No. 26
June 2019

The Mitchell Forum

Systems of Systems:
What, Exactly, is an Integrated Air Defense System?

By Maj Peter W. Mattes, USAF

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates.

Abstract

When discussing the strategic challenges posed by great power adversaries such as Russia and China the term "integrated air defense system"—otherwise known as an IADS—is often invoked, but done so incorrectly or out of context. It is critical that both U.S. military mission planners and intelligence support personnel have a common and correct understanding of what constitutes an IADS in the modern context to be operationally relevant for any air campaign, much less campaigns against highly capable militaries. This understanding includes the recognition that a linear, simplistic approach to defeating a complex IADS is insufficient, and instead requires truly integrated multi-domain military operations. The purpose of this paper is to clarify the understanding of an IADS and highlight some operational deficiencies that exist due to dated knowledge and understanding of the technological evolution of modern IADS. It is the intent that the reader will understand the key terms and concepts associated with IADS, as well as why tactics such as "IADS rollback," without multi-domain and multi-effect approaches, are archaic and ineffective against modern systems. Analysts and planners alike must understand that true destruction or denial of singular IADS nodes or mediums of communication may not occur in modern air campaigns. Rather, more realistic effects that seek to disrupt, degrade, or delay the utility of IADS that are simultaneously applied may aggregate together, and give space to allow for the targeting and successful destruction of "centers of gravity" in any future air campaign.

Introduction: The IADS in Modern Warfare

"By 2030, the threats facing the United States around the world will be formidable. They will have twice, if not three times, the lethality and range of today's threats. Imagine a nation roughly 300 nautical miles (nmi) by 300 nmi in size, with a coastline bristling with anti-access/area- denial (A2/AD) weaponry. Such capabilities could include modern weapons such as hypersonic cruise missiles, fifth generation fighters, air-to-air missiles with 150 nmi ranges, digital adaptive electronic warfare waveforms, and perhaps long-range (300 nmi plus) and ultra-long-range (500 nmi) surface-to-air missiles (SAMs). Potential adversaries could enhance traditional ground-based-radar detection methods with advanced passive detection systems and possibly further augment them by acoustic detection means and advanced cyber abilities. These advances would contribute to an adversary's primary goal of attacking and disabling our capabilities before we employ them."

– Then-Maj Gen VeraLinn "Dash" Jamieson,
Air Combat Command director of intelligence,
October 2015[1]

America's adversaries are rapidly advancing their military technologies to dull the combat edge the U.S. Air Force could once virtually guarantee in any conflict. Noted airpower theorist and strategist Air Force Col John Warden observed that "since the German attack on Poland in 1939, no country has won a war in the face of enemy air superiority, no major offensive has succeeded against an opponent who controlled the air, and no defense has sustained itself against an enemy who had air superiority," and that the attainment of air superiority "consistently has been a prelude to military victory."[2] America's potential adversaries know this, especially after observing the success of Operation Desert Storm, and are not simply focused on increasing the accessibility and range of their weapons. Rather, they are developing holistic capabilities that operate in a variety of domains—including traditional domains such as land, sea, and air, as well as in space, cyberspace, and across the electromagnetic spectrum. These capabilities are not just offensive in nature. America's would-be adversaries are also developing defensive capabilities to thwart the U.S. Air Force's ability to seize the initiative and establish air supremacy in any future conflict. These defensive capabilities are purposely organized into what is termed an "integrated air defense system"—or an IADS.

The purpose of this paper is to clarify the understanding of an IADS and highlight operational deficiencies that stem from a lack of knowledge of these systems, and appreciate of the technological advancements seen in modern IADS in recent years. It is the goal of this discussion for the reader to better understand the key terms and concepts associated with modern IADS, and comprehend why certain operational philosophies (such as "IADS rollback") require substantial adaptation in planning and execution in order to be effective in modern air campaigns.

