmful to the information owner." (Waltz, 1998) Both capture and affect by UAS are collection processes.
- Tactics – Attack tactics -the operational processes employed to plan, sequence, and control the countermeasures of an attack. These tactics consider objectives, desired effects [covertness, denial, disruption of service; destruction, modification, or theft of information], degree of effects; and target vulnerabilities." (Waltz, 1998)
- Understanding attack mechanisms helps information security designers to prepare for defense. In the information business, the common standard of information security (INFOSEC) is CIA, which

means confidentiality, integrity and availability. (Nichols R. K., 2002) Reviewing the attack tactics – factors above, brings to mind Parker's brilliant expansion of the CIA basis for securing information. (Parker, 2015)

- "Parker expanded the traditional INFOSEC framework. Traditionally, users were concerned with preservation of: confidentiality, integrity and availability (CIA) information from disclosure, modification, destruction, or use; by prevention, detection, recovery; to *reduce loss or reduce risk of loss*. Parker was ahead of his time. He saw INFOSEC as preservation of six elements: availability, utility, integrity, authenticity, confidentiality, possession of information; from accidental or intentional destruction, interference, use of false data, modification or replacement, misrepresentation or repudiation, misuse or failure to use, access, observation or disclosure, copying, stealing or endangerment. This was done by: avoidance, deterrence, prevention, detection, mitigation, transference, sanction, recovery, or correction to meet a standard of due care,
  Avoid loss, reduce loss, or / and eliminate loss." (Parker, 2015) Parker even envisioned the means to accomplish his information security framework. Two controls were to be robustly instituted: government controls to include: employee clearances, the principle of need-to-know, mandatory access control, classification of information, and cryptography and business controls include: need-to-withhold, discretionary access control, copyright and patent, and digital signatures. (Parker, 2015)
- "Techniques –the technical means of capturing and affecting information of humans – their computers, communications, and supporting infrastructures." (Waltz, 1998)
- Motive – varied but most common are: ideological, revenge, greed, hatred, malice, challenge, theft.
- "Invasiveness – Attacks may be active or passive. Active attacks invade and penetrate the information target. Passive attacks sit on the line and observe behaviors, information flows, timing, and energy." (Waltz, 1998)
- "Effects –may vary from small- harassment to theft, from narrow, surgical modification of information to large-scale cascading of destructive information that brings down critical infrastructure." (Waltz, 1998) The Stuxnet attack on the Iranian centrifuges in in 2015 was a brilliant example of large-scale effects on critical infrastructure. (Holloway, 2015)
- Ethics and legality- Traditional intelligence activities are allowed in peacetime (capture information by UAS) but information attacks that affect information are not covered adequately by law. Unlike real property, information is a property that may be shared, abused, copied, and stolen without evidence or the knowledge of the legitimate owner.

A taxonomy of attack countermeasures may be viewed in a two-dimensional attack matrix:

Rows are labelled perceptual, information, or physical. Columns are headed by attack category: capture or affect. From a UAS standpoint, we are only interested in characterizing the information infrastructure level of the attack. Before we extract the Figure 8.1 Attack Matrix row in (Waltz, 1998) page 255, two more avenues of approach are available to the attacker:

- "Direct, or internal, penetration attacks this involves penetrating a communication link, computer, or database to capture and exploit internal information, or to modify, add, delete, insert, or install a malicious process." (Waltz, 1998)
- "Indirect, or external, sensor attacks – perfect for UAS / UAVs flying above the targets. The attacker presents open phenomena to the systems sensors or information to sources, media, Internet, satellite, third parties, to achieve counter information objectives. These attacks include insertion of information, spoofing of information (GPS), to sensors or observation of behavior of sensors or links interconnecting fusion nodes." (Waltz, 1998)

Extracting just one information row from Waltz's Attack Matrix (Waltz, 1998) we have:

Table 12-2 Extracted Information Infrastructure Row from Waltz Attack Categories (Waltz, 1998)

