SYM-AM-22-048

Excerpt from the Proceedings of the Nineteenth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 11–12, 2022

Published: May 2, 2022

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Reducing Asymmetry in Countering Unmanned Aerial Systems

Captain Christian Thiessen—is an Infantry Officer in the Marine Corps. Currently he is a Graduate Student seeking a dual degree in information warfare systems engineering and applied design for innovation at the Naval Postgraduate School. His thesis is titled Redesigning the Counter-Unmanned Systems Architecture. [christian.thiessen@nps.edu]

Dr. Douglas L. Van Bossuyt—is an Assistant Professor in the Systems Engineering Department at the Naval Postgraduate School in Monterey, CA. His research focuses on the nexus of failure and risk analysis, functional modeling and conceptual system design, trade-off studies and decision-making, and resilient systems. He has published over 60 peer reviewed technical journal articles and conference papers on these and related topics and holds two U.S. patents. He holds a PhD in mechanical engineering with a minor in industrial engineering from Oregon State University. [douglas.vanbossuyt@nps.edu]

Dr. Britta Hale—is a Cryptographer and Assistant Professor in Computer Science at the Naval Postgraduate School in computer science. Hale has a PhD from the Norwegian University of Science and Technology (NTNU) and a Master of Science from Royal Holloway University of London (RHUL). Her focus areas include cryptography and cryptographic applications, extending to security applications for uncrewed systems and counter-uncrewed systems, and other emerging environments and technologies. She has experience in industry research on security for critical systems. Hale is a member of the Internet Engineering Task Force (IETF) and International Association for Cryptologic Research (IACR). [britta.hale@nps.edu]

Abstract

Current Counter Unmanned Aerial Systems (C-UAS) rely heavily on low-efficiency techniques such as broadband radio frequency (RF) jamming and high-intensity lasers. Not only do such techniques come at the cost of second and third order effects—such as collateral jamming risks to operational systems, a large RF footprint, and high energy use—but they also present an asymmetry between threat and response. Many commercial, off-the-shelf UAS devices are inexpensive compared to the C-UAS systems historically under focus in Department of Defense (DoD) acquisition. This work argues for leveling that asymmetry by exploring C-UAS autonomy-on-autonomy options by using cyberattack payload capabilities residing on a UAS. By reducing the attack surface to focus on a particular target, these cyber techniques provide scalpel-edged control to the operator, reducing risk to own systems, RF footprint, and collateral damage.

Keywords: UAS, C-UAS, electronic warfare, cyber, secure acquisitions, advancement of military operations

Introduction

In the past decade, unmanned aircraft systems (UAS) have proliferated on the battlefield, giving technologically inferior combatants an advantage over their more sophisticated and numerically superior competitors. This was never more evident than in 2014 when ISIS used consumer UASs to surveil and target coalition forces during fighting in Raqqa, Syria (Almohammad & Speckhard, 2017). Then in the 2017 battle to retake the city of Mosul, the terrorist group leveraged their Facebook and Twitter presence to record and post jaw-dropping videos of their ambushes using UASs retrofitted with grenades (Warrick, 2017). Several years later, the 2020 Nagorno-Karabakh War between Armenia and Azerbaijan further demonstrated the need for robust short-range air-defense to counter-unmanned aircraft systems (C-UAS) when the numerically inferior Azeri military dismantled the Armenian army and destroyed over 350 armored vehicles (Sukhankin, 2021a, 2021b). More recently, Ukraine achieved remarkable success against the Russians using the same tactics and equipment as the Azeris (Perrigo, 2022). These examples show how poor and technologically inferior combatants can employ inexpensive technology in a sophisticated manner to negate an opponent’s center of gravity.

This is telling given what is known about asymmetric warfare: By engaging in a war of asymmetry, where an actor’s interests and political vulnerability are inversely proportional, strong actors are more likely to lose opposite approach interactions (Arreguin-Toft, 2005). Taking the lessons from Ivan Arreguin-Toft’s research as well as the initial results of the American war in Afghanistan, it is clear that the best way for a stronger combatant to counter asymmetry is by taking an indirect approach of their own.

		Weak Actor Strategic Approach	
		Direct	Indirect
Strong Actor Strategic Approach	Direct	Strong Wins	Weak Wins
	Indirect	Weak Wins	Strong Wins

Figure 1. Strategic Approach Model. (Arreguin-Toft, 2005; Figure 3)

In this work, we consider the current C-UAS approach and technologies and assert that instituting a constellation of aerial security patrols tasked with UAS interdiction will provide installation commanders a more robust method for countering the asymmetric threat posed by UASs. Networking stand-in electronic warfare (EW) and cyber-attack devices provides a layered perimeter to augment the current systems with persistent deterrence that mimics the security patrols used in modern defensive operations.

This paper will begin with a discussion on what makes a modern defense-in-depth approach successful, then move onto a more technical discussion on electronic warfare and cyber-attack methods. Additionally, this paper will cover the countermeasures currently in procurement by the Department of Defense (DoD) and the Department of Homeland Security (DHS). Finally, this paper will conclude with two example scenarios in which this framework could be adopted by the DoD and DHS acquisition communities to create the most effective means of countering unmanned aircraft.

Defense-in-Depth

Marine Corps Warfighting Publication 3-01, *Offensive and Defensive Tactics*, defines a defensive operation as “an operation conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable to offensive or stability operations” (U.S. Marine Corps, 2019). Defensive operations create the conditions that allow a friendly force to recover and regain operational initiative by denying an enemy’s access to vital areas or by eroding an enemy’s ability to concentrate firepower in an attack. While there are myriad defensive positions to analyze, they are designed to defend-in-depth using a main engagement area, a support area, and a security area where forward positioned troops gather information and interdict the enemy. In the example shown in Figure 1, the defenders use the perimeter defense to give 360-degree coverage of a vital asset, which in the case of C-UAS would be the defense of a military base or installation.