Finally, it is the goal of this paper to make clear that a modern IADS is far more complex than a singular surface-to-air missile (SAM) or its associated battalion command vehicle (BCV). Analysts and operational planners should have a common language when discussing IADS, and should incorporate this knowledge in order to effectively plan against these complex systems as the mission dictates. To accomplish this, this paper will define what an IADS actually is by breaking down its key component terms: "air defense," "systems," and "integrated." This paper will then provide several key conclusions and recommendations.

What is an IADS?

It is critical that both military mission planners and requisite intelligence support personnel have a common and correct understanding of what constitutes an IADS in order to be operationally relevant to any air campaign—particularly in the context of planning against the modern peer militaries fielded by nations such as Russia and China. This understanding includes the recognition that a linear, simplistic approach to defeating modern, complex IADS is insufficient and instead requires truly integrated multi-domain operations.

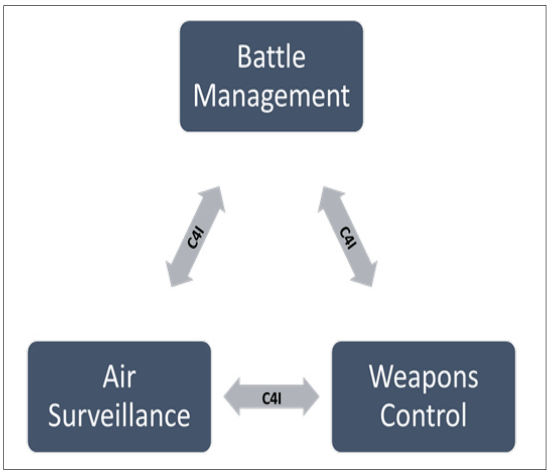

Figure 1: Three functions of an IADS enabled by command, control, communications, computers, and intelligence (C4I).

An integrated air defense system, according to one expert, "is the structure, equipment, personnel, procedures, and weapons used to counter the enemy's airborne penetration of one's own claimed territory."[3] Fundamentally an IADS is more than one element, weapon, or person. It is an amalgamation of all the above elements, organized to minimize the effects of the air domain. As shown in Figure 1, an IADS performs three functions:

- Air surveillance
- Battle management
- Weapons control

Of these three functions, air surveillance alone includes five specific functions that produce air domain awareness for commanders:

- Detect
- Initiate
- Identify
- Correlate
- Maintain

Air surveillance is often described as the "eyes" of a system, and represents the introduction of threats or potential targets to an IADS. A radar performing its inherent function will "detect" an ingressing aircraft into an IADS operating area. These initial detections are unknown entities that could be "clutter" from the environment. The "initiate" function of the IADS will then transform these radar returns into "tracks." These airborne tracks will remain anonymous to the system until the "identify" function occurs, at which point the track is categorized as being a friend, a foe, or an unknown aircraft.

These three phases are all occurring relatively independently (in older systems especially) which necessitates a "correlate" function. As a hypothetical, if a system has three tracks that are in close proximity to each other, a sensor operator has the option to consider the tracks a single entity or three different aircraft. Correlation is a critical function in this context, as it can have a significant impact on weapon resourcing and assignment. Lastly, the "maintain" function allows for specific tracks to be continuously monitored. The modern evolution of air defense technology has allowed for automation of much of this data, though. A form of data fusion occurs from this seamless transfer of data, resulting in less "man in the loop" processing and more "man on the loop" paradigms in contemporary IADS. This means there is a reduction in the ability to defeat the human factor involved in these systems, and there is now increased importance for multiple effects to be brought to bear against air surveillance nodes in order to degrade the awareness of an IADS.