- "Object: Capture
- Level of Attack: Information Infrastructure – Capture Information Resource
- Security Property Attacked: Privacy is breached
- Avenue: Indirect (Observe, Model Infer)
    - Passive intercept of message traffic
    - Non-intrusive mapping of network topology
    - Cryptographic analysis" (Waltz, 1998)
    - "EMS spectral analysis and categorization" (Nichols R. K., 2002)
    - Direct: Penetrate and Observe
        - Network attack and penetrate to secure unauthorized access to data
        - Trojan horse program
        - Install sniffer
        - Install spoofing software
- "Object: Affect
- Level of Attack: Information Infrastructure – Affect Information Resource
- Security Property Attacked: Integrity of data is invalidated; Availability of services degraded
- Avenue: Indirect: Cause effects through sensors or over the open network without penetration of target
    - Deceive: issue deceptive e-mail (phishing) message or conduct deceptive network behavior
    - Disrupt, Deny or destroy: Deny network data collection service by DDOD or Syn flood attacks that disrupt access to public or private sources. Insert an open message traffic and data that diverts attention and processing resources. Insert sensor data that upsets guidance or control process" (Waltz, 1998)[UAS perfect].
- Direct: Penetrate and affect targeted infrastructure and affect
    - Deceive: Insert Trojan horse with deception action. Modify, corrupt data by viral agent.
    - Disrupt, Deny, Destroy: Insert malicious code to deny or disrupt service ibn single host computer or entire network

Modern military activities are focused on network- centric operations. They are concerned with the primary threats to networks and especially the messaging and interconnecting links. The explosion of

wireless and IoT devices has ramped up INFOSEC concerns. Some system designers are now trying to mitigate the treats to their networks based on Blockchain technology. Blockchain is harped as a revolution in cryptographic protection. Started with Bitcoin, proponents would use Blockchain technologies to protect business, money and military networks. (Tapscott, 2016) "The managing author disagrees with this approach on many grounds including reviewed security holes, privacy issues, single-source point of failure and the fifty –one percent emersion/ dominance attack. (Jay, 2018) Lastly, the data is held in the dark web where the worst of malevolent actors anonymously play." (Nichols R. K., 2018)

Going back to first principles of INFOSEC, primary active threats to networks and network messaging (includes communication links, EMS vectors, interconnected nodes, wired / wireless hardware, and access points, frankly everything that talks to anything in the networks). The messages may have different formats, however, they are known. UAS systems are not just collectors of information or signals in the sky. They can convert, modulate, attenuate, insert, delete information as programmed to do so, and can initiate a network attack! (Nichols R. e., 2016)

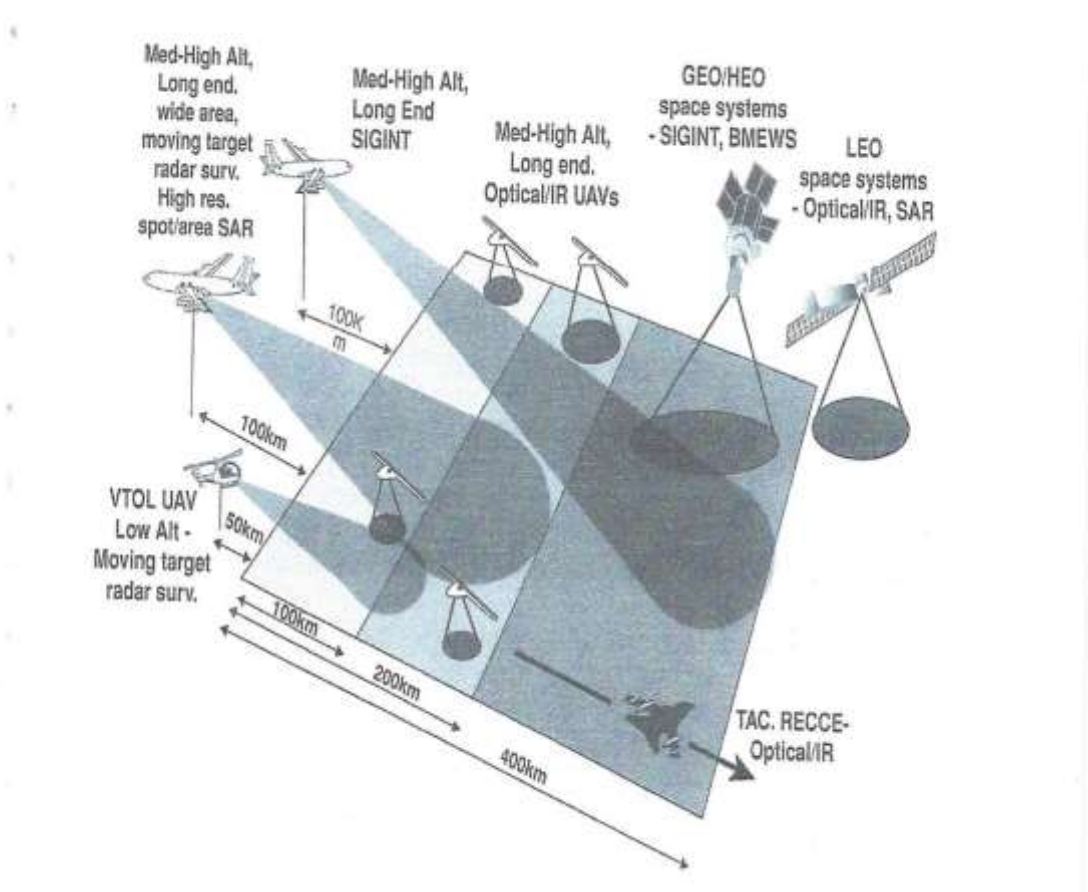
There are five types of network intrusive actions: Access, Denial, Inter-message or spoofed message, Intra-message, and data storage. The functional objective of access is for an invalid user to gain access to the system, and the unauthorized user elevates his/her access at a higher level than authorized. The functional objective of denial is to deny service requests and to disrupt the flow of messages in the system, rendering it completely inoperable or reduced in operating capacity to some degree. There are four inter-message intrusive actions: spoofing (like GPS in naval situations), modification, replay, and leakage. All these are compromises of identity, authentication, message, or content in transit. Intra-message violations are either repudiation (Didn't order the book) or security content (breach of firewall or security device / rule). Data storage intrusions include message pre-plays or direct corruption of sources or integrity while in storage (sending random bits into backup disks is an example). (Waltz, 1998)