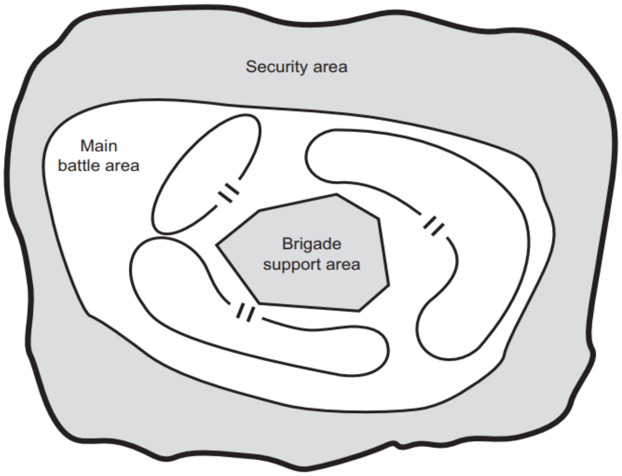

Figure 2. Sample Perimeter Defense (Figure 9-1; U.S. Marine Corps, 2019)

Defensive operations are characterized by maneuver, preparation, flexibility, mutual support, and surprise to disrupt an adversary's attack momentum. In a defense-in-depth, this is achieved by engaging the enemy at the earliest opportunity with security forces as well as moving reserve and fire support units to a position of advantage (U.S. Marine Corps, 2002). This gives the defense a buffer against an attacker's main thrust, ensuring the attacker commits their forces in piecemeal fashion, and preventing them from massing firepower where they intend.

In the context of defending infrastructure against adversarial UAS, the goal of the defense is to maintain normal operations without interruption or degradation from an attack. Given that most bases and critical infrastructure in the continental United States have defined physical perimeters with restricted operating zones for aircraft to fly in and out of, the main engagement area in the C-UAS fight becomes a matter of procedure based on local environmental restrictions (Air Land Sea Application Center, 2019). In defensive operations, this engagement area development establishes control measures and trigger lines to outline specific weapons and actions to be taken given a set of circumstances. These escalation of force procedures are well-defined for human incursions onto a military facility, yet they remain immature in the C-UAS fight.

In the planning process for carrying out defense-in-depth, the Marine Corps teaches its officers seven steps of engagement area development (U.S. Marine Corps, 2017). One of the first actions taken is to gain depth in the battle space by launching security patrols to interdict would-be attackers. These security patrols are designed to increase the situational awareness of the ground force commander and are given with several guiding principles: observe, report, and protect against enemy infiltration or ambush (U.S. Marine Corps, 2000). This may, or may not, require a security patrol to engage the enemy kinetically, making it an essential tool for the successful execution of a ground commander's mission.

This begs the question, why is there not a similar process for defending U.S. bases and infrastructure against adversarial UASs? We believe the answer is that there has yet to be a serious incursion or multi-wave attack using only unmanned systems. The current method for defending military installations and critical infrastructure from UAS incursions mirrors the static defense of forts and castles rather than the maneuverable defenses of the 21st century. If defensive positions are supposed to be designed for maneuver and flexibility, a defense in the current C-UAS landscape is anything but. Instead of adhering to traditional escalation of force procedures, the current C-UAS architecture uses the most capable weapons first, like the CACI

Skytracker (Pitsky, 2021) and Anduril Sentry Tower (Anduril, 2021) first. As a metaphor for defensive operations, this is more akin to opening fire with crew-served weapons instead of beginning an engagement with security patrols and harassing fires. Ultimately, the lack of defensive layers allows an attacker increased mobility to target the defender's most lethal assets.

With an understanding of the current systems and how they match, or do not match, customary planning guidance, the DoD and DHS should incorporate the concept of aerial security patrols into the C-UAS framework. To fully realize this, friendly unmanned platforms can be terrestrially or aerially deployed to act as patrols, giving installations a forward presence to assist in the full gamut of C-UAS kill-chain actions. Because many of the kill-chain functions can be offloaded and stripped away to the main sentry tower, these C-UAS devices can be modular and customizable enough to meet the form, fit, and function of the host device.

Electronic Warfare in the C-UAS Kill-Chain

To limit collateral damage and to increase effectiveness in countering unmanned systems, the DoD and DHS have focused their efforts on the non-kinetic electronic warfare technology built by Anduril, CACI, Sierra Nevada Corporation, and Lockheed Martin. Electronic warfare has three subcomponents: electronic attack, electronic support, and electronic protection, the first two being the most important to the purpose of this paper. Electronic support in C-UAS consists of the techniques conducted in the first three steps of the kill-chain, "Detect, Track, and Identify," while electronic attack consists of the techniques to "Mitigate" an adversarial UAS. This section will primarily focus on the electronic attack techniques contained within radio frequency (RF) jamming.

RF jamming is designed to sever the communication link between a UAS and its ground control station (GCS) by injecting substantial amounts of electromagnetic energy, referred to as noise, into a receiving antenna (Parlin et al., 2018). Uplink jamming disrupts the receiving antenna of the target UAS, while downlink jamming interferes with the receiving antenna of the GCS (Lichtman et al., 2016). Uplink and downlink jamming can be accomplished by two types of jammers: stand-off and stand-in. Stand-off jammers are devices that exist among friendly forces, typically employed as terrestrial or aerial platforms (e.g., the MADIS and EA-18G Growler). Stand-off jammers are notorious for consuming copious amounts of power to overcome the free-space path loss associated with their use. Stand-in jammers exist amongst their targets but must be located closer to their target, requiring a host-device or person to decrease the distance to their target (Brown et al., 2007).