After surveillance, the battle management aspect of an IADS includes four functions:

- Threat evaluation
- Engagement decision
- Weapon type selection
- Engagement authority

Battle management represents a key transition from identifying a threat to committing against that threat through command decisions. Air surveillance provides the potential threat or target; this decision is effectively finalized through threat evaluation and the move to engage. Battle management makes the determination that a given radar track is in fact a threat to the entity being protected by an IADS. Once a given track is a determined to be a threat the decision to engage occurs. This engagement determination involves the selection of a weapon to engage the threat. The role and responsibility of a weapon system informs a decision maker's selection to ensure a relatively efficient engagement balanced against the variety of threats that may exist at the same time or in a similar geographic region (such as an IADS' area of responsibility). The engagement authority is the final step in battle management that confirms the threat, engagement, and weapon selection decisions.

Battle management makes the determination that a given radar track is in fact a threat to the entity being protected by an IADS. Once a given track is a determined to be a threat the decision to engage occurs.

Battle management represents a key transition from identifying a threat to committing against a threat through command decisions. These decisions transition into weapons control where a particular weapon system performs the weapons pairing, acquiring, tracking, guiding, killing, and assessing functions. Within weapons control, more refined levels of air surveillance and battle management tasks are occurring. The difference is these decisions are strictly related to the specific weapon system that is authorized to engage a specific threat.

The complexity of modern command, control, communications, computers, and intelligence (C4I) systems and processes used by IADS are often underestimated and not appropriately analyzed. For example, it is important to note that it would be highly unusual to observe an individual weapon system component of an IADS, such as a fire control radar, providing air surveillance within an IADS. However, because these weapon systems share similarities with air surveillance or battle management tools, they appear as though they can do just that, and are often mistakenly thought to perform the same battle management function.

The similarities that certain weapon system components have with IADS battle management functions and air surveillance tools leads to control functions and guidance aspects of air defense systems being analyzed more than other elements of an IADS' kill chain. This is because capabilities such as fire control radars and firing batteries that make decisions and have radars themselves are perceived as performing their function across the entire system, irrespective of a weapon's role or responsibility in the larger IADS.

This complexity also makes the task of defeating IADS more difficult, especially modern systems. The sheer variety of methods and tools that analyze and exploit different sections of the electromagnetic spectrum allow for adversary communication methods, in effect, to harden against a variety of lethal and non-lethal effects that could be used in suppression of air defense activities. No longer can an operation against a modern, complex IADS plan to achieve a singular effect against a singular node or IADS communication medium. These communication mediums include but are not limited to: traditional landlines, fiber-optic cable networks, and myriad options for communicating within the radio frequency and electromagnetic spectrums.

Air Defense and IADS

The phrase "air defense" is the metaphorical heart of the IADS acronym, and for good reason. Air defense, as its name implies, is the act of safeguarding some protected asset or assets. Specifically, it is the inherent protection against threats in the air domain. But not all militaries approach air defense in with a similar mindset. The Russian approach to air defense, for example, stipulates that air defense units are to "protect troops and facilities from a different means of air attack (strike aviation, cruise missiles, UAVs) in a combined arms combat environment and on the march."[4] In support of this responsibility, Russian air defense units perform the following tasks: air defense combat, detection of enemy aircraft and providing warning for the protected units, destruction of the means of an enemy air attack, and theater missile defense support.[5]

Air defense, as its name implies, is the act of safeguarding some protected asset or assets. Specifically, it is the inherent protection against threats in the air domain.

In contrast to the Russian approach, the U.S. Air Force has historically mischaracterized air defense weapons systems based on their range and altitude. A tactical SAM (TACSAM), for example, has been traditionally considered a short-range mobile system, while a strategic SAM (STRATSAM) is viewed as a longer-range system. The assigned mission and defended asset though should be the key consideration when trying to understand the role of an air defense weapon or IADS. As such, the tactical or strategic nomenclature of a specific air defense system should not be tied to the range of the system (or the maximum recommend intercept range—MRIR) though a positive correlation does exist. The implication for an air campaign is that this view of air defense could result in an analytical misunderstanding as to the impact an air defense weapon could have in a region or around a defended asset. It could also mean the misprioritization of effects against a particular system, which could result in the destruction of a component that is of little consequence to the operation at hand where disruption or denial effects would suffice.