A simple NCO attack strategy can be initiated from any source including UAS over the target network. (Nichols R. e., 2016) Phase 1 is Reconnaissance begins by searching for and collecting passwords or cryptographic password files to be computer-brute-forced; gaining access, finding unused accounts, and establishing covert access. Phase two is penetrate and act which involves gaining entry, check for surveillance, gain system control, attack by searching directories, acquiring useful data, searching for evidence and destroying both evidence and audit trails, and surveillance if possible, then replacing control and logging off as if the attacker was never there. (Nichols R. e., 2016)

Practically every known computer system is vulnerable to attacks. Clark wrote the Red Team Field Manual of software attacks on every modern system and structure on the market, including *NIX, Windows, networking, web, databases, programming and wireless. (Clark, 2013) To be fair, White and Clark also wrote a Blue Team Field Manual which covered countermeasures such as scanning, vulnerability analysis, network discovery, service disabling, firewalls, detection (visibility) PCAP tools, NETCAT tools, respond and analysis, remediation, tactics, incident management, and security incident identification (SCHEMA). (White, 2017) One of the best books on practical countermeasures for network security is by (Nichols R. R., 2000) entitled *Defending your Digital Assets against Hackers, Crackers, Spies and Thieves.*

Network-centric Operations (NCO)

Figure 12 -1 UAS Surveillance Network



Source: Austin, R, S: (2010), CT: Unmanned Aircraft Systems: UAVS Design, Development and Deployment. London: Wiley Aerospace Series.

