Chapter 10: UAS Intelligence, Surveillance and Reconnaissance (ISR)

Student Learning Objective

The student will gain knowledge on UAS intelligence, surveillance, and reconnaissance systems. Topics include sensors, missions including history, the current state of industry, and planning and execution considerations for gathering datasets using this technology.

History/Background of UAS ISR

UAS for intelligence, surveillance, and reconnaissance is a well-known application of the technology. “The clear majority of UAVs are used purely for intelligence, surveillance, and reconnaissance (ISR) missions. In current military usage, they range from the Global Hawk, with a wingspan greater than a Boeing 737 airliner, to Nano-helicopters that weigh a few grams, and all points in between” (Lambeth, 2006). FLIR Systems produces the Black Hornet 3 and, “At 32 grams, offers the lowest size, weight, and performance for UAS available…flies 2 kilometers at speeds of over 21 kilometers an hour. The Black Hornet 3 also incorporates sharper imaging processing featuring the FLIR Lepton® thermal micro camera core and a visible sensor to allow greater image fidelity, (with) an improved encrypted military-approved digital datalink, enabling seamless communications and imagery significantly beyond line-of-sight and in closed areas” ("FLIR Launches Next-Generation Black Hornet 3 Nano-UAV," 2018).

A UAS is simply a “truck” for the sensor system. It is the tool that is used to move, power, and task the sensor in the air. With such a wide variety of “trucks” available today, ISR appears to be limited more by human innovation and imagination than technology itself.

The ability to extend missions, gather previously unknown or unavailable information, and keep human operators out of harm's way forms the basis of why UAS are more suitable for the dull, dirty, and dangerous missions. UAS do not get bored, tired, lose focus, require minimal training as compared to humans and do not carry the bias of humans, the data gathered is “truth” to the sensor system. “The physical movement of drones is only one aspect of their potential vulnerability. The still image or video cameras routinely fitted to UAVs serve as a live link back to their operators – and enable drones to be used as highly maneuverable real-time eyes in the sky.” (CyberRisk, 2017) “They provide the visual and location information they carry and yield a high-value target for malicious third parties.” (CyberRisk, 2017)

The tactics and techniques that are applied to today's technology stem from the field of remote sensing. Remote sensing has a long history as it began with humans attempting to see and sense phenomena from a distance; from using pigeons to balloons to aircraft satellites, to UAS. Now UAS are coupled with space-based platforms for information and command and control. This field of study has allowed advances in military movement, attack and defend, as well as civilian surveying, and developing, freedom of movement throughout our world.

During Napoleon’s campaigns, the French used observation balloons to monitor enemy activities. In 1831 Napoleon understood the true importance of remote sensing for shaping the battlefield as he stated, “If I always appear prepared, it is because before entering on an undertaking, I have meditated for long and foreseen what may occur" (Napoleon Bonaparte, 1831). This technique continued through the U.S. Civil War.

Remote sensing as defined by Lillestand and Keifer is, "the science and art of bating information around an object, area or phenomenon through the analysis of state acquired by a device that is not in contact with the object, area or phenomenon under investigation" (Lillesand, Kiefer, & Chipman, 2014). In simple terms, it is the ability to study different point of interest from afar without having to physically sample the item.

History of Photography

The history of photography is one that started with the early Greeks and pinhole cameras. These were very basic, and the image was upside down and was not permanent (Bellis, 2017). It was not until the 1800s that an image was able to be permanently stored on media. Cameras and film were progressing at different speeds. They finally came together in the 1830s. Nicephorus Niepce and Louis Daguerre, both of France, created the capability to produce permanent images that could be replicated. Nicephorus Niepce died before France recognized the achievement, and because of that, the first photographs were known as daguerreotypes. One of the problems that continued to plague the early photographers was the amount of time it took to develop the film. Prior to 1829, it was not unusual for a film to take eight hours to develop the film.

Prior to 1829, it was not unusual for a film to take eight hours to develop. Daguerre discovered a method that took less than thirty minutes (Lucibella, 2013). Once the photographic and film development methodology was published, aerial photographs were taken with a wide variety of objects – most typically kites and balloons. The first American to take aerial photographs was James Wallace Black, who took photographs of the Boston harbor in 1860, see Figure 10-1. The 1906 San Francisco earthquake photographs were taken from a kite (King, 2012).

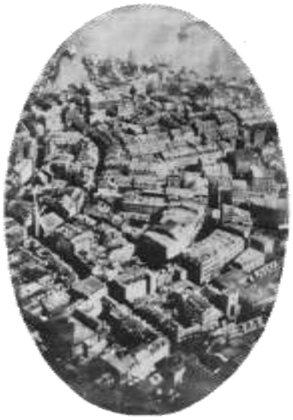


Figure 10-1 Boston Harbor, 1860, James Wallace Black. *Source*: Schultz, C. (2013). This Picture of Boston, circa 1860, is the World's Oldest Surviving Aerial Photo. Retrieved from: https://www.smithsonianmag.com/smart-news/this-picture-of-boston-circa-1860-is-the-worlds-oldest-surviving-aerial-photo-14756301/#RohlhYJZRcJzyVy7.99

Remote Sensing

Remote sensing systems continue to change the way wars are fought. Information is gathered and analyzed that allows leaders to “see more, understand better and decide quicker.” Observing enemy activity using high ground to survey the battlefield and then relay this information to military leaders goes back to ancient times. Military leaders understand the importance of high ground. With remote sensing systems, this high ground can be extended far beyond humans’ normal observation abilities.

The introduction of the airplane by World War I enhanced the world’s military capability to gather intelligence beyond enemy lines; gathering aerial photographs that would provide vital intelligence before, during and after a battle.

Limitations on airplanes, photography systems, and the time required to process intelligence lead to ever-increasing research and development by militaries around the world.

The US recognized the limitations of using standard aircraft for its intelligence gathering and began research on new remote sensing systems to improve its intelligence gathering capability. These platforms would be designed to fly undetected at higher altitudes, faster airspeeds, and with advanced camera systems. This capability assisted in tracking enemy equipment, movements, as well as their research and development programs. Early systems would offer the ability for the first time in the US to have an “eyes on” ability for treaty verification, something that the Soviet Union was not prepared for, nor did it want the US to have.

“The U-2 project was undertaken in the early 1950s; first flight occurred in August 1955. This project was created by the Central Intelligence Agency (CIA) because they required better intelligence gathering systems to amass intelligence on the Soviet Union. Collection efforts against the Soviet Union with modified bomber aircraft had taken place. However, those missions were vulnerable to counterintelligence observation, anti-aircraft fire, and fighter intercepts. It was thought a high-altitude aircraft such as the U-2 would be hard to detect and almost impossible to shoot down. Understanding the principles of high ground, the CIA began working on platforms that could be used specifically for reconnaissance operations.” (Malesky, 2002)The U-2 gained public attention, “during the U-2 Crisis when pilot Francis Gary Powers was shot down over Soviet territory on May 1, 1960.” (Malesky, 2002)

“The U-2 aircraft that was funded by the CIA and built by the U.S. starting in the 1950s. It became the subject of many "incidents," or diplomatic confrontations, with the Soviet Union during the Cold War. The most famous of these run-ins is referred to as *the* U-2 incident began on May 1, 1960, and what was to have been the twenty-fourth U-2 overflight of the Soviet Union.” (FAQS, 2018) At this time, Gary Powers was one of the most experienced U-2 pilots in the world and “the overflights had become routine to him.” (Malesky, 2002) The CIA issued its U-2 pilot's cyanide capsules and a poison needle hidden in a bisected silver dollar. Powers never took them along. Even more alarming was that, “Powers had become more and more cavalier. The morning of departure for Peshawar, he even packed his wallet with an assortment of

American German and Turkish money for his layover in Norway; his wife packed him a lunch for the shuttle flight to Pakistan" (Barnes, 2005).