Russian SAMs have been acquired by each of its military service components to provide specific capabilities for specific missions. What makes a given system tactical or strategic in defensive nature is tied more towards the "center of gravity" (to borrow Warden's terminology) that a SAM has been tasked to defend. These centers could include leadership, key infrastructure, forward echelons of fielded forces, or ballistic missile systems, among others. These centers of gravity are defined by their apportionment to a specific command and control (C2) structure and assigned mission. This is an important distinction as the S-300, 400, and 500 SAM systems (also known as the SA-10, SA-20, and SA-21) have tremendous advertised ranges, some reaching out to 500 miles. But, a vast majority of Russian air defense assets are of the short and medium-range variety, according to recent analyses.[6] A range, in distance, is more closely aligned to the primacy a given system has within an IADS. An S-500 (with a reported 500 nautical mile reach) would probably be the first line of defense for a given IADS over the expected combat radius of a Su-35 Flanker or a Pantsir-S1 (SA-22) missile system.

The term "air defense" provides the functional characteristic of an IADS from a target development perspective. It aids in understanding what a specific system does, how it functions within a greater target system, and its significance.[7] It is obvious that systems like the S-400 (SA-21) or the SA-11/17/27 Buk series, or Pantsir (SA-22) are designed to provide air defense. However, other systems like Sukhoi's Su-35 Flanker or Mikoyan's MiG-35 Fulcrum may also provide air defense, much like the defensive counter air (DCA) role of a U.S. Air Force F-15C Eagle. The same is true for electronic warfare equipment, as air defense is not resigned to a single domain. Other domains and defense capabilities can indirectly or directly affect air operations, and positively support air defense.

...other systems like Sukhoi's Su-35 Flanker or Mikoyan's MiG-35 Fulcrum may also provide air defense, much like the defensive counter air (DCA) role of a U.S. Air Force F-15C Eagle. The same is true for electronic warfare equipment, as air defense is not resigned to a single domain.

A System of Systems

Across the USAF, it is common that a SAM is often simplified into a singular key component, such as a missile or a radar, for targeting purposes, or that a singular SAM system (a missile and its radar) is represented as an IADS. This unintentionally de-emphasizes the other components of the SAM system or the greater IADS. So the question is—what is a system, in the context of the IADS discussion?

Merriam-Webster defines a system as "a regularly interacting or interdependent group of items forming a unified whole."[8] It is well understood that aircraft, like a multi-role Su-35 fighter, consist of an engine, a fuselage, wings, avionics (such as a radar), landing gear, an infrared search and track sensor, electronic countermeasures, and armaments appropriate to its mission. A system like the S-400 SAM should not be analyzed simply as a transporter-erector-launcher (TEL) or as a singular radar. In fact, Russian defense firm Rosoboronexport (the S-400's manufacturer) describes its system in much richer terms:

> *"The Triumph [air defense missile system] consists of the 30K6E battle management system, six 98ZH6E SAM systems, ammunition load comprising the 48N6E3 and [or] 48N6E2 surface-to-air missiles (SAMs) and 30Ts6E maintenance facilities."*[9]

Using just the Russian firm's own description, at least seven different vehicles are required for the S-400 system to carry out its mission. This also overlooks other indirectly required components, which could include command and control vehicles, generators, fuel and oil, engineering equipment, transportation and resupply vehicles, support personnel, and the defended asset itself—whether a military unit or physical infrastructure.

However, this description is just one part of a grander IADS. The reality of an S-400 working in an IADS is that it is just one component in a series of systems that comprise an IADS. There could be one S-400 or multiple S-400s in an IADS, depending on the mission at hand or area to be defended. These weapons could be tied together with dissimilar capabilities as well. For example, an S-400 could be deployed in a system with a Pantsir-S1. Analyzed literally, one may draw a false conclusion that this is just a single example of these two systems working in close proximity. The reality is that these systems often work together as a result of their roles and responsibilities. Rosoboronexport describes the role of the Pantsir-S1 as a road-mobile capability that is able to reinforce air defense groupings "when repelling massive air attacks."[10] It is also important to note this is just one example of only two systems working in close geographic proximity. The comparison highlighted here has direct parallels to aircraft and electronic warfare capabilities as well. Ultimately, all these systems are interconnected in order to provide a seamless, integrated defense from air attack.