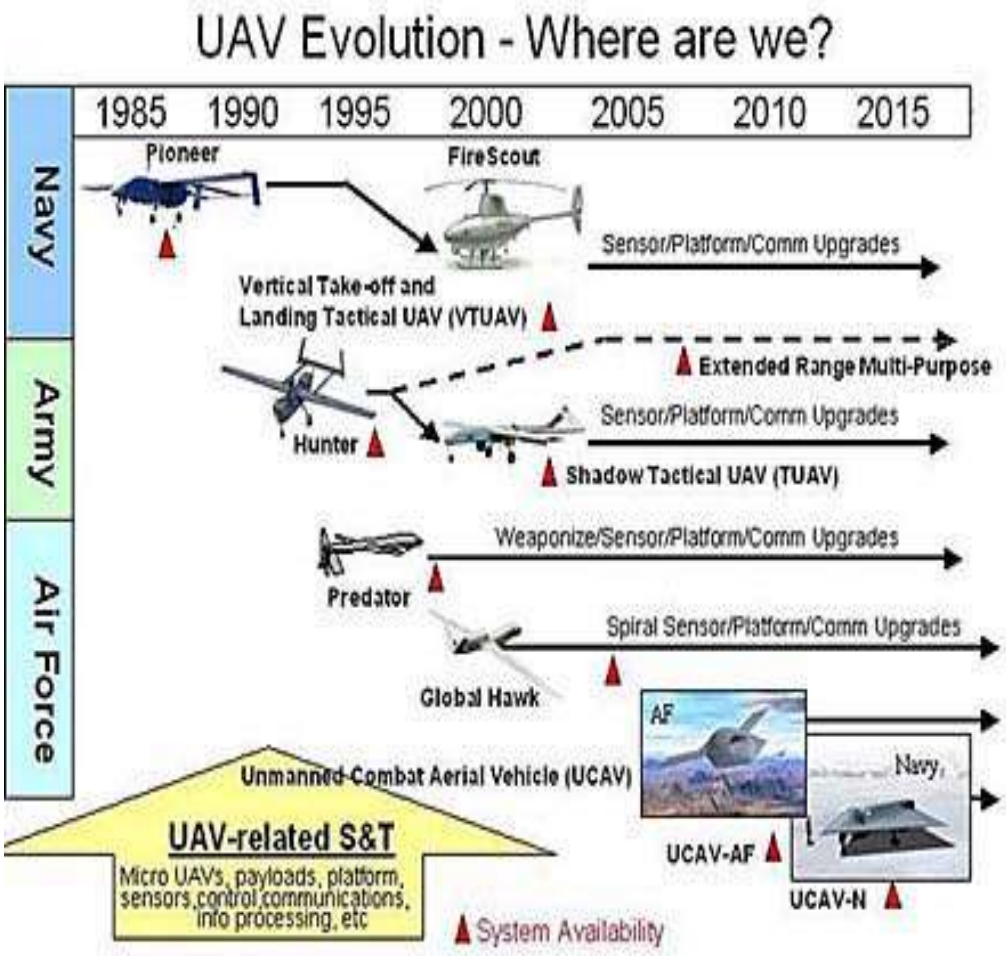
UAS systems – especially military ones – rarely operate in a vacuum. They receive and process information from many sources, which include satellites, manned aircraft, naval vessels and ground-based systems. UAVs may be the top supplier of information to a network. Figure 12-1 illustrates a surveillance network using airborne systems. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010) Every theater of war and all their military activities may be coordinated through a network. This is called network-centric operations (NCO). An "NCO has four characteristics using robust technologies:

- Secure communications between systems via multiple links,
- Standardization of interfaces between key systems,
- Adaptable and user-friendly interfaces with human operators,
- Coordinated radio frequency bandwidth." (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010)

The strength of a UAS NCO is that the UAS leader is not limited to surveillance. It is not just the collection agent / technology. The HALE UAS may disseminate information which it has self-acquired or received. The UAS is one of the reasons for information dominance achieved via an NCO. UAS systems have come a long way in just a brief time. See Figure 12-2 UAV evolution since 1995. A range of activities, air-, sea-and land-borne, covering reconnaissance, surveillance, support, defensive and attack operations may be coordinated through a UAS lead NCO. (Austin, Unmanned Aircraft Systems: UAVS Design, Development and Deployment, 2010)

However, NCOs do have weaknesses. If a major system fails, like GPS, then the whole network may be subject to catastrophic failure. Most NCOs have both fail-safe and fall back options.

Figure 12-2 UAV Evolution



Source: Library, L. (2018, August 23). Government Resources: Defense, Military, and Security: Drones (Military). Retrieved from https://library.louisville.edu/ekstrom/gov_defense/dronesmil

Coast Guard Roles

The U.S. Coast Guard (USCG) plays a vital role in *Information Dominance (ID)*. The National Fleet

Policy in 2014, established the partnership of the USCG and USN to enhance both branches capabilities and identify emerging threats. With the combination of Department of Defense and Homeland Security in the maritime infrastructure the partnership brings the U.S. ability to gather intelligence to the next level. (See Figure 12-3) However, this is not the first time the USCG took part in the world of intelligence. The CG-210, a 75-foot Coast Guard patrol boat, was the first boat in U.S. history to become a signal-intercept ship. (Bennett, 2016) During the 1920's the CG-210 employed counterintelligence to stop illegal rum runners. Over 12,000 rum-runner messages were decrypted in a three-year span by Elizabeth Friedman. (Bennett, 2016)