"Gary Powers took off from a U.S. air base at Rawalpindi, Pakistan. The mission profile on this flight codenamed Grand Slam was to be the most ambitious U-2 flight yet. Powers flight plan would take him from Turkey to Soviet nuclear-weapons facilities in the Ural Mountains, then over various railroads, then to intercontinental ballistic missile sites in Siberia, then back across northern Russia, finally to several shipyards before leaving Soviet airspace above the Arctic Circle and landing in Bodo, Norway." (Malesky, 2002)

"Powers was detected by Soviet radar while still fifteen miles from the Afghan-Soviet border. The radar detection was not unusual. In fact, all previous U-2 flights over the Soviet Union had been detected at some point. The previous U-2 flights had not counted on stealth to save them, but on the fact that the Soviets had no fighter jets or, for the first few years, surface-to-air missiles that could fly high enough to shoot it down. However, the newly developed surface-to-air missile, designated as the SA-2 had improved capabilities" (Malesky, 2002).

The U-2 program would again be in the spotlight on October 14, 1962, when it, "photographed the Soviet military installing nuclear warhead missiles in Cuba, precipitating the Cuban Missile Crisis. However, later in the Cuban missile crisis, another U-2 was shot down, killing the pilot, Major Rudolph Anderson." (Burr, 2012).

The CIA armed with the knowledge that the Soviets had developed Surface to Air Missiles (SAMS) that could intercept the U-2, began development of a faster, higher-flying reconnaissance aircraft, even before the U-2 became operational. Lockheed Martin proposed an aircraft codename OXCART that later became the famous USAF SR-71, unofficially known as the "Blackbird." Although the intent of the system was not only to enhance the US intelligence capability, it was more survivable. The speed of the SR-71 would prove to be its survivability capability. "The SR-71 remained the world's fastest and highest-flying operational manned aircraft throughout its career. From an altitude of 80,000 ft (24 km), it could survey 100,000 square miles per hour (72 square kilometers per second) of the Earth's surface. On July 28, 1976, an SR-71 broke the world record for its class - an absolute speed record of 2,193.1669 mph (3,529.56 km/h), and a US "absolute altitude record" of 85,068.997 feet (25,929 m)." (Haynes, 1996). The SR-71 had been fired upon many times, the standard countermeasure was simply to accelerate. Twelve aircraft are known to have been lost, all through non-combat.

Original capabilities for the SR-71 included Optical/Infrared Imagery systems, (the infrared systems were discontinued in the later years of the program) Side Looking Radar (SLR), later Synthetic Aperture Radar System (ASARS-1) an Electronic Intelligence (ELINT) gathering system. Onboard systems recorded sensor information and maintenance data (Malesky, 2002).

UAS now usher in a new era of capabilities and vulnerabilities. "Protocols implemented on the ground station applications enabling communications with the UAVs (and permitting users to pilot them via wireless remote control) were found to be unsecured. This allowed hackers to install malware on the systems running the ground stations. In addition, the telemetry feeds used in monitoring the vehicles and facilitating information transfer through wireless transmission were vulnerable to interception, malicious data injection, and the alteration of pre-set flight paths," (CyberRisk, 2017) Forward progress is not without tradeoffs, as depicted in the chart below, each ISR platform has limiting factors and tradeoffs. See Table 10-1.

Table 10-1 ISR Platform Tradeoffs

SPACE	UAVs	MANNED
LIMITED # ASSETS	VULNERABILITY	VULNERABILITY DRIVEN CONOPS
TRADES BETWEEN QUALITY/REVISIT/SAMPLE RATE	DUTY CYCLE	LIMITED FOOTPRINT
LARGE DATA SOURCE	SMALL FOOTPRINT	DUTY CYCLE
DISSEMINATION & INTEGRATION	RELIABILITY	PREDICTABLE
PREDICATABLE	ATTRITION COSTS	HIGH ACQUISITION & SUSTAINMENT COST
HIGH ACQUISITION COST	Cyber Risk	REGIONAL BASING

Source: (Snyder, 2003)

UAS ISR-Purpose/Market Sector/Product/Economic Opportunity

Purpose of Technology: Intelligence, Surveillance, Reconnaissance for Dual Use-Military-Law Enforcement and Civilian Sectors

Markets Sector Serviced:

Military/Government Applications (Law Enforcement-counter drugs/terrorism etc.)

- ❑ Border Patrol / Monitoring
- ❑ Military monitoring of ports and inland activity for national security
- ❑ Guardian Angel for ground troops
- ❑ Node and Network Discovery
- ❑ Monitor Shipping/Pipeline Monitoring
- ❑ Damage assessment
- ❑ Prevent Movement
- ❑ Re-supply
- ❑ Radio Relay / Translator
- ❑ Chem./Bio Attack Rapid Response

Commercial applications

- ❑ Precision Agriculture (Imagery/Crop Spraying)
- ❑ Humanitarian Assistance and Disaster Response
- ❑ Delivery of Healthcare and Food Supplies
- ❑ Wildlife protection and research
- ❑ Environmental Monitoring/Research
- ❑ Energy/Mining Infrastructure Protection
- ❑ Sports/Media Entertainment and Journalism

Product/ Economic Opportunity:

Information is the product that ISR creates, and unmanned vehicles can provide unprecedented amounts of it. However, there is a need to manage the flood of data. “Data is the new oil,” Intel Corp. Chief Executive Officer Brian Krzanich, he cited a growing competitive “separation” between companies that collect and understand their data and those that do not. A single autonomous car can generate the same data trove as 3,000 people surfing the Internet, while a small drone fleet could easily create 150 terabytes of data per day. (Tyson, 2016). A singe UAS in a single mission can create even more data than a single autonomous car.

Hacking drones is now becoming a market sector all on its own. “Military technology companies from around the world are rushing to design, build, and sell drones that hack and track, while others want to own the business of hacking of the drones themselves. The burgeoning market is foreshadowing battles that could play out in the skies and, for some companies, bring significant profits” (O'Neil, 2018).

Power by the hour offers the ability to sell the information once to a specific customer or to offer it to several customers, allowing for a greater rate of return. A turn-key UAS offering may include the information as a product with training and support of the equipment with a host country owning/controlling/maintaining and operating system or a combination of product sales and service support contracts.

Mission Drives the Sensor Requirements

The mission drives the payload choices, and the payload should drive the platform. In reality this tends to be the reverse. The platform creates compromised trade-offs between a higher quality sensor that weighs more and consumes power versus a lower quality sensor that is less expensive, lighter, but will require more passes to get useable information or will provide a less clean data set. “As military UASs continue to evolve and shrink-think of swarms of tiny drones-their resulting payload footprints pose numerous SWaP (Size, Weight and Power) design space constraints and tradeoffs, together witeh sensor processing, data link bankwith and security issues as well” (Cole, 2016). Keeping in mind that the more passes to collect data can increase the cyber footprint and create needless cyber vulnerabilities. “You can get information much faster if you do the processing in near-real time onboard the aircraft and then get the data down the link” (Cole, 2016).

Standard ISR Camera Sensors

The average payload on a UAS is a passive sensor that does not emit any signals or energy, it sends and or records this data entirely in passive mode. Standard ISR payloads consist of a sensor, normally a camera such as the popular Go-Pro cameras shown below, that offer many user-friendly features while still acquiring high-quality data that can be processed onboard the aircraft, sent down on a live downlink for processing on the ground, or a combination of these techniques. “Military UAS users are seeking actionable intelligence from their sensors in real time-whether the sensor is part of a radar, electronic warfare or ISR sensor chain” (Cole, 2016)

Go Pro Camera Comparison. See Figure 10-2.

Figure 10-2 GoPro Camera Comparisons

Feature	Hero5 Camera	Hero6 Camera	Fusion Camera
Photo	12MP / 30 fps Burst	12MP / 30 fps Burst	18MP / 30 fps
Video	4K30	4K60	5.2K30
Spherical Capture	No	No	Yes
Waterproof	33ft (10m)	33ft (10m)	16ft (5m)
Voice Control	Yes	Yes	Yes
Video Stabilization	Yes	Advanced	Advanced
Quick Stories	Yes	Yes	No
HDR Photo Capture	No	Yes	No
Touch Zoom	No	Yes	No
Auto Low Light	Yes	Yes	No
Exposure Control	Yes	Yes	No

Advanced Wind Noise Reduction	3-mic processing	3-mic processing	4-mic processing
360 Audio	No	No	Yes
GPS	Yes	Yes	Yes
Wi-Fi +Bluetooth ®	Yes	Yes	Yes
5GHz Wi-Fi for Offload to Phone	No	Yes	Yes

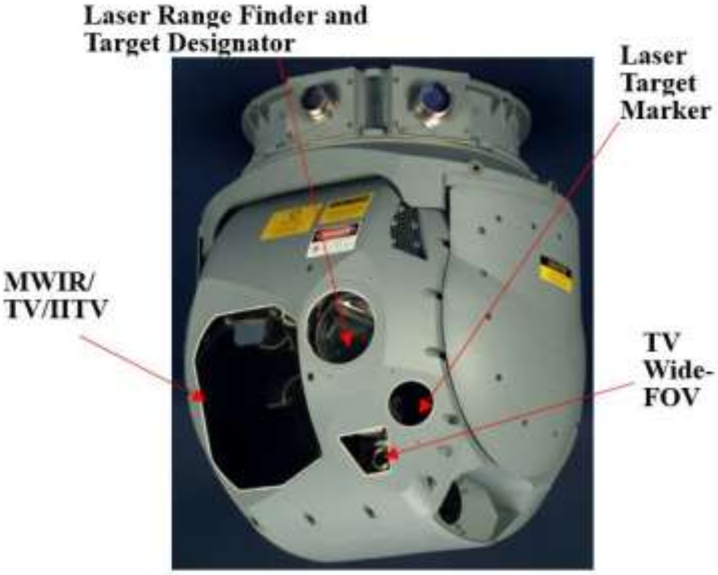
Source: (GoPro, 2018). The Ultimate GoPro. In F. t. R. G. F. You (Ed.), GoPro: GoPro.

Newer designs include the modularity of cameras including a camera that is a, “drone that comes with a 4K camera and has autonomous features… (and is able to) transform the drone into something that can fly, a home security camera, a wearable, or a camera mounted on a stick. It’s a versatile product packed into a single device” (McKalin, 2018).

Multispectral and Hyperspectral Sensors

To gain additional insight into target areas, the use of multispectral and hyperspectral sensors allows for extended data collection. “The main difference between multispectral and hyperspectral is the number of bands and the bandwidths. Multispectral imagery generally refers to three to ten bands. To be clear, each band is obtained using a remote sensing radiometer. A hyperspectral image could have hundreds or thousands of bands” These sensors tend to need copious amounts of power to operate and create pairing issues for datalinks that can handle the amount of data being generated. This is a consideration if the data is going to be encrypted as the data rates will be derogated and real-time monitoring may not be possible. “Multispectral and hyperspectral imagery gives the power to see as humans (red, green and blue), goldfish (infrared) and bumble bees (ultraviolet). We can see even more than this as reflected EM radiation to the sensor”("Multispectral vs Hyperspectral Imagery Explained," 2018). Pictured in Figure 10-3 is Raytheon’s Multi-Spectral Targeting System (MTS) for Predator MQ-1.

Figure 10-3 Raytheon’s Multi-Spectral Targeting System (MTS) for Predator MQ-1



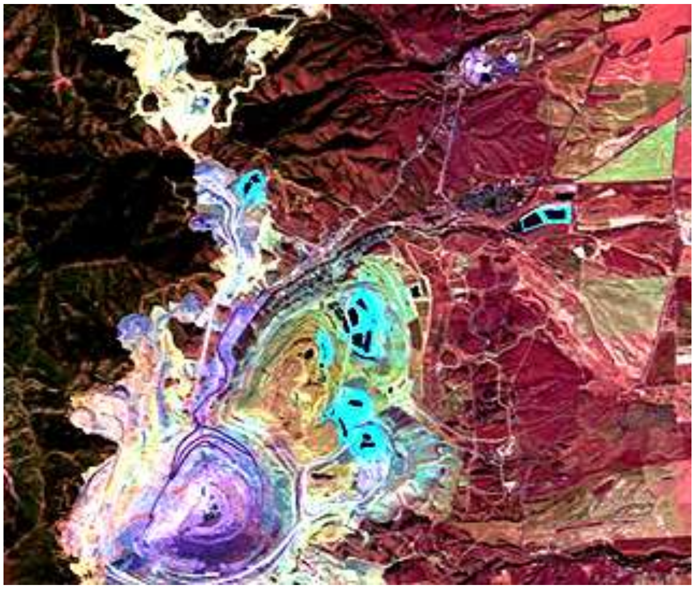
Source: (Snyder, 2003) Snyder, J. (2003). The Latest Tools, Techniques and Opportunities in UAV Design. In. Arlington, VA: Mongo Industries, LLC.

A UAS is an excellent pairing for a multispectral or hyperspectral sensor due to the proximity the UAS allows to the target area and the increase in data collection available in relation to the proximity of the sensor to target.

> “Hyperspectral imaging combines taking pictures of a scene or object, with a spectral view at each point of resolution in the scene. The result is a 3-dimensional data set that can be sliced to view multiple images at separate wavelengths or sliced to show how the spectra vary along different spatial positions across the image in one direction. If the acquisition system or the object is moving, the 4th dimension of time is added.” ("Hyperspectral Imaging," 2018).

Below is a US Government photograph of Arizona mining operations captured with the hyperspectral imaging. See Figure 10-4

Figure 10-4 Hyperspectral Imaging

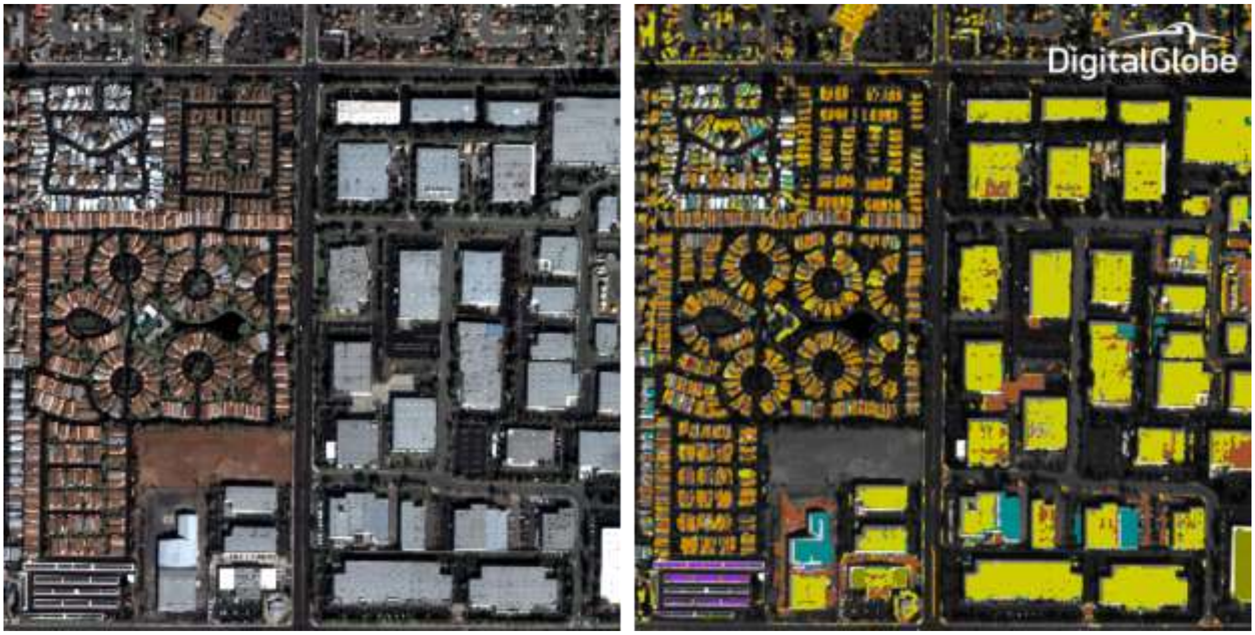


Source: ("Hyperspectral Imaging," 2018) Hyperspectral Imaging. (2018). Hyperspectral Imaging, Retrieved from URL: http://www.sensorsinc.com/applications/military/hyperspectral-imaging/ Multispectral vs Hyperspectral Imagery Explained. (2018). Retrieved from https://gisgeography.com/multispectral-vs-hyperspectral-imagery-explained/

A Changing World Creates a Changing Target Set and Sensor Requirement- SWIR

Since 9-11, the requirements for ISR capabilities quickly moved from the ability to photograph a military installation, or large piece of equipment such as a tank, to the difficult requirement to locate individuals or small groups. “Past reconnaissance needs were more strategic in nature, today's needs are highly tactical, demanding an elevated level of persistence and the ability, in many cases, to identify individual humans in the field of interest. Many approaches have been employed and proposed, but in recent years, the exceptional capabilities of shortwave infrared (SWIR) technology have made SWIR the "Next Generation" of imaging technology for ground, airborne and space technology.” ("Using SWIR in Intelligence, Surveillance, and Reconnaissance (ISR) Military and Security Systems," 2018)

Figure 10-5 Shortwave InfraRed (SWIR) bands

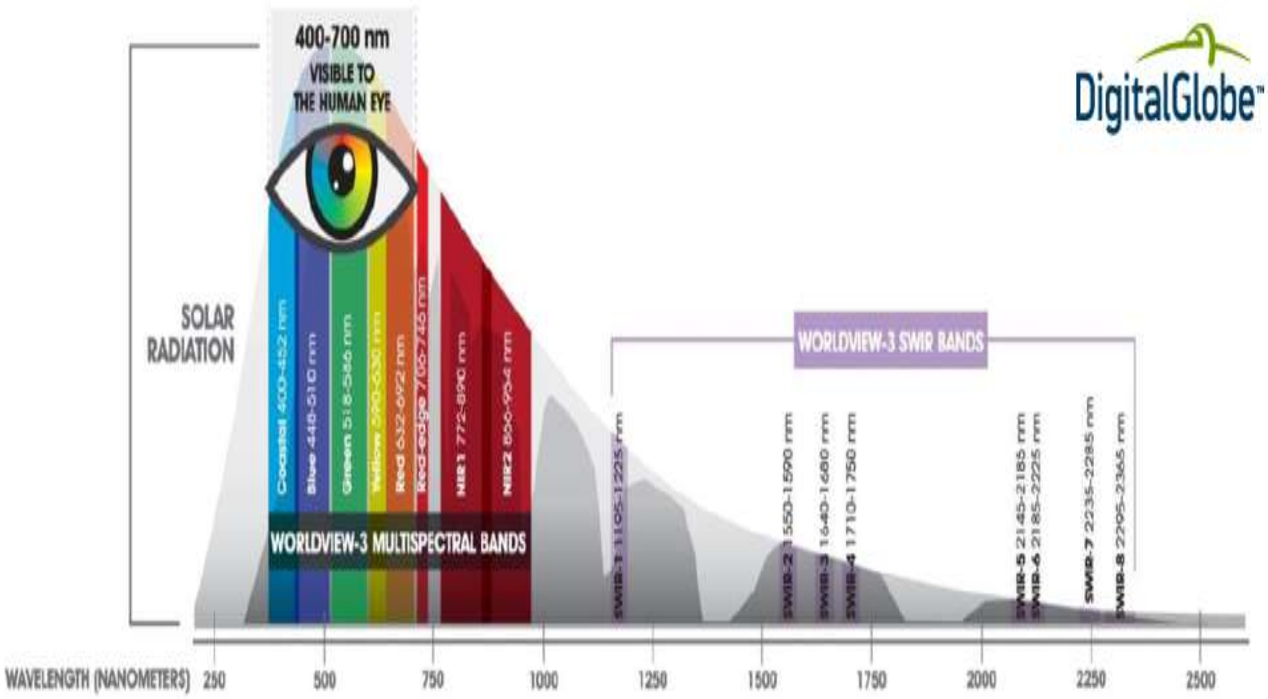


Source: Young, D. (2018). Our eyes can play tricks on us but shortwave infrared (SWIR) imagery reveals all – part 1 of 2. Retrieved from URL: http://blog.digitalglobe.com/technologies/our-eyes-can-play-tricks-on-us-but-shortwave-infrared-swir-imagery-reveals-all-part-1-of-2/

Pictured here is image (Figure 10-5) with eight Shortwave InfraRed (SWIR) bands which are ideal for material identification and mapping. Visible imagery is shown on the left and classification using SWIR imagery is shown on the right. Note that different roof top materials that look the same in the visible imagery are clearly differentiated in the SWIR imagery (Young, 2018).

SWIR cameras and sensors can see reflected light in the shorter wavelengths. Small targets such as humans become distinguishable, with the “typical difference being that all hair shows as white due to the lack of moisture in hair. Conversely, skin shows darker, due to its high moisture content. It is said that long and medium wave sensors provide detection, while SWIR and visible sensors provide recognition.” ("Using SWIR in Intelligence, Surveillance, and Reconnaissance (ISR) Military and Security Systems," 2018). This spectrum is illustrated below, and it is easy to see why using SWIR sensors on a UAS is an advantage over the old ISR sensors. See Figure 10-6.

Figure 10-6 SWIR advantage over old ISR sensors



Source: Young, D., (2018). Our eyes can play tricks on us but shortwave infrared (SWIR) imagery reveals all – part 1 of 2. Retrieved from: http://blog.digitalglobe.com/technologies/our-eyes-can-play-tricks-on-us-but-shortwave-infrared-swir-imagery-reveals-all-part-1-of-2/

Bomb-Sniffing Drone Technology

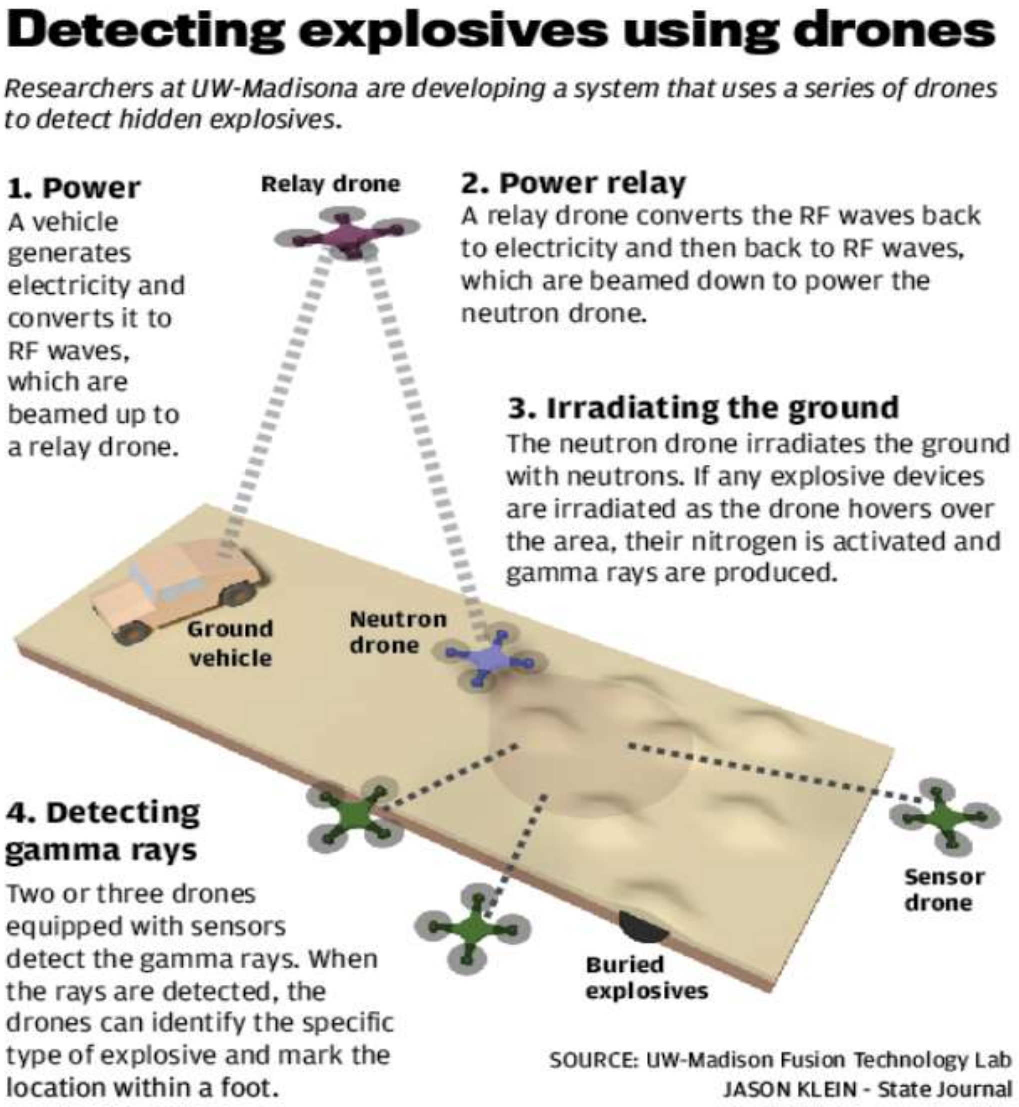
UAS can be outfitted with sensor suites that can detect improvised explosive devices and other active landmines from past wars. This not only offers direct security, but it also offers a safer way to detect landmines. "Sensors look for gamma rays or other particles with the signatures of specific materials, such as explosives or a nuclear device. It is the same technology used at security checkpoints to scan luggage and shipping containers in airports, but the breakthrough for the UW-Madison scientists was making the radiation source small enough to mount on a drone" (R. Schultz, 2016). Drug and bomb-sniffing drones can detect dangerous chemicals from 1.8 MILES away." Unmanned drug-sniffing drones have been introduced in the Netherlands. They fly over houses (video), sniff for weed and scan for grow lights. Police say they are not breaking the law because the samples can be taken without entering the building." (Zenpus, 2009). See Figure 10-5 for bomb sniffing logic for UAS Figure 10-5 for bomb sniffing logic for UAS.

Cave Mapping

Unique missions' development will mean the UAS uses are only limited to the innovation of the operator and limits of physics. One such application is the mapping of underground mines, normally a dangerous job attempted by humans, it is one that UAS are well suited to accomplish. UAS, "will be able to carry out safety checks by monitoring the build-up of water and checking the extent of roof collapses, and search for valuable mineral deposits that may have been missed" (Hambling, 2017).

A standard quad-copter UAS is outfitted with, “powerful LED lights, cameras, and sonar. Initially, they tried flying it using the drone’s on-board camera to guide them, an approach known as First Person View (FPV) piloting” (Hambling, 2017).

Figure 10-7 for bomb sniffing logic for UAS



Detecting explosives using drones

Researchers at UW-Madisona are developing a system that uses a series of drones to detect hidden explosives.

1. Power
A vehicle generates electricity and converts it to RF waves, which are beamed up to a relay drone.

2. Power relay
A relay drone converts the RF waves back to electricity and then back to RF waves, which are beamed down to power the neutron drone.

3. Irradiating the ground
The neutron drone irradiates the ground with neutrons. If any explosive devices are irradiated as the drone hovers over the area, their nitrogen is activated and gamma rays are produced.

4. Detecting gamma rays
Two or three drones equipped with sensors detect the gamma rays. When the rays are detected, the drones can identify the specific type of explosive and mark the location within a foot.

SOURCE: UW-Madison Fusion Technology Lab
JASON KLEIN - State Journal

Source: Schultz, R. (2016). Bomb-Sniffing Drone Technology. Retrieved from: https://www.uasvision.com/2016/04/29/bomb-sniffing-drone-technology/

Using a multi-mission sensor suite, the variety of data that can be collected and stored in a brief period is far superior to human lead collections. “Sonar sensors, which use sound waves to detect objects, produce less data than video cameras. This means they can be used to create a 3D model more quickly, possibly even in real time…the sonar model is less accurate; a yet-to-be-published paper shows that it provides effective navigation. Given that it uses fewer data and therefore less processing power, the mapping could potentially be done onboard the drone” (Hambling, 2017).

UAS offers the ability to create modular designs for sensor suites, allowing many options for data acquisition to be tested in a short amount of time. This offers the ability to determine the best mix of sensors, platforms, and data acquisition capabilities, "we are also experimenting with lidar, which maps using lasers. Also, they are running tests with data from X-ray fluorescence analyses, which detect different elements, to train machine learning to identify minerals in rock walls." (Hambling, 2017).

Mission and Sensor Planning and Considerations

Several issues must be considered in planning a successful UAS mission in order to acquire the required data in a useable format, in a timely and secure manner as "the next front in the cyberwar is literally above your head" (O'Neil, 2018). Information can be stored on the vehicle for later retrieval, or it can be real time or near real time sent back to the ground for processing. Several factors will determine the optimal method to obtain and secure the information, including encryption threat environment, timeliness, and the consequences (if any) if the information is intercepted or compromised. "Maldrone backdoor malware kit has been developed as a universal hack, applicable to all makes and models of UAV. Maldrone silently interacts with a drone's device drivers and sensors, allowing the user to hijack and control the UAV remotely" (CyberRisk, 2017). The below graphics offer some sense of planning that must be done in looking at flight paths and sensor limitations, including security of the information.

One technique for securing information that must be sent using non-secure or hackable methods is to obfuscate the true data that is being collected. This can be done by increasing the number of passes and collecting a larger dataset than the mission requires, effectively flooding the sensor with data so an adversary would not be able to discern the truly valuable data from the noise. "Poorly secured or unsecured wireless networks are particularly vulnerable, with attack scenarios envisaged where compromised or purpose-bought UAVs could be flown or discreetly landed near a hot spot and used to stage Man in the Middle (MIM), data injection, and similar attacks over guest and short-range Wi-Fi, Bluetooth, and other wireless connections. The success of such attacks might be bolstered by the fact that traditional security measures operate on the assumption that no-one could get close enough to such short-range wireless connections to pose a serious threat". (CyberRisk, 2017)

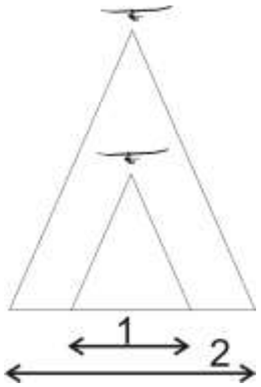
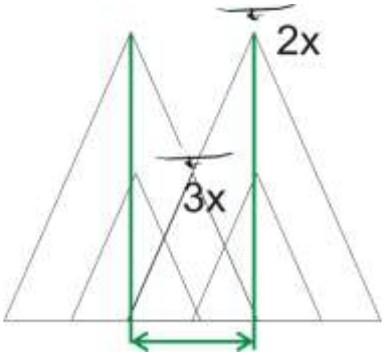
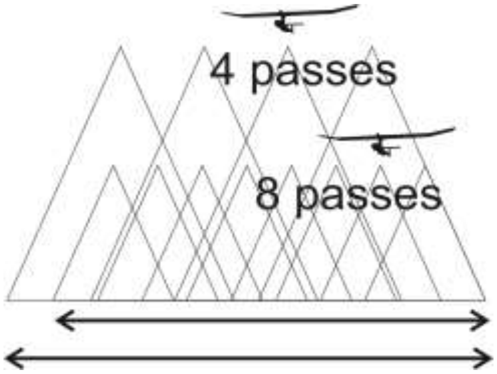
"As depicted in Table 10-2 below a mission that might only need one or two passes at a lower altitude, instead might be flown at multiple altitudes and additional passes over the target allowing for the obfuscation of the true targeted data. This technique also allows for additional data analysis on an area, however, due to storage, data links, timing and threat environments this technique is not always employed." (Bosak, 2014)

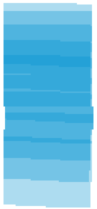
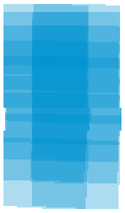
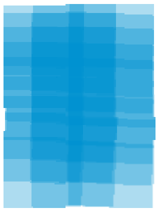
"One easily can deduce 72km^2 map surface in a single direction straight flight.

However, assuming returning flight and only 60% overlap, one gets (100%+40%) *720m=1008m strip width and only one hour of flying in one direction.

This yields only 50.4km^2 map surface with returning flight." (Bosak, 2014)

Table 10-2 “Surface, map shape, and flight altitude” (Bosak, 2014)

 “If you are mapping a linear object, doubling the altitude, you are doubling surface coverage” (Bosak, 2014)	 “Choosing to make two passes may improve geometry matching, because of overlap requirement, flying high you are reducing flight time only by about 1/3, because outside regions have valid bitmap but poor geometry.” (Bosak, 2014)	 “With regular map shape and multiple passes, flying two times higher requires two fewer passes and flight time and provides an extra surface at map edges. However, the area should be flat as there will be no multi-angle information allowing to orthonormalize high objects along the edges.” (Bosak, 2014)

 “A single-leg mission. Typical along-overlap is high, around 75-90%.” (Bosak, 2014)	 “Two-leg mission. Typical 60% side-overlap shown. Along-overlap 75-90%.”	 “Three-leg mission. Typical 60% side-overlap shown.” (Bosak, 2014)

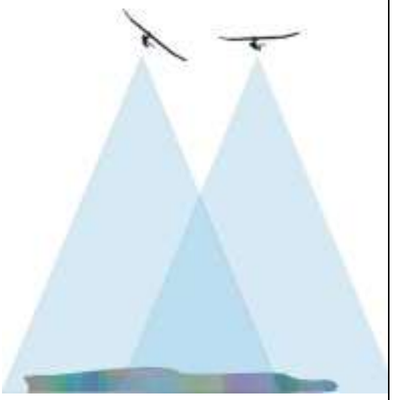
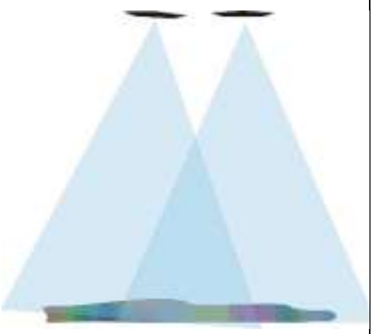
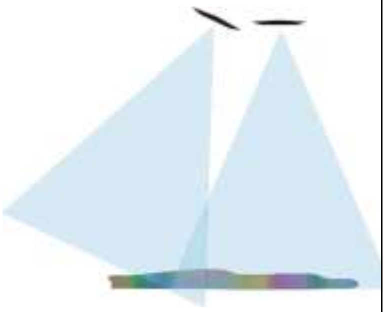
	(Bosak, 2014)	

Source: (Bosak, 2014)

Importance of stabilized head

“Since increasing overlap is so costly in mission time and so important in urban areas, UAS can use roll-stabilized head and has aerodynamic design successfully attenuating oscillations in pitch and yaw axes. The use or roll-stabilized head increases useful surface during turns and increases processing success rate thanks to overall more predictable photo properties. See Figure 10-8.” (Bosak, 2014)

Figure 10-8 Importance of stabilized head

 “With stabilized head, the overlap stays guaranteed, even in turns.” (Bosak, 2014)	 “Without the stabilized head, typical deviations of a few degrees already require extra few percent of overlap pre-planned. This is costly regarding flight time and worsens significantly during windy weather.” (Bosak, 2014)	 “Without the stabilized head, photos taken during turns are completely useless for reconstruction, typically overlapping by few degrees and only in corners. No airplane can make a full turn that is flat.” (Bosak, 2014)

Source: (Bosak, 2014). Secrets of UAV Photomapping. Retrieved from URL: http://ww1.aerialrobotics.eu/pteryx/pteryx-mapping-secrets.pdf

“Both small UAV like flying wings and even large UAS with several meters wingspan tend to respond for navigation with changing 0-5 deg roll both directions even when ordered to ‘fly straight’ over the ground. The reason is, while the ground path is straight, the wind blows in any direction, usually as much as 45 deg different at altitude than at ground level, with little direction change but much more wind speed variation. This means the UAS has to bank left and right all the time in order to stay on its path"

Protecting the Systems from the Cyber Threat

Sensors, datalinks, platforms and power supplies tend to be built independently without cyber protection standards built in leaving the systems vulnerable. The very nature of "plug and play" tends to create incompatibility in cyber protection with virtually no data standards.

"Analysis of the configuration and flight controllers/microprocessors of several popular UAV models having multiple rotors revealed weaknesses associated with both the telemetry links streaming data to and from a drone via serial port connections (in which information could be captured, modified, or injected), and the UAVs' connections to their ground station interface (whose data link could be spoofed, enabling hackers to assume complete control of the vehicle)" (CyberRisk, 2017).

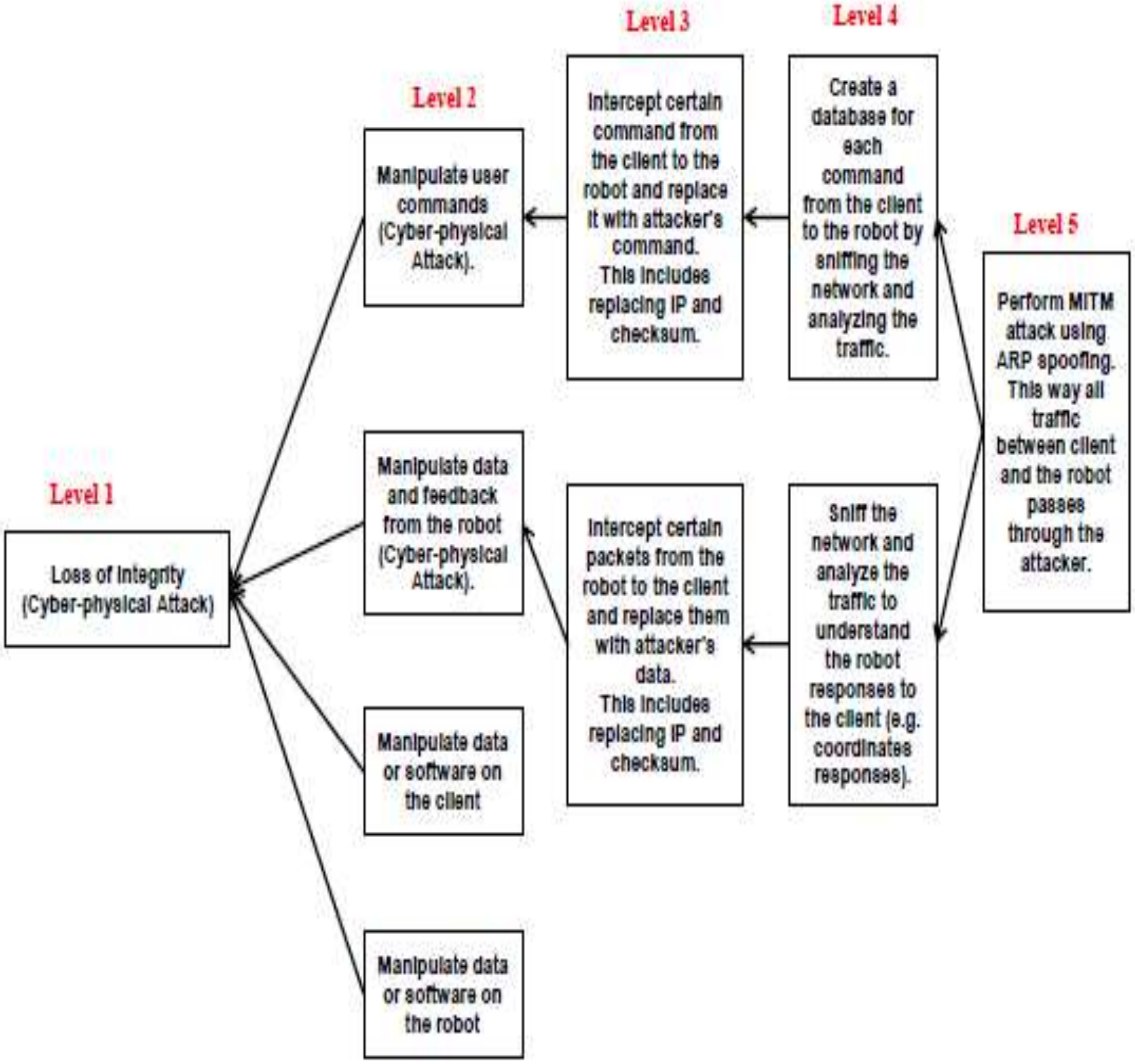
The dangers of weak security protocols is becoming more apparent as reported by CNN on December 17, 2009 as, "Insurgents were able to use a mass-market software program to view live feeds from U.S. military Predator drones monitoring targets in Iraq. There also is evidence that UAV feeds also have been hacked in Afghanistan, but there was no evidence the militants were able to take control of the remote aircrafts' systems in either country. The inexpensive software, created by a Russian company called SkyGrabber, is downloadable off the Internet. It allows users to take advantage of unprotected communication links in some of the UAVs" (Mount & Quijano, 2009).

An attacker can have many objectives in launching an attack. Possible goals include the loss of data integrity, the link to the vehicle, or the payload. An example of an attack tree that demonstrates different branches of attacks based on a MIM attack is shown below in Figure 10-7.

"The loss of integrity (Level 1 of the attack tree) is achieved by manipulating the communication stream between the client and the server creating cyber-physical impacts. The branches of the tree represent the methods attackers can achieve their goal. The arrows in the attack tree indicate the sequence through which each attack proceeds" (Ahmad Yousef et al., 2018).

Encryption offers some level of protection.

Figure 10-9 MIM Attack Effects


Level 1
Loss of Integrity (Cyber-physical Attack)
Level 2
Manipulate user commands (Cyber-physical Attack).
Manipulate data and feedback from the robot (Cyber-physical Attack).
Manipulate data or software on the client
Manipulate data or software on the robot
Level 3
Intercept certain command from the client to the robot and replace it with attacker's command. This includes replacing IP and checksum.
Intercept certain packets from the robot to the client and replace them with attacker's data. This includes replacing IP and checksum.
Level 4
Create a database for each command from the client to the robot by sniffing the network and analyzing the traffic.
Sniff the network and analyze the traffic to understand the robot responses to the client (e.g. coordinates responses).
Level 5
Perform MITM attack using ARP spoofing. This way all traffic between client and the robot passes through the attacker.

Source: Ahmad Yousef, K. M., AlMajali, A., Ghalyon, S. A., Dweik, W., & Mohd, B. J. (2018) Analyzing Cyber-Physical Threats on Robotic Platforms. Sensors (Basel, Switzerland), 18(5), 11-12. doi:10.3390/s18051643

However, compromises occur due to mission requirements. Encryption can overload data links, take up valuable bandwidth and cause undesirable flight and control characteristics if a real time data link and control is required for the mission. Not using encryption is a trade-off that a Pentagon official said, “that many of the UAV feeds need to be sent out live to numerous people at one time, and encryption was found to slow the real-time link. The encryption therefore was removed from many feeds. Removing the encryption, however, allowed outsiders with the correct tools to gain unauthorized access to these feeds” (Mount & Quijano, 2009).

“Is there a perfect solution to the security issues involved in UAS operations? No. There is always a degree of risk to be mitigated.” (Nichols, 2002) However, what if a the UAS payload or flight control systems is lost to a hacker or an enemy nation it would be advisable to build a way of remotely disabling or destroying the information, sensor and or vehicle? Over the years many concepts and ideas have come forward including the idea of a “zero out” chip that would automatically delete all information on a UAS upon a compromised status. Cornell University and Honeywell Aerospace in laboratory testing is developing a method of vaporizing electronic circuits, without laying a hand on the actual device.

The design method is, “When the shell is exposed to a certain frequency of radio waves, tiny graphene-on-nitride valves between the cavities open, allowing the chemicals to mix and react. Along with applications such as data protection, it is hoped that the technology might also find use in things like environmental sensors that can be remotely vaporized once they're no longer needed” (Coxworth, 2018).

Conclusions

Although ISR payloads have increased in capability and the wide range of data collections, the goals and mission of remote sensing platforms remain constant. The ISR platforms and the sensors that they carry stared off as balloons, and went into airplanes, then into satellites, and are now being put into unmanned aerial systems with modular payloads, allowing vast amounts of information to be collected.

The wide variety of sensor payloads should drive the missions and data collects, however in the real world it is often the platform that dictates the sensors choices, which can impact the ability to collect the data required. The weight and power requirements of the sensor must be considered when planning the flights. The mission profile (number of passes and angles) are all considerations when pairing a sensor with a platform including all mission data collection parameters that drive the ISR requirements. Sensor data security and the threat of attacks within the cyber domain must be addressed. Mission planning will require tradeoffs between access to the target area, sensor capability and availability, information time dominance and cyber/data security requirements.

Students are encouraged to continue researching and learning about the new sensors systems, data links and cybersecurity techniques for use on UAS. As the market expands, more sensors will be built and optimized specifically for UAS, leading to more cyber attacks and the vulnerability of the data, as well as the UAS vehicles before during and after missions.

Discussion questions

1. How could you use physical security and UAS flight characteristics to supplement a UAS cybersecurity plan?
2. How has UAS changed the nature of ISR after the attacks on 9-11?
3. What sensors would you use to map the health of agricultural crops?
4. What is the best way to secure the data collected by UAS, collecting it and storing onboard or using data links to process the information on the ground? Please explain your answer.
5. Name three unique missions that UAS payloads are configured for today that in the past humans would have been assigned to do. Research three additional missions’ payloads and discuss how these payloads are being integrated on UAS.

Bibliography

Bosak, K. (2014). *Secrets of UAV Photomapping.* Retrieved from http://ww1.aerialrobotics.eu/pteryx/pteryx-mapping-secrets.pdf

CyberRisk. (2017, March 16). *he Usage of Drones in Cyber Attacks – Both as Targets for Attack and as Potential Attack Vectors.* Retrieved from CyberRisk Blog: https://www.cyberisk.biz/the-usage-of-drones-in-cyber-attacks/

Malesky, L. A. (2002). Just one more U-2 overflight of the Soviet Union was one too many for Francis Gary Powers. *Military History*, pp. 19(5), 26. .

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

Readings

Ahmad Yousef, K. M., AlMajali, A., Ghalyon, S. A., Dweik, W., & Mohd, B. J. (2018). Analyzing Cyber-Physical Threats on Robotic Platforms. *Sensors (Basel, Switzerland), 18*(5), 11-12. doi:10.3390/s18051643

Barnes, T. (2005). Mayday for the U-2. Retrieved from http://area51specialprojects.com/u2_mayday.html

Bellis, M. (2017). The History of Photography: Pinholes and Polaroids to Digital Images. Retrieved from https://www.thoughtco.com/history-of-photography-and-the-camera-1992331

Burr, W. (2012). *Cuban Missile Crisis Day by Day: From the Pentagon's "Sensitive Records".* Washington, DC: National Security Archive Electronic Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB398/.

Cole, S. (2016). Small UAS payloads pose Swap and bandwidth challenges. Retrieved from http://mil-embedded.com/articles/small-pose-swap-bandwidth-challenges/

Coxworth, B. (2018). Circuits self-destruct in response to radio waves. Retrieved from https://newatlas.com/radio-waves-vaporize-electronics/53134/

FLIR Launches Next-Generation Black Hornet 3 Nano-UAV. (2018). Retrieved from https://www.businesswire.com/news/home/20180605005630/en/FLIR-Launches-Next-Generation-Black-Hornet-3-Nano-UAV

GoPro. (2018). The Ultimate GoPro. In F. t. R. G. F. You (Ed.), *GoPro*: GoPro.

Hambling, D. (2017). Drone maps mines to explore unsafe caverns and seek out minerals. Retrieved from https://www.newscientist.com/article/2127123-drone-maps-mines-to-explore-unsafe-caverns-and-seek-out-minerals/

Haynes, L. (1996). SR-71 World Record Speed and Altitude Flights. Retrieved from http://www.wvi.com/~sr71webmaster/spd_run001.html

Hyperspectral Imaging. (2018). Retrieved from http://www.sensorsinc.com/applications/military/hyperspectral-imaging/

King, F. (2012). Kite Photo of Post-Quake San Francisco (1906). Retrieved from http://www.bigmapblog.com/2012/kite-photo-of-post-quake-san-francisco-1906/

Lambeth, B. S. (2006). Air Power Against Terror: America's Conduct of Operation Enduring Freedom. In. Santa Monica, CA: RAND Corporation.

Lillesand, T., Kiefer, R. W., & Chipman, J. (2014). *Remote Sensing and Image Interpretation*: Wiley.

Lucibella, M. (2013). January 2, 1839: First Daguerreotype of the Moon. Retrieved from https://www.aps.org/publications/apsnews/201301/physicshistory.cfm

McKalin, V. (2018). PITTA Is a Modular Camera That Can Transform into a Drone. Retrieved from https://sanvada.com/2018/01/02/pitta-modular-camera-can-transform-drone/

Mount, M., & Quijano, E. (2009). Iraqi insurgents hacked Predator drone feeds, U.S. official indicates. Retrieved from http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html

Multispectral vs Hyperspectral Imagery Explained. (2018). Retrieved from https://gisgeography.com/multispectral-vs-hyperspectral-imagery-explained/

O'Neil, P. (2018). Drones emerge as new dimension in cyberwar. Retrieved from https://www.cyberscoop.com/apolloshield-septier-drones-uav-cyberwar-hacking/

Schultz, C. (2013). This Picture of Boston, circa 1860, Is the World’s Oldest Surviving Aerial Photo. Retrieved from https://www.smithsonianmag.com/smart-news/this-picture-of-boston-circa-1860-is-the-worlds-oldest-surviving-aerial-photo-14756301/#RohlhYJZRcJzyVy7.99

Schultz, R. (2016). Bomb-Sniffing Drone Technology. Retrieved from https://www.uasvision.com/2016/04/29/bomb-sniffing-drone-technology/

Snyder, J. (2003). The Latest Tools, Techniques and Opportunities in UAV Design. In. Arlington, VA: Mongo Industries, LLC.

Tyson, M. (2016). "Data is the new oil" declares Intel CEO Brian Krzanich. Retrieved from http://hexus.net/ce/news/automotive/99277-data-new-oil-declares-intel-ceo-brian-krzanich/

The Usage of Drones in Cyber Attacks – Both as Targets for Attack and as Potential Attack Vectors. (2017). Retrieved from https://www.cyberisk.biz/the-usage-of-drones-in-cyber-attacks/

Using SWIR in Intelligence, Surveillance, and Reconnaissance (ISR) Military and Security Systems. (2018). Retrieved from http://www.sensorsinc.com/applications/military/swir-for-isr

Young, D. (2018). Our eyes can play tricks on us but shortwave infrared (SWIR) imagery reveals all – part 1 of 2. Retrieved from http://blog.digitalglobe.com/technologies/our-eyes-can-play-tricks-on-us-but-shortwave-infrared-swir-imagery-reveals-all-part-1-of-2/

Zenpus, S. (2009). Drug-Sniffing Drones Take to the Skies in the Netherlands. Retrieved from https://hardware.slashdot.org/story/09/04/30/1629253/drug-sniffing-drones-take-to-the-skies-in-the-netherlands