Integration and Air Defense Systems

Integration, the first term invoked in the IADS descriptor, is what brings together several disparate systems to form a comprehensive air defense. The intent behind integration is "to form, coordinate, or blend into a functioning or unified whole."[11] Integration marries a variety of systems into an efficient defensive enterprise. This integration allows for the three functions of an IADS to simultaneously and repeatedly occur. In effect, it takes the linear IADS kill chain (as depicted in Figure 2) and allows several parallel kill chains to happen at the same time. Mischaracterization of how IADS work comes from an underappreciation of how various systems and their components function within the larger IADS enterprise. Outdated approaches and plans to defeat an IADS are reminiscent of the childhood "telephone game" idea: if one breaks a link in the chain, the whole system will fall. Modern IADS, though, are more like social media platforms such as Facebook. Removing one user doesn't stop a comment thread on a post, to use one analogy. Thus, the use of multiple attacks to deny, delay, and degrade the message must happen because it is improbable that any one attack can permanently break a critical link.

At the component level, some systems have the capability to run a highly localized version of an IADS. For example, an S-400 has its own organic air surveillance capability (ASV), battle management, and engagement functions. However, it is untrue to think that a singular S-400 operates independently or singularly in providing air defense. In this case, an S-400 would (at a minimum) work in close proximity (both temporally and spatially) with a Pantsir-S1 to provide comprehensive air defenses maximizing the strengths of one system while mitigating weaknesses or vulnerabilities of another system. Integration allows for the efficient conduct of air defense. Said another way, it prevents an Su-35, S-400, or Pantsir-S1 from engaging a single evaluated threat at the same time, but allows for each system to engage multiple threats seamlessly.

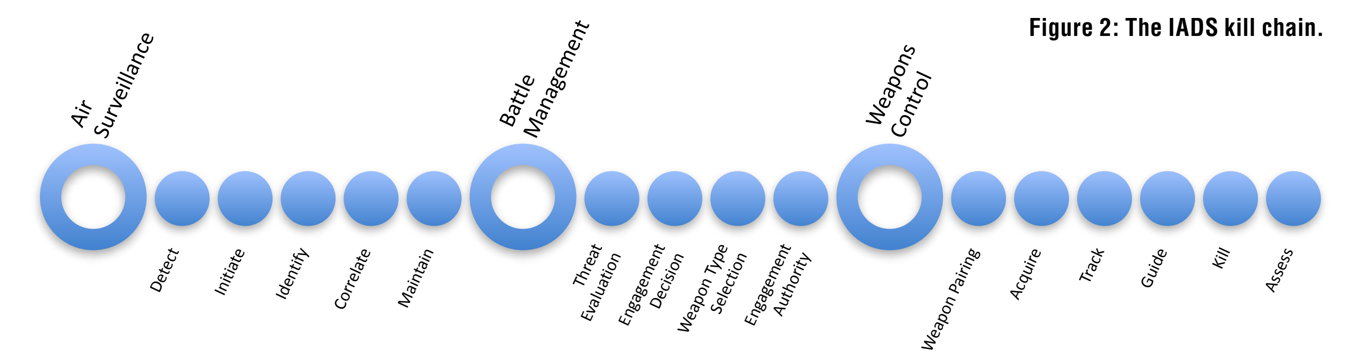

Figure 2: The IADS kill chain.