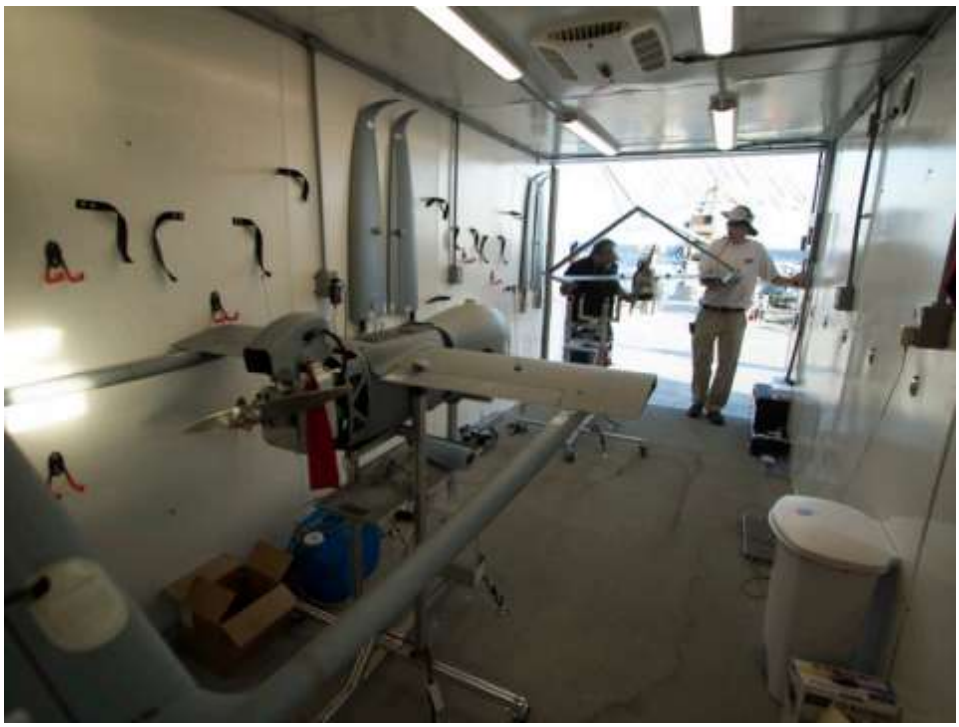
Figure 12-3 United States Coast Guard and Navy

Source: By U.S. Navy photo by Photographer's Mate Airman Apprentice Patrick Gearhiser [Public domain], via Wikimedia Commons https://commons.wikimedia.org/wiki/File:US_Navy_060517-N-4014G-130_The_Pre-Commissioning_Unit_Texas_(SSN_775)_sails_past_the_Coast_Guard_cutter_Sea_Horse_(WPB-87361).jpg

As of today, the Coast Guard "sees a clear opportunity to perform many of its missions faster, cheaper and more safely through the use of short-range unmanned aircraft systems," said Lt. Cmdr. Ryan Lampe, short-range UAS platform manager in the Office of Aviation Forces. (Haring, 2018) The sUAS of choice, (Host, 2018), is used to gather intelligence, surveillance, reconnaissance and provide real time imagery. Real time imagery includes taking photos of the ocean surface, checking for anomalies, and alerting the aircraft's operator for further investigation. The ScanEagle can provide VHF/UHF communications relay

and Target illumination. However, after seven years of use the ScanEagle will be challenged by the USCG acquisition of the Aerosonde. The Aerosonde (Figure 12-4) is larger sUAS that has the capabilities to fly over 150,000 flight hours in temperature extremes. The sUAS also has communications relay, but the stand out feature is the available day and night full-motion video.

Figure 12-4 sUAS Aerosonde



Source: Textron (2018, August 23). Aerosonde Data Sheet. Retrieved from Textron Systems, https://www.textronsystems.com/sites/default/files/resource-files/TS%20US%20Aerosonde%20Datasheet.pdf

There is one other sUAS the USCG is exploring to add to their inventory. The Puma (See Figure 12-5) is the USCG hand-launched sUAS that is current being tested. The Robotic Aircraft Sensor Program for the Maritime Environment (RASP-M), under the DHS, has allowed for the testing of Puma in Mississippi and Connecticut. The advantage of the hand-launched sUAS is the ease of launch and the ability to carry a payload, such as a high definition camera. This provides intelligence ranging from if an approaching vessel has weapons to data of a maritime environmental incident.