RF jamming, also referred to as noise jamming, uses a jamming carrier signal modulated with a random noise waveform to disrupt the communication by inserting Gaussian noise into the receiver. The bandwidth of the jamming signal can be as wide as the entire spectrum width used by the target or as narrow as a single channel (Poisel, 2011). The former refers to broadband, full-band, or barrage jamming to place noise energy across the entire width of the frequency spectrum used by the target. This technique is useful against all communications by placing the jammer between an adversary's communication links. To mitigate fratricide, directional antennas are used to avoid interference with friendly communications in the same frequency band (Stutzman & Thiele, 2013). Because broadband jamming generates a signal like broadband noise, the jamming power is lowered to meet the needs of the entire frequency band. Additionally, since broadband jamming raises background noise levels, it can attack the synchronization and tracking processes of the communication scheme it is going after (Poisel, 2011). It may be obvious, but the primary limitation with broadband jamming is its inefficient consumption of power, which necessitates a large system size, and the likelihood to inflict unintentional collateral damage to adjacent communication systems.

Communications engineers are constantly designing and employing techniques to lower the probability of communications detection (LPD), interception (LPI), and exploitation (LPE), while expanding access to multiple users (Sklar, 2001). This led engineers and system designers to spread spectrum signal modulation techniques through two primary techniques: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS; Sklar, 2001). Both FHSS and DSSS are considered “anti-jam” communications schemes because they vary the frequencies used, use time hopping, and implement narrow-beam antennas to put the jammer at a significant disadvantage.

However, just because the signal has anti-jam properties does not mean the signal is impervious to disruption. This is due to the notion that the intelligibility of information transfer can be sufficiently degraded by partial jamming (e.g., jamming only 30% of a voice transmission degrades the transfer; Poisel, 2008). Therefore, to negate anti-jam properties, a jammer can use an unmodulated carrier signal centered on the transmitting frequency that can be modulated with tone signals or with a variable-bandwidth noise signal. These tones are placed on specified frequencies identified from prior target knowledge to raise the noise floor and prevent signal reception (Poisel, 2011).

The goal of jamming a communications signal is no trivial matter. In seeking to deny reliable connection between two hosts, there are significant tradeoffs made with the jamming device’s size, power, antenna, and development cost. To make matters harder, the spread spectrum techniques seek to create jam-resistant waveforms to “force a jammer to expend its resources over a wide-frequency band, for a maximum amount of time, and from a diversity of sites” (Sklar, 2001).

The most efficient means of jamming FHSS signals is with a follower jammer where only a portion of each dwell is jammed, meaning the jammer must ascertain the newly detected energy and determine if it is the correct signal to jam (Poisel, 2011). A follower jammer is best employed with a specific protocol in mind and with significant reverse engineering of the intended signal. *Protocol aware* or *smart jamming* algorithms then become the most effective way to jam a signal without deleterious effects to the surrounding environment by disrupting portions of a digitized signal based on their necessity to deny the intended communications link. This requires extensive synchronization and knowledge about the target signal to track the timing and phase of the transmitted signal. Another major limitation in protocol aware jamming is the time delay from initial signal acquisition to predicting the next frequency the signal hops to—this is done in milliseconds, and the frequency hopping pattern can be non-deterministic (Poisel, 2011).

Historically, RF jamming has been the most common C-UAS mitigation technique and is limited by terrain, weather, equipment cost, and potential disruption of friendly and civilian devices (Wang et al., 2021). Due to the clutter in the frequency bands where most UAS communicate, RF detection and mitigation becomes incredibly complicated. The LPD, LPI, and LPE characteristics of FHSS and DSSS signals enable them to hide amongst the background clutter, making it harder for attackers to identify and disrupt signals of interest. Many modern devices are hardened against rudimentary RF jamming techniques, which has led to new jamming techniques and high-power consumption that increase complexity of the C-UAS device.

It should be reiterated; regardless of which RF jamming technique is used, there is a requirement for substantial amounts of power which increases the physical parameters of a system. This has a detrimental effect on the form, fit, and function of a modular payload to interface with other systems. Additionally, RF jamming has negative effects on the other sensors integrated on a host aircraft. Because of the collateral damage and SWaP considerations, integrating RF jamming on manned and unmanned aircraft becomes a more complex problem to solve (Brown et al., 2007). As drones continue to operate in commonly utilized frequency bands and in urban environments, high power output and digital signal processing will continue to be the norm.

Profiling Current C-UAS Technology

Size, weight, power, and development cost are among the many constraints that companies developing C-UAS technology have to contend with. These companies must design systems that not only work properly—a technological feat in and of itself—but they must also contend with societal and legal limitations as well. In a 2019 survey on current drone technologies, the authors identified 537 C-UAS technologies designed to counter unmanned aircraft through kinetic or non-kinetic actions (Michel, 2019). Despite the market density, the main trend of this study showed that unmanned countermeasures are getting increasingly bulky and expensive to procure and sustain, while the targets they are supposed to thwart are only getting smaller and more expendable. The asymmetry in threat versus countermeasure is much like the asymmetry in tactics and strategy. Thus, where such asymmetry exists, reducing asymmetry can be achieved through rethinking the problem. This leads to an inflection point where the SWaP requirements of a host device and non-kinetic electronic warfare and cyber-attack techniques can be utilized to mitigate threats from small UASs.