These weapon systems accomplish this integration via redundant communication mediums. While common in modern systems, it is important to note this is not a requirement within an IADS. In a classical sense, hand-held radios have accomplished this function in a concept that parallels how air traffic control manages assigned airspace. The information age has brought about an evolution to this concept by significantly increasing the options adversary air defenders can use to communicate. These newer mediums include satellite communications, 4G cellular networks, public switch telephone networks (PSTNs), data links, cloud computing systems, Wi-Fi networks, and others. Not only does the modern range of communication mediums and networks allow for de facto redundancy, but it also allows for the seamless passage of data that is irrespective of a unit's echelon or span of control. As a result, the hierarchical or linear understanding of an IADS is not a correct representation of the interoperability of tactical units to higher headquarter units.

Not only does the modern range of communication mediums and networks allow for de facto redundancy, but it also allows for the seamless passage of data that is irrespective of a unit's echelon or span of control.

Modern IADS integration and communication mediums further allow or enable the concept of "skip echelon" to occur with regularity—where communications skip an intermediate step of an organization. As an example, a mid-level battle management node has been destroyed or isolated from the rest of the IADS in a combat action. In response, an individual air defense unit reaches out directly to a division or leadership headquarters. This is a significant change from the Iraqi IADS of Operation Desert Storm, the Serbian IADS of Operation Allied Force, or Libyan IADS of Operation Odyssey Dawn that strategists faced as adversaries in past conflicts. These IADS embodied 1980s era technology at best (with some of these systems dating back to the 1970s), featuring limited communication means and static assignment of air defense roles or responsibilities. The increased potential for integration and modern communication tools available to contemporary IADS allow for the seamless sharing of data that is only limited by an adversary's decision to delegate responsibilities or decision making.

It is important to note that "older" IADS had the capability to skip echelon but were organized in what could be regarded as complicated or more established hierarchical organizations. Modern IADS feature more complex communication mediums and integration options, and connectivity is far more malleable. As such, the paradigm of the IADS rollback in an air campaign is at risk or outdated if not adapted with a multi-domain, multi-effect approach—since modern, complex IADS can mitigate the destruction or isolation of singular nodes potentially faster than the complex problem-solving approach to current rollback strategies.[12]

Conclusion and Recommendations

The *2018 National Defense Strategy* identifies Russia and China as "revisionist powers" that are significantly challenging US military advantage in every domain: air, land, sea, space, and cyberspace.[13] A modern, complex IADS greatly enables these nations to challenge the United States military, and enable an environment where they can potentially project their own forces to degrade or eliminate any American advantage. As a result, it is imperative that intelligence analysts and operational planners understand and adopt a correct understanding of a modern, complex IADS in order to properly communicate the threat to decision makers at the tactical, operational or strategic level in support of campaign goals. A common understanding must be communicated at all echelons of command and laterally across those echelons to create a shared mental model and enable a culture of critical thinking that will be crucial to defeating modern, complex IADS.

The reliance on traditional IADS "rollback strategy" in modern joint combat operations should be phased out. Instead, leaders and planners need to encourage true interoperability by harnessing both lethal and non-lethal effects across domains to defeat modern air defenses.

The reliance on traditional IADS "rollback strategy" in modern joint combat operations should be phased out. Instead, leaders and planners need to encourage true interoperability by harnessing both lethal and non-lethal effects across domains to defeat modern air defenses. Analysts and planners alike must understand that true destruction or denial of singular nodes or mediums of communication may never occur in a given operation. More realistic effects that seek to disrupt, degrade, or delay, and that are simultaneously applied may aggregate to allow for the destruction of enemy centers of gravity—to include IADS.

Ultimately, military analysts and campaign planners should not walk away from this problem set thinking modern, complex IADS are akin to the *Kobayashi Maru* training scenario from the *Star Trek* film and television franchise—where trainees are thrown into a "no-win" combat scenario. Realistically, analysts and planners should know and understand the lessons from Operations Desert Storm, Allied Force, and Odyssey Dawn, and strive to significantly adapt their operational approach in order to enable the U.S. Air Force's unique ability to seize the initiative in any future conflict. A full understanding of potential adversary IADS centers of gravity—including human dependencies, critical equipment and infrastructure, communications, plans, and deployment and employment tactics, techniques, and procedures will remain critical to developing and executing an effective multi-domain counter-IADS strategy. These requirements will only rise as system complexity steadily increases and technologies improve through the 2030s and beyond. ✪

Endnotes

1 VeraLinn Jamieson and Maurizio Calabrese, "An ISR Perspective on Fusion Warfare," *The Mitchell Forum*, No. 1 (Arlington, VA: The Mitchell Institute for Aerospace Studies, October 2015): 1-9, http://docs.wixstatic.com/ugd/a2dd91_df2f54c534b34ac1bac674b7379aa788.pdf (all links accessed May 2019).

2 John A. Warden, *The Air Campaign: Planning for Combat* (Washington, DC: National Defense University Press, 1988), 13, https://apps.dtic.mil/dtic/tr/fulltext/u2/a259303.pdf.

3 Author email exchange with Lynne Braun, National Air and Space Intelligence Center (NASIC) IADS Analyst, March 2019. The description of an IADS quoted here was attributed to David B. Culp, of SAIC, by Braun in her exchange with the author.

4 Lester W. Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth, KS: U.S. Army Foreign Military Studies Office, 2016), 266, https://www.armyupress.army.mil/Portals/7/Hot%20Spots/Documents/Russia/2017-07-The-Russian-Way-of-War-Grau-Bartles.pdf.

5 Ibid.

6 Grau and Bartles, *The Russian Way of War*, 268.

7 Joint Chiefs of Staff, *Joint Targeting,* JP 3-60 (Washington, DC: Joint Chiefs of Staff, September 28, 2018).

8 *Merriam-Webster Online*, s.v. "System," https://www.merriam-webster.com/dictionary/system.

9 Rosoboronexport, "Air Defence Missile System S-400 Triumph," online English language fact page, http://roe.ru/eng/catalog/air-defence-systems/air-defense-systems-and-mounts/s-400-triumf/.

10 Rosoboronexport, "Air Defence Missile/Gun System Pantsir-S1," Online English language fact page, http://roe.ru/eng/catalog/air-defence-systems/air-defense-systems-and-mounts/pantsir-s1/.

11 Merriam-Webster Online, s.v. "Integrate," https://www.merriam-webster.com/dictionary/integrate.

12 Stanley A. McChrystal, Tantum Collins, David Silverman, and Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio/Penguin, 2015), 57.

13 United States Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Arlington, VA: Department of Defense, January 2018), 2.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Maj Peter W. Mattes, USAF, is an intelligence officer, currently serving as the director of operations for the 19th Weapons Squadron, Nellis AFB, NV, part of the Air Force Weapons School. He leads the squadron's weapons instructor course (WIC) cadre and is a senior instructor teaching the Air Force's most advanced and integrated intelligence, surveillance, and reconnaissance (ISR) training. Mattes is responsible for day-to-day squadron operations, and leadership of the permanent party and students. In addition to serving as an Air Force Weapons School instructor, he has supported a variety of Air Force platforms and missions, specifically the F-16CM, the Distributed Common Ground System (DCGS), and Air Operation Centers (AOC). Mattes has deployed in support of Operations Odyssey Dawn, Unified Protector, New Dawn, Freedom's Sentinel, Resolute Support, Restore Hope and Inherent Resolve. He earned a B.S. in systems engineering management and his commission from the U.S. Air Force Academy in 2008.

Mattes would like to thank Air Force Lt Gen VeraLinn "Dash" Jamieson, Lt Col Brandon Alford, Mark Butler, Lynne Braun, Antonio Brown, John Callaghan, Brian Fishpaugh, and Jeff Lierly for their contributions to this analysis. All views expressed are those of the author and do not necessarily reflect the views of these contributors, the U.S. Air Force, or the Department of Defense.