Figure 12-5 sUAS Puma

Source: Textron (2018, August 23). Aerosonde Data Sheet. Retrieved from Textron Systems https://www.textronsystems.com/sites/default/files/resource-files/TS%20US%20Aerosonde%20Datasheet.pdf

The Coast Guard uses National Security Cutters (NCS) or commonly referred to "go-fast boats". (Biesecker, 2018) for sUAS. The NCS are technology advanced, capable of launching small boats and serve as a flight deck. NCS perform homeland Security and defense operations in the maritime space.

"Unmanned aircraft systems have the potential of being major force multipliers for the Coast Guard," said Cmdr. Dan Broadhurst, UAS Division Chief for the Office of Aviation Forces (CG-711). (Haring, 2018) "They can provide persistent, tactical wide-area surveillance, detection, classification and identification functions that we currently do not have access to." (Haring, 2018) (See Figure 12-6)

Figure 12-6 United States Coast Guard UAS Concept

Source: Haring, L, (2018, January 19). Research, Development, Test and Evaluation Spotlight: Long-Range, Ultra-Long Endurance Unmanned Aircraft System. Retrieved from http://coa/stguard.dodlive.mil/2018/01/rdte-spotlight-long-range-ultra-long-endurance-unmanned-aircraft-system/

USCG is currently researching to acquire long-range, 24-hour endurance, UAS. The long-range drone would be used for intelligence, surveillance and reconnaissance missions. Additional USCG requirements include the UAS to conduct operations at a 15,000-foot mean above sea level and various maritime sensors, including electro-optic and infrared full-motion video, surveillance radar, radio frequency and direction finding, and tactical communications radio and datalink. (Biesecker, 2018)

Often referenced as the forgotten service, the USCG is far from being retired. The USCG has a long history with their intelligence and counterintelligence skills. The USCG is evolving with technology, not just by using UAS functionality. They have used UAS for the past eight years. The Coast Guard has ongoing research that allows for the branch to identify and obtain the best in industry UAS for intelligence and reconnaissance missions. They will continue to be a valuable partner to the USN in defense at sea and protecting the homeland.

Discussion Questions

1) UAS systems are both collection agents and directive information agents. Enumerate the points in the network- centric model that are most vulnerable to UAS surveillance or intrusion.
2) How vital is the UAS platform in terms of Information Dominance on the battlefield?
3) The USCG seems to be a silent service, with a huge mission with limited personnel active over all our water and coastlines. Research and report on five areas where they use UAS as effectively as any of military services.
4) Do the same research but focus on Civilian components / uses for UAS surveillance, collection and intrusion actions – specifically on a computer network.

Bibliography

Army, U. (2013). *Unmanned Systems Integrated Roadmap FY2011 - 2036.* Washington: Createspace Independent Publishing Platform.

Army6, U. (1996, August 27). *Information Operations.* Retrieved from FM 100-6: https://fas.org/irp/doddir/army/fm100-6/index.html

Army-M, U. (2012). *Joint Publication JP 6-01, Joint Electromagnetic Spectrum Management Operations.* Washington: US Government.

Austin, R. (2010). *Unmanned Aircraft Systems: UAVS Design, Development and Deployment.* London: Wiley Aerospace Series.

Bennett, M. (2016, August 8). *The TOP SECRET story of Coast Guard code breaking.* . Retrieved from coastguard.dodlive.mil: http://coastguard.dodlive.mil/2016/08/the-top-secret-story-of-coast-guard-code-breaking/

Biesecker, C. (2018, April). *Long-Range Coast Guard Drone to Undergo Tech Demo - Avionics.* Retrieved from Aviation Today: https://www.aviationtoday.com/2018/04/12/long-range-coast-guard-drone-undergo-tech-demo

Brothers, E. (2018, June 18). *Insitu to provide UAS services to US Coast Guard - Aerospace Manufacturing and Design.* Retrieved from Insitu - Aerospace Manufacturing and Design. : http://www.aerospacemanufacturinganddesign.com/article/insitu-uas-services-us-coast-guard-061818/

Chiefs, J. (2014, November 20). *Information Operations.* Retrieved from JP 3-13 Change 1: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Clark, B. (2013). *Red team Field Manual (RTFM).* New York: NP.