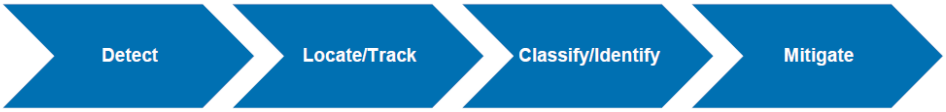

Figure 3. C-UAS Kill Chain (Figure 3-1; Patel & Rizer, 2019)

For the purposes of understanding the C-UAS kill-chain, the technology used in detecting, locating, and classifying UAS can be parsed separately from the mitigation measures. The digital signal processing required for the first three-quarters of the kill-chain are the most complex problems for C-UAS companies to tackle because of a UAS's low-energy output physical characteristics that make them appear as small birds. Companies like CACI and Anduril have created robust platforms to meet the needs of the first three-quarters of the kill-chain by building target libraries to help in building digital signal processing and computer-vision algorithms for their sensor packages.

Static, ground-based C-UAS sites are typically employed aboard military bases, secure facilities, and other strategic points of interest. Because they have access to shore power, they contain the most robust suite of countermeasures, integrating most sensor types with several mitigation methods. Additionally, these systems can have an autonomous mode that allows the platform to move through the kill-chain with a human-on-, -in-, or -out-of-the-loop. Unfortunately, these platforms require enormous amounts of shore power to operate the various sensor packages onboard (Wang et al., 2021). Additionally, because they are in static positions, they become easier targets for adversaries to attack or sabotage. Lastly, because the sensors on fixed and terrestrial sites use the high-end solutions, they are extremely expensive to acquire, maintain, and sustain throughout their product life cycle (Wang et al., 2021).

Ground-based, mobile platforms are designed to be mounted on vehicles and operated while moving. Depending on the transportation vehicle, they can be very capable in austere environments by carrying a modest amount of power and sustainment before needing to return to base for rest and refit. However, despite their mobility, these C-UAS systems like the Marine Air Defense Integrated System (MADIS), built by Sierra Nevada Corporation and Lockheed Martin, have several glaring limitations (Barrett, 2019). First off, they are human operated which requires extensive operator training on the system. Second, because they are general-purpose EW systems, the ground-based mobile systems require significant amounts of power that have a large RF signature. This power consumption means that the ground-based, mobile C-UAS cannot conduct persistent sensing without nearby resupply. Third, they are extremely expensive. The MADIS is a $150 million program of record, and as it seeks to bring in more capabilities, it will increasingly become more expensive (Missile Defense Advocacy Alliance, 2020). Finally, because the MADIS is expensive, bulky, has significant power requirements, and contains sensitive equipment, it must be carefully protected. Loss of such an aerial defense system could itself be catastrophic, such as the fate of the Russian surface-to-air missile convoy under Ukrainian Bayraktar TB-2 attack (Ukraine Armed Forces, 2022).

Handheld C-UAS systems are operated by a single individual or team of individuals. The Dedrone DroneDefender is a good example of a lightweight handheld system that resembles a small arms weapon with highly directional antennas (Dedrone, n.d.). The handheld devices are cheaper than the fixed, mobile, or UAS-based devices. Additionally, the low power and portability of these systems gives another advantage over their larger counterparts; handheld systems can jam an entire frequency band with minimal collateral damage to friendly communications farther afield because of signal attenuation over longer distances. However, there are downsides to the lower power settings. Namely, they only operate on one or two frequency bands and lack a smart library, necessitating a broadband jam of the 2.4 or 5.8GHz frequency bands. They are only effective over shorter distances to a target, and the broadband jamming can lead to the unintended disruption of friendly or civilian communications nearby. Thus, in high-density electromagnetic spectrum environments like airports and border crossings, using the DroneDefender becomes precarious. Finally, even though they are more portable than their mobile or fixed counterparts, handheld systems are still bulky and unwieldy; Dedrone's DroneDefender weighs 15.8 lb, making it a cumbersome piece of gear for operators to carry for sustained periods of time. The DroneDefender is a fine piece of equipment for the close-in fight where collateral damage does not matter, but at high altitudes, it fails to be effective against adversarial aircraft.

Table 1. Pros and Cons of Current C-UAS Technology

	Current Systems	**Current C-UAS Pros**	**Current C-UAS Cons**
Ground to Air	MADIS	Mobility	High-Power Consumption
	Compact Laser Weapon	Small Form Factor	Easily Disrupted
	DroneDefender	Handheld	BBN Jamming Only
	CACI Skytracker	Purpose-Built for COTS UAS	Fixed Position
	Anduril Sentry Tower	Exquisite AI Backbone	Expensive
	Shotguns	Close-Range	Potential Fratricide
Air to Air	Nets	Capture Target	Short-Range
	Anduril's Anvil	Kinetic Kill w/o Fratricide	Extensive Flight Path Metrics
	Explosives	Target Destruction	Damages Friendly Device

By and large, the current systems procured have met the needs of the DoD and DHS for the initial wave of UAS usage. The systems have proven records of operational success around the world and will continue to work well against singular incursions like the ones experienced over the past decade. However, as this section has noted and Table 1 summarizes, there are serious limitations associated with the current technology. Therefore, it is necessary to look to the past to the initial stages of aerial warfare and how we might introduce the same lessons learned to countering unmanned aircraft.

Cyber

Cyber mitigation measures are the ultimate complement to traditional electronic attack mitigation measures like RF jamming. Instead of putting broadband noise into the ether like broadband noise jamming, cyber-attacks offer a scalpel's edge approach to C-UAS. Because UASs operate using the same digital modulation principles as terrestrial information systems, they are also vulnerable to the same attacks conducted over the past few decades. While there are inherent technical limitations to each cyber-attack technique, this methodology typically requires less power because of the *a priori* knowledge about an information system. Second, cyber-attacks lower the risk of collateral damage to surrounding infrastructure. And finally, because there are lower SWaP requirements in comparison to RF jamming, delivering cyber-attacks against adversarial UASs from a friendly UAS becomes reality. This section will discuss cyber-attack techniques that gained prominence in the past two decades and how the attacks can be used to target UASs.

A Man-in-the-Middle (MITM) occurs when an adversary intercepts the communication between two communicating devices, allowing the attacker to alter or obtain information in the exchange (Conti et al., 2016). This attack compromises the integrity, confidentiality, and access control of a given security scheme without ever notifying the server or the client. By subverting access controls and intercepting the communications, an attacker can subsequently alter and manipulate the information transmission between devices at their discretion – including hijacking a target or spoofing Global Navigation Satellite System (GNSS) navigation (Common Attack Pattern Enumeration and Classification [CAPEC], 2021). Figure 4 represents an impersonation attack where Eve maliciously spoofs messages (i.e., sends forged messages to Bob, who believes he is speaking with Alice). Meanwhile, Alice cannot regain connection to Bob because Eve has blocked her ability to communicate.

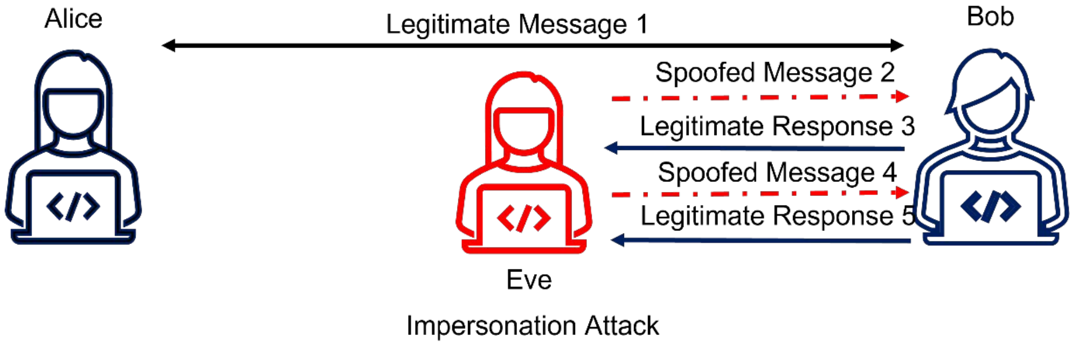

Figure 4. Impersonation Attack

According to the CAPEC, a cyber-attack community resource operated by the government-contracted MITRE Corporation, a MITM has the following prerequisites: first, two entities must be communicating with insufficient cybersecurity protections, allowing an attacker to eavesdrop on the communication exchange with or without the target's knowledge. Second, there is a lack of sufficient mutual authentication between the targets giving way to attacker interposition. From this point, an attacker can subsequently manipulate the actions of its target (CAPEC, 2021). Given that a MITM is reliant upon the exploitation of protocol or system vulnerabilities, it can be viewed as more of an end state vice an attack vector, as seen in Figure 4. In this figure, Eve is the MITM seeking to intercept the network traffic between Alice and Bob. Once Eve can establish a network connection either between her targets or spoofing one to the other, she can then conduct a variety of attacks, including the hijacking of the network traffic.

While much different from a MITM, Denial-of-Service (DoS) protocol attacks such as UDP (CERT Division, 1997) and TCP/SYN floods (CERT Division, 2000) or deauthentication (Bellardo & Savage, 2003) attacks can be an integral part of achieving that end state. Both the UDP and TCP/SYN flood are examples of DoS attacks that are more effective when multiple systems are used as sources of attack traffic (Douligeris & Mitrokotsa, 2004). This creates a Distributed-DoS (DDoS) using computers and other networked devices to create a surreptitious botnet that prevents normal communications from occurring as planned (Mirkovic & Reiher, 2004). Both flood attacks are easy to carry out using open-source tools like Low-Orbit Ion Cannon (Nagpal et al., 2015) or hping3 (Sanfilippo, 2006) to flood a target server with TCP or UDP packets to disrupt the service connection. DDoS attacks gained particular prominence in the late 2000s and early 2010s when the hacktivist group Anonymous used these vulnerabilities to shut down the service connections at Visa and Mastercard after the payments companies removed their support for the WikiLeaks website (Olson, 2012). The DDoS is particularly sinister if implemented properly, as this type of attack is unpreventable and can only be mitigated through firewall strengthening and filtering protections.

GNSS spoofing is an attack method where a spoofer generates a counterfeit signal for each authentic signal received to distort the relative true location of a target in favor of a counterfeit location that is more favorable for the spoofer (Kerns et al., 2014). For an attacker to sufficiently exert control of a target device via GNSS spoofing, the attacker must capture the GNSS signal of interest dynamically or through *a priori* knowledge. GNSS spoofing requires the insertion of a MITM but can be especially effective in negating an adversary’s use of waypoints for UAS movement and control.

The cyber-attack techniques outlined in the preceding paragraphs provide a baseline for attack vectors against adversarial UASs. To make this a fully realized effort, a library of attacks is needed specifically designed to mitigate the threats posed by commercial UASs and integrated with a menu of options on a user interface. This interface could be fully automated, giving the operator-on-the-loop a common operating picture of local threats and actions taken that the operator needs to be alerted to.

While this was only lightly touched on in the introduction, cyber-attacks notably consume less power than RF jamming. Each attack type exploits a different protocol vulnerability than the other and, while some can be patched easily, many UAS manufacturers continue to design and build UASs with known vulnerabilities. For many consumers, a fully optimized product at a low price point is more important than data privacy and security. The cyber-attack techniques discussed in this section are not meant to be a one-size-fits-all approach like RF jamming, but instead they are meant to give a variety of attack solutions for escalation of force procedures in countering unmanned systems.

Progression of Counter-Aerial System Development

In aerial defense for standard enemy aircraft, there has been a historic progression where ground-based anti-aircraft artillery was avoidable by aircraft use of the wider airspace (obstacles or altitude) until aerial interdiction patrols were introduced to either intercept the enemy or force them into lower altitudes and the kill-zone. The flexibility afforded by aircraft designed for air-combat extended the effectiveness of a defense.

Thus, it is easy to extend this same natural progression to aerial combat with unmanned systems. Whereas we currently use centralized, ground-based systems, the right type of friendly UASs using low-SWaP payloads could make aerial interdiction patrol and improved airspace control a reality. Instead of designing only general-purpose EW platforms like the MADIS, Sentry Tower, and Skytracker, the DoD and DHS can develop a suite of aerial interdiction platforms designed for purpose-built EW and cyber-attacks. Just as aircraft have specific mission sets, the same should be said for C-UAS. There is a reason the A-10 does not do the job of the F-22 or vice versa. While the A-10 can fight against an aerial threat, it does not have the speed, maneuverability, or weaponry like the F-22 to fight effectively. Similarly, the F-22 is not designed for the close-air support afforded by the A-10's 30mm Gatlin gun (Air Combat Command, Public Affairs Office, 2020).

The maneuverability afforded by decentralization of technology is essential to counteract the current centralized methods. Instead of static towers with limited or no mobility, networking a family of mobile devices designed to tackle each subset of the C-UAS problem leads to maneuverability. For example, an airborne C-UAS device designed to fit in the payload bay of a fixed-wing Group 2 UAS can effectively mitigate enemy UASs for over 24 hours by overcoming the signal attenuation that occurs in ground-to-air systems like the Sentry Tower, MADIS, and DroneDefender.

Case Study – Defending a Hydro-Electric Power Facility

Example Scenario

Consider the following case study of defense of a hydro-electric power facility on the Pacific west coast as the target.

Begin Scenario

At the hydro-electric facility, the guard on watch receives notification from the northeast tower's radar sensor that there is a 95% chance of the presence of multiple UASs moving at 20 miles per hour towards the tower. A few seconds later, the guard receives another notification, this time of 10 UASs flying at 25 miles per hour[1] directly at the southwest tower located on the dam's primary entryway. The guard has a system of typical and current mitigation measures available at his disposal via a display. The display shows a heterogeneous swarm operating on the 2.4 GHz band. Due to the swarms' rapid speed and multi-directional attack, the guard chooses to jam the entire 2.4 GHz band using the northeast and south tower's omnidirectional antenna suites.

The jamming effect causes the UAS devices to act as if they have hit an invisible wall – a few collide and drop out of the sky, and the swarm stops in place and continues to hover. At this point, several more UASs self-land. Meanwhile, back at the command center, the guard receives an updated situation report from his heads-up display, showing the targeted UASs returning to their point of origin, causing the guard to assume that the system is working. As the jamming system resets and the guard is about to send in a report on the attack, the tracking system identifies another UAS swarm approaching the southwest tower, this time operating on the 5GHz band. Since the system is resetting, the guard is unable to re-start the broadband jam, and the UAS deliver shape charge after shape charge to the walls of the dam, causing explosions along the dam's center. As the guard contacts local authorities to inform the need for evacuation, the dam bursts, and tens of thousands of tons of water pour out.

The dam finally disintegrates, and power immediately goes out in the nearby metropolitan city as well as significant parts of the surrounding region because of their reliance on the power generated by the dam. Airplanes trying to land in the city airport lose connection with the air traffic control station, and while the ground crews work to get the backup generators operational, many flights are diverted. The larger aircraft can make it to other airports, but smaller planes with dwindling fuel supplies are forced to find open clearings for emergency landings in the heavily wooded Pacific Northwest.

[1] Data-sheet for Intel Drone Light Shows states current max speed up to 17 m/s (38 mph; Intel, 2021)

After the UAS attack, large-scale physical infrastructure damage is identified, including roads, power grids, buildings, and the dam itself. Power loss disrupted businesses, transport, and security systems. Moreover, back-up generator functionality does not cover the months needed to restabilize power, leading to power grid blackouts and interruptions in normal operations. In comparison, the entire attack was executed by low-cost commercial devices.

Example Scenario (New Version)

In the ensuing scenario, we will revisit the same attack, but the C-UAS protections are enhanced with a security patrol of UASs armed with drone hijacker devices.

Begin Scenario

At the hydro-electric facility, each tower was augmented with a new type of UAS security patrols: drone hijackers ("Alphas"). This was a significant upgrade in the defense as the Alphas are deployed forward of the sentry towers on a patrol schedule and can receive mid-flight updates from the towers to guide their attack methods. Additionally, given their small form-factor and low power consumption, the Alphas can patrol for an hour apiece, giving the watch officers a persistent presence to augment the sentry towers.

The guard on watch receives notification from the northeast tower's radar sensor that there is a 95% chance of the presence of multiple UAS moving at 20 miles per hour towards the tower. A few seconds later, the guard receives another notification, this time of 10 UASs flying at 25 miles per hour directly at the southwest tower located on the dam's primary entryway. The guard's display shows a heterogeneous swarm operating on the 2.4 GHz band. Due to the swarms' rapid speed and multi-directional attack, the guard chooses to deploy the Alphas against the approaching swarm for mid-air interdiction. The guard reserves the capability to jam the entire 2.4 GHz band using the northeast and south tower's omnidirectional antenna suites as a back-up.

The Alphas begin to issue a flood of UDP packets and deauthentication frames. As with the centralized system, the two swarms function as if they have hit an invisible wall and a few drop out of the sky, and the swarm stops in place and continues to hover. Several more UASs begin to-self land.

Meanwhile, back at the command center, the guard receives situation updates from his heads-up display showing several UASs dropping out, and the guard assumes the system is working. As the guard is about to send in a report on the attack, the tracking system identifies another UAS swarm approaching the southwest tower. The guard sends an updated instruction set to the Alphas before activating the jamming system, sending RF noise out of the tower's omnidirectional antennas to broadband jam the entire 5 GHz band. The new UAS swarm stops, and the Alphas take a forward position for preemptively mitigating any new incoming threats. In the ensuing 10 minutes, a ground team is dispatched and captures five suspects on all-terrain vehicles carrying several large briefcases filled with small UASs and explosives.

Framework Comparison and Conclusion

In summary, the current framework, while sufficient for the C-UAS fight in the late-2010s and early 2020s, will likely be outpaced by emerging drone technologies in the coming decades. More specifically, when drone swarms become more readily available, they will increasingly be a threat to critical infrastructure and military installations. The proposed ground-to-air C-UAS systems under development by Northrup Grumman (2020) and other defense industrial base companies may be necessary additions for the high-end C-UAS fight. However, there are inherent technical limitations to overcome using terrestrial systems, creating an opportunity to use UASs as aerial interdiction platforms. Designers of aerial C-UAS systems should focus on the technological advancements of the past three decades and develop low-size, weight, and power (SWaP) EW and cyber-attack techniques for UAS mitigation. While we recognize (and Table 2 represents) the limitations with UASs as stand-in EW and cyber-attack platforms, these aerial systems offer flexibility and maneuverability on the battlefield with a targeted interdiction to overcome the limitations of ground-based technologies. Finally, the lack of interference from telephone poles, trees, and buildings affords aerial systems the ability to extend the operational range of non-kinetic countermeasures. With an aerial variant, this operational range is only limited by the output power of the transmitting C-UAS device, which can be varied by using host power or its own power source.

Table 2. Pros and Cons of Future C-UAS Technology

	Future Systems	Future C-UAS Pros	Future C-UAS Cons
Ground to Air	AFRL NINJA	Reliability, Fully Funded	Bulky
	MADIS/FWS	Mobility	High-Power Consumption
	Inter-Networked Systems	Small Form Factor	Easily Disrupted
	mmWave Directed Energy	Handheld	BBN Jamming Only
Air to Air	Autonomous Stand-in Hijackers	Usurp Control of Target	Requires Target RE
	Cryptographic Protocol Attacks	Precision	Requires Target Profile
	DDoS Attacks	Effective against Swarms	Spreading Complexity
	Stand-in GNSS Jammers	Easier to Implement	Attack Profile Modification
	Stand-in RF Jammers	Close Proximity to Target	Potential Communication Fratricide

Current systems and methods for countering UAS have found many successes in the past decade. However, because the Sentry Tower, Skytracker, and MADIS are terrestrial systems, they only provide limited robustness and depth as a solution set. Additionally, the research and development of C-UAS emerging technologies fails to address the asymmetry posed by UAS threats. Instead of getting smaller and cheaper, tomorrow's directed energy weapons and lasers are increasingly expensive to build, manufacture, and sustain over the product life cycle.

Thus, reconsideration of C-UAS methods and how such systems are procured and integrated within the DoD and DHS is advised. By developing a family of networked systems that focuses on cyber-attack methodologies, the current systems on hand will be able to withstand a multi-wave and multi-frequency attack. The use of UASs during the ISIS insurgency, in the Nagorno-Karabakh war, and in the Ukrainian conflict prove that any state, or non-state, actor with modest funding can build an air force to cripple their adversary. The framework proposed herein seeks to address and mitigate that asymmetry by leveraging the technological expertise and intelligence of the defense industrial base.

References

Air Land Sea Application Center. (2019). *Multi-service tactics, techniques, and procedures for air and missile defense*. https://armypubs.army.mil/epubs/DR_pubs/DR_d/ARN15491-ATP_3-01.15-000-WEB-1.pdf

Air Combat Command, Public Affairs Office. (2020, December). *A-10C Thunderbolt II*. Air Force. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104490/a-10c-thunderbolt-ii/

Almohammad, A., & Speckhard, A. (2017). *ISIS drones: Evolution, leadership, bases, operations and logistics* (ICSVE Research Reports). International Center for the Study of Violent Extremism. https://www.icsve.org/isis-drones-evolution-leadership-bases-operations-and-logistics/

Anduril. (2021). *Anduril—sentry tower* [Defense technology]. https://www.anduril.com/hardware/sentry/

Arreguin-Toft, I. (2005). *How the weak win wars: A theory of asymmetric conflict*. Cambridge University Press.

Barrett, B. (2019, July 22). The Marines' new drone-killer aces its first test. *Wired*. https://www.wired.com/story/iran-drone-marines-energy-weapon-lmadis/

Bellardo, J., & Savage, S. (2003, May 16). *802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions*. 12th USENIX Security Symposium, USENIX Security 2003, Washington, D.C. https://www.usenix.org/legacy/events/sec03/tech/full_papers/bellardo/bellardo_html/

Brown, K., Drake, S., Mason, K., Piotrowski, A., & Swierkowski, L. (2007). A distributed stand-in EW hunter-killer system. *2007 10th ^{In}ternational Conference on Information Fusion*, 1–8. https://doi.org/10.1109/ICIF.2007.4407985

CERT Division. (1997). *CA-1996-01: UDP port denial-of-service attack* (CERT Advisory REV-03.18.2016.0; 1996 CERT Advisories). Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf#page=123

CERT Division. (2000). *CA-1996-21: TCP SYN flooding and IP spoofing attacks* (CERT Advisory REV-03.18.2016.0; 1996 CERT Advisories). Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf#page=123

Common Attack Pattern Enumeration and Classification (CAPEC). (2021). *CAPEC-628: Carry-off GPS attack* (CAPEC Report CAPEC-628). The MITRE Corporation. https://capec.mitre.org/data/definitions/628.html

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in ththeiddle attacks. *IEEE Communications Surveys Tutorials*, *18*(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Dedrone. (n.d.). *Data sheet—DroneDefender counter-UAS device*. Retrieved January 3, 2022, from https://gdmissionsystems.com/-/media/General-Dynamics/Ground-Systems/PDF/Counter-UAS---Dedrone/DroneDefender-DataSheet.ashx?la=en&hash=516300C425D3CDA5C69CBAD29C1886EEFD9EA54A

Douligeris, C., & Mitrokotsa, A. (2004). DdoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. https://doi.org/10.1016/j.comnet.2003.10.003

Intel. (2021). *Intel drone light show premium fact sheet*. https://inteldronelightshows.com/wp-content/uploads/sites/3/2021/01/Intel-Drone-Light-Show-Premium-Fact-Sheet-23112020.pdf

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617–636. https://doi.org/10.1002/rob.21513

Lichtman, M., Jover, R. P., Labib, M., Rao, R., Marojevic, V., & Reed, J. H. (2016). LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation. *IEEE Communications Magazine*, *54*(4), 54–61. https://doi.org/10.1109/MCOM.2016.7452266

Michel, A. H. (2019). *Counter-drone systems* (2nd ed.). Center for the Study of the Drone, Bard College. https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DdoS attack and DdoS defense mechanisms. *Association of Computing Machinery*, *34*(2). https://doi.org/10.1145/997150.997156

Missile Defense Advocacy Alliance. (2020, July 8). *Marine air defense integrated system (MADIS) – Missile Defense Advocacy Alliance*. Missile Defense Advocacy Alliance: U.S. – Air Defense, Intercept. https://missiledefenseadvocacy.org/defense-systems/marine-air-defense-integrated-system-madis/

Nagpal, B., Sharma, P., Chauhan, N., & Panesar, A. (2015). DDoS tools: Classification, analysis and comparison. *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 342–346.

Northrup Grumman. (2020, July 8). Defining possible against unmanned aerial systems [Defense contractor]. *Counter Unmanned Aerial Systems (C-UAS)*. https://www.northropgrumman.com/what-we-do/land/counter-unmanned-aerial-systems-c-uas

Olson, P. (2012). *We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. Little, Brown. https://books.google.com/books?id=ncGVPtoZPHcC

Parlin, K., Mahtab Alam, M., & Le Moullec, Y. (2018). Jamming of UAV remote control systems using software defined radio. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 1–6.

Perrigo, B. (2022, March 1). Ukraine's secret weapon against Russia: Turkish drones. *Time*. https://time.com/6153197/ukraine-russia-turkish-drones-bayraktar/

Pitsky, P. (2021). *SkyTracker® technology suite* [Defense contractor]. CACI. https://www.caci.com/sites/default/files/2021-06/F424_2106_Corian%20Flyer.pdf

Poisel, R. (2008). *Introduction to communication electronic warfare systems* (2nd ed.). Artech House, Inc. http://pws.npru.ac.th/sartthong/data/files/Introduction%20to%20Communication%20Electronic%20Warfare%20Systems.pdf

Poisel, R. (2011). *Modern communication jamming principles and techniques* (2nd ed.). Artech House, Inc.

Sanfilippo, S. (2006). *Hping*. Hping. http://www.hping.org/documentation.php

Sklar, B. (2001). *Digital communications: Fundamentals and applications* (2nd ed.). Prentice Hall Professional Technical Reference.

Stutzman, W. L., & Thiele, G. A. (2013). *Antenna theory and design* (3rd ed.). John Wiley & Sons, Inc.

Sukhankin, S. (2021a). The Second Karabakh War: Lessons and implications for Russia (Part one). *Eurasia Daily Monitor*, *18*(2). https://jamestown.org/program/the-second-karabakh-war-lessons-and-implications-for-russia-part-one/

Sukhankin, S. (2021b). The Second Karabakh War: Lessons and implications for Russia (Part two). *Eurasia Daily Monitor*, *18*(7). https://jamestown.org/program/the-second-karabakh-war-lessons-and-implications-for-russia-part-two/

Ukraine Armed Forces. (2022, February 27). Байрактари в роботі. Наші оператори ювелірно криють колони ворожих військ. Знищено російський БУК в районі Малина Житомирської області. Бийтеся, вороги! Не буде вам спокою на нашій землі! Https://facebook.com/100068564836091/posts/257372956558197/ https://t.co/dH2UEUbKST [Twitter]. *@ArmedForcesUkr*. https://twitter.com/ArmedForcesUkr/status/1497997019515961347

U.S. Marine Corps. (2000). *Marine Corps warfighting publication 3-11.3: Scouting and patrolling*. Headquarters Marine Corps.

U.S. Marine Corps. (2002). *Marine Corps warfighting publication 3-1: Ground combat operations*. Headquarters Marine Corps.

U.S. Marine Corps. (2017). *Rifle platoon in the defense B3J0435XQ student handout*. The Basic Officers Course, Marine Corps Training Command.

U.S. Marine Corps. (2019). *Marine Corps warfighting publication 3-01: Offensive and defensive tactics*. Headquarters Marine Corps.

Wang, J., Liu, Y., & Song, H. (2021). Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), 4–29. https://doi.org/10.1109/MAES.2020.3015537

Warrick, J. (2017, February 21). Use of weaponized drones by ISIS spurs terrorism fears. *The Washington Post*. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net