DHS. (2018, May 15). *DHS-Cybersecurity-Strategy.* Retrieved from DHS: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

DoD-IW. (1998, February). *Military Critical Technologies List Part II.* Retrieved from FAS: https://fas.org/irp/threat/mctl98-2/mctl98-2.pdf

FAA. (2018, August 26). *Request a Part 107 Waiver or Operation in Controlled Airspace.* Retrieved from FAA: https://www.faa.gov/uas/request_waiver/

Griffith, J. a. (1997, January). *Information Dominance v Information Superiority.* Retrieved from IWAR: http://www.iwar.org.uk/iwar/resources/info-dominance/issue-paper.htm

Haring, L. (2018, January 19). *Research, Development, Test and Evaluation Spotlight: Long-Range, Ultra-Long Endurance Unmanned Aircraft System.* Retrieved from http://coastguard.dodlive.mil/2018/01/rdte-spotlight-long-range-ultra-long-endurance-unmanned-air

Holloway, M. (2015, July 16). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* Retrieved from Stanford.edu/courses/2015: http://large.stanford.edu/courses/2015/ph241/holloway1/

Host, P. (2018, January 31). *US Coast Guard evaluating ScanEagle ocean surface anomaly detector payload.* Retrieved from https://www.janes.com/article/77496/us-coast-guard-evaluating-scaneagle-ocean-surface-anomaly-detector-payload

Information Dominance definition. VAdm Card, K.L & VAdm Rogers, M.S. (2013) *Navy Strategies for Achieving Information Dominance 2-13-2-17: Optimizing Navy's Primacy in the Maritime and Informational Domains. Washington, US Navy:* Retrieved 10/12/2018 from https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Information_Dominance.pdf

Jay, J. (2018, June 1). *Blockchain-platform-eos-found-containing-critical-security-vulnerabilities.* Retrieved from SC Media - SCmagazine UK: https://www.scmagazineuk.com/blockchain-platform-eos-found-containing-critical-security-vulnerabilities/article/1472602

Library, L. (2018, August 23). *Government Resources: Defense, Military, And Security: Drones (Military).* Retrieved from gov_defense/dronesmil: https://library.louisville.edu/ekstrom/gov_defense/dronesmil

Mighty-Team. (2018, August 23). *5 differences between the Navy and Coast Guard.* Retrieved from We are the mighty: Team Mighty. (2018, April 2). 5 differences between the Navy and Coast Guard. Retrieved from https://www.wearethemighty.com/articles/5-differences-between-the-navy-and-the-coast-guard

Navy, U. (2004). *The Navy Unmanned Undersea Vehicle (UUV) Master Plan.* Washington.

NavyID, U. (2010, May). *US Navy's Vision for Information Dominance.* Retrieved from DoD Publications: http://edocs.nps.edu/dodpubs/topic/vision/vision2010.pdf

Nichols, R. e. (2016). Drone Wars: Threats, Vulnerabilities and Hostile Use of UAS. *INFOWARCON16 Proceedings.* Nashville, KY: INFOWARCON.

Nichols, R. K. (2002). *Wireless Security: Models, Threats, Solutions. New York: McGraw-Hill.* New York: McGraw-Hill.

Nichols, R. K. (2018, May 2). A Primer on Cryptocurrency & Blockchain. *KSU Invited Presentation before Lions Club* . Salina, KS, USA: KSUP.

Nichols, R. R. (2000). *Defending your Digital Assets against Hackers, Crackers, Spies and Thieves.* New York: McGraw-Hill RSA Press # 1.

Parker, D. B. (2015, September 12). *Toward a New Framework for Information Security?* Retrieved from Wiley Online: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118851678.ch3

Rivest, R. S. (1978, February 1). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). *Communications of the ACM, 21 (2)*, pp. 120–126. doi:10.1145/359340.359342.

Taleb, N. N. (2010). *The Black Swan: the impact of the highly improbable (2nd ed.).* London: Penguin.

Tapscott, D. a. (2016). *Blockchain Revolution: How the technology behind Bitcoin is changing money, business and the world.* New York: Penguin Random House.

Textron. (2018, August 23). *Aerosonde Data Sheet.* Retrieved from Textron Systems: https://www.textronsystems.com/sites/default/files/resource-files/TS%20US%20Aerosonde%20Datasheet.pdf

Waltz, E. (1998). *Information Warfare: Principles and Operations.* Boston: Artech House.

White, A. a. (2017). *The Blue Team Field Manual.* New York: NP.

Zenco, M. (2016, January 12). *Reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy.* Retrieved from NY Times: https://www.nytimes.com/roomfordebate/2016/01/12/reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy