REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
20-04-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE

Counterintelligence and Future War:
How the Office of Special Investigations is Poised to Support Department of Air Force Commanders

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Galvan, Vanessa (Major)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The US Department of Defense (DOD) fulfills a duty to the American public to maintain an ample supply of proficient service members capable of deterring war and ensuring national security. In 2018, release of the updated National Defense Strategy tasked a DOD-wide adjustment and encouraged a redesign of service-specific manning, finances, and capabilities. The services were tasked to be jointly competitive in any domain, despite great power competition from near peer threats, and regardless of future conflict. DAF commanders are therefore expected to recognize and respond to near peer threats using capabilities from across the range of military operations. A practical and proven method to meet these needs is through leveraging CI activities, such as information and activities meant to protect against foreign espionage or intelligence activities as predicated by the National Security Act of 1947. DAF commanders can leverage the OSI as a reputable and evolving federal law enforcement and CI agency to provide CI expertise in non-permissive and domestic environments. OSI will guard critical technologies and data; detect and mitigate threats; deliver global specialized services; conduct critical criminal investigations; and offensively engage foreign adversaries and threats. This arsenal of adaptive capabilities reinforced by unique operational authorities derived from Executive Order 12333 are tools available for the DAF to promote US national security interests in a more comprehensive manner than conventional DAF intelligence entities can provide.

15. SUBJECT TERMS
Counterintelligence; Office of Special Investigations; Department of Air Force; future war; law enforcement

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	44	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Counterintelligence and Future War: How the Office of Special Investigations is Poised to Support Department of Air Force Commanders

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Vanessa Galvan, United States Air Force

AY 2019-20

Mentor and Oral Defense Committee Member: Dr. Claire M. Metelits, PhD
Approved: //SIGNED//
Date: 20 APRIL 2020

Oral Defense Committee Member: Brigadier General Terry L. Bullard, Commander, OSI
Approved: //SIGNED//
Date: 20 APRIL 2020

Executive Summary

Title: Counterintelligence and Future War: How the Office of Special Investigations is Poised to Support Department of Air Force Commanders

Author: Major Vanessa Galvan, United States Air Force

Thesis: This paper contends that counterintelligence (CI) is a vital aspect of warfighting, and the Department of Air Force (DAF) commanders should employ CI in future wars planning, policy, and operational efforts. The Office of Special Investigations (OSI) can help illuminate the obscurity of future war, operate in a multi-domain conflict, and enhance DAF desired end states.

Discussion: The US Department of Defense (DOD) fulfills a duty to the American public to maintain an ample supply of proficient service members capable of deterring war and ensuring national security. In 2018, release of the updated National Defense Strategy tasked a DOD-wide adjustment and encouraged a redesign of service-specific manning, finances, and capabilities. The services were tasked to be jointly competitive in any domain, despite great power competition from near peer threats, and regardless of future conflict. DAF commanders are therefore expected to recognize and respond to near peer threats using capabilities from across the range of military operations. A practical and proven method to meet these needs is through leveraging CI activities, such as information and activities meant to protect against foreign espionage or intelligence activities as predicated by the National Security Act of 1947. DAF commanders can leverage the OSI as a reputable and evolving federal law enforcement and CI agency to provide CI expertise in non-permissive and domestic environments. OSI will guard critical technologies and data; detect and mitigate threats; deliver global specialized services; conduct critical criminal investigations; and offensively engage foreign adversaries and threats. This arsenal of adaptive capabilities reinforced by unique operational authorities derived from Executive Order 12333 are tools available for the DAF to promote US national security interests in a more comprehensive manner than conventional DAF intelligence entities can provide.

Conclusion: OSI is the DAF decision-maker's most robust defense in understanding evolving threats to their respective operational environments. OSI's CI authorities and especially its CI support to force protection activities provide more operational latitude than what traditional DAF intelligence and law enforcement entities can provide. OSI can also supplement traditional DAF intelligence community gaps in CI training and experience. OSI subject matter experts should be embedded in key DAF billets to ensure creativity and courage help bolster the DAF against future adversaries. OSI is a CI-capable force poised to support DAF commanders in future war triumph.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

THE OFFICE OF SPECIAL INVESTIGATIONS (OSI) PROVIDES SUPPORT TO THE DEPARTMENT OF THE AIR FORCE WHICH ENCOMPASSES THE US AIR FORCE AND US SPACE FORCE AS OF 20 FEBRUARY 2020. LEGACY REFERENCES TO THE OSI PREDATING 20 FEBRUARY 2020 WILL APPEAR THROUGHOUT THIS PAPER AS THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS (AFOSI). BOTH DENOTATIONS OF THE AFOSI OR OSI SHOULD BE CONSIDERED INTERCHANGEABLE FOR THE PURPOSES OF THIS PAPER.

List of Tables

Page

Table 1. MCIO Training & Agent Status Comparison 5
Table 2. OSI LOEs Nested within DAF Priorities 7
Table 3. OSI Integration to the Joint Planning Process and the Intelligence Process 24
Table 4. OSI Examples via the Joint Planning Process 25
Table 5. OSI Integration to the AFWIC Operating Construct 26

Table of Contents

Page

EXECUTIVE SUMMARY ii

DISCLAIMER iii

LIST OF TABLES iv

PREFACE vi

INTRODUCTION 1

OSI AS A WARFIGHTING CAPABILITY 3

DEPARTMENT OF AIR FORCE PREPARATION FOR MULTIDOMAIN CONFLICT 13

IMAGINING FUTURE WAR 18

RECOMMENDATIONS AND BEST PRACTICES 22

CONCLUSION 27

ACRONYMS 28

ENDNOTES 29

BIBLIOGRAPHY 33

Preface

In December 2015, a television newsfeed of Americans killed in Afghanistan was confirmed as the Office of Special Investigation's (OSI) deadliest loss of life at one time. Four special agents and two partnered Security Forces Defenders were killed by a motorcycle-borne improvised explosive device attack during a routine mission outside of the defended base perimeter, commonly referred to as outside the wire, or OTW missions. These missions exhibit counterintelligence (CI) support to force protection (FP) and they provide Department of Air Force (DAF) commanders an intimate understanding of non-permissive environments and help shape ways to identify and mitigate viable threats to Air Force assets. The 2015 mission was no exception, although the attack prompted OSI senior leaders to temporarily suspend such missions and evaluate how it conducted CI activities. The review affirmed the value of OSI methods, yet it identified a need to evolve and bolster OSI's CI mission to counter a rapidly changing national security environment. In preparation to assume command of OSI, Brigadier General (BG) Terry Bullard determined the agency's future would enhance DAF preparation for multi-domain conflict via its full-spectrum CI program. A vital counterbalance to increasing near peer threat competition, OSI's family of agents, linguists, support staff, and industry partners combine resources, capabilities, technology, and skills in order to shape DAF defense and bolster the intelligence community (IC). OSI's CI authorities and activities provide more operational latitude than what traditional DAF intelligence and law enforcement entities can, to include OTW missions when appropriate. Fellow agents and other brothers and sisters in arms must not falter in our necessary pursuit to shape future warfare and help prevent premature ends-of-watch.

- Dedicated to our Fallen[1]

"[The Office of Special Investigations] must enable the Air Force to confront and engage peer and near-peer competitors in the regions they look to dominate, counter rogue nations, and continue to battle the global scourge of violent extremism.[2]"

- *BG Terry Bullard*
  Commander, OSI

Introduction

The US Department of Defense (DOD) fulfills a duty to the American public to maintain an ample supply of proficient service members capable of deterring war and ensuring national security.[3] These capabilities are realized through ensured force lethality, strong coalition partnerships, and flexibility to adjust the department as needed.[4] Release of the 2018 National Defense Strategy (NDS) prompted a DOD-wide adjustment, as it encouraged a redesign of service-specific manning, finances, and capabilities. The military services were tasked to be jointly competitive in any domain, despite growing near peer threats and regardless of future conflict.[5] In anticipation of great power conflict, the US Air Force (USAF) redesigned its warfighting platforms, officer promotion practices, and mobility and logistics arenas.[6] Despite aspirations to grow to 386 operational squadrons within the next decade,[7] it was deemed financially unlikely.[8] Regardless, the USAF is currently facing wide-ranging threats[9] to counter and reinforce their role as a legitimate and adaptable warfighting option. Although senior civilian policy makers and military commanders obligingly adjust force design models and budget allocations in consideration of prospective conflict, NDS alignment is not enough to ensure future war success.

Anticipating the potential enemy, alongside their motivations and capabilities, will increase military service preparedness for future conflict. Department of Air Force (DAF) commanders are expected to recognize and respond to near peer threats using capabilities from across the range of military operations.[10] A practical and proven method to meet these needs is

through leveraging counterintelligence (CI) activities. A timeless effort, CI includes the collection of intelligence and conducting activities to defend against foreign-endorsed espionage or intelligence actions[11] as predicated by the National Security Act of 1947. For DAF commanders, the Office of Special Investigations (OSI) is their exclusive agency to provide CI expertise. Comprised of roughly 3,000 agents and support personnel, the OSI family directly impacts the safety and viability of both United States and coalition partners in non-permissive and domestic environments. OSI publicly outlines that they provide partner nations and domestic industry partners capabilities to guard key technologies and data; identify and thwart threats; deliver focused global support; conduct critical criminal investigations; and offensively challenge foreign enemies and threats.[12]" This arsenal of adaptive capabilities provides the DAF exclusive tools to promote US national security interests.

Global security conditions continue to challenge US priorities, and how US military services respond is critical to their force relevancy and longevity. Multi-domain conflict looms over all the services in their efforts to ensure national priorities are protected. Perhaps most impacted now is the DAF, which has shifted its force design posture to accommodate air and space domains in future war. A 2019 Rand study on inter-service considerations for modern-to-future war, suggests the USAF is amid a core identity quandary; unsure of its relevance as a simultaneous warfighter and enabler.[13] Notably absent from many current joint force leadership positions, are DAF commanders.[14] Consequently, Joint Publication (JP) 3-10, *Joint Security Operations in Theater* recognizes that "an effective CI process is one of the most important ways commanders…can contribute to maintaining adequate joint security.[15]" USAF contributions to a near peer fight cannot simply hedge on air superiority and orchestrated targeting and intelligence, surveillance, and reconnaissance (ISR) assets.[16]

The DAF has another asset to closer incorporate with ground operations integrated across joint, partner, and multi-service elements: its OSI agents and their inherent CI capabilities. Whether through CI support to FP and DAF asset protection, to sharing technical best practices with allied partners, OSI agents have the prowess and individual relationship building skills germane to any conflict or environment. As US military services continue to plan and posture for future war success, DAF commanders should enable OSI CI as an essential planning and execution tool. This paper contends that CI is a vital aspect of warfighting, and DAF commanders should employ CI in future wars planning, policy, and operational efforts. OSI can help illuminate the obscurity of future war, operate in a multi-domain conflict, and enhance DAF desired end states.

OSI as a Warfighting Capability

Fashioned after the Federal Bureau of Investigations, the OSI was established in August 1948 as a Congressional initiative to align various USAF investigative efforts in an unbiased, professional manner.[17] OSI agents are borne of extensive security background investigations and formal selection boards based on a whole person concept. Uniquely comprised of civilian, enlisted, and commissioned officer special agents, all screened and designated OSI applicants must successfully complete the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) to earn their badge and credentials. FLETC provides US federal LE entities the same foundational start; it is attended by over ninety additional federal LE agencies and has been an OSI partner for the past sixteen years.[18] OSI agent trainees specialize in weapons, defense tactics, crime scene processing and forensics, antiterrorism (AT) training, interrogations or interviews, court testimony, and military and

federal law studies while at FLETC.[19] Depending on the sensitivity of some OSI missions, credentialed agents may also undergo additional screening methods such as polygraph examinations or special access program procedures.

OSI blends felony-level criminal justice with an equal emphasis and responsibility on CI. This distinguishes OSI from the other military criminal investigative organizations (MCIO) across the DOD (*see Table 1*) whom are compartmentalized into LE or intelligence duties. For the DAF, non-OSI law enforcement is made up of Security Forces, whose Defenders provide an initial layer of protection for an installation ranging from perimeter defense, airplane defense, or physical protection of US nuclear capabilities.[20] DAF intelligence capabilities, even when expanded for US Space Force (USSF) interests, are tied to analyzing raw data and pulling usable intelligence for commanders to use in planning or operations.[21] Most like OSI, the Department of the Navy (DON) has the Naval Criminal Investigative Services (NCIS) to conduct felony-level LE and CI activities. This capability extends to US Marine Corps (USMC), although USMC law enforcement battalions – most like DAF Security Forces – will undergo a phased divestment of three battalions by 2030 due to excess capacity identified in their force design concept.[22] For the Department of Army, their traditional LE and intelligence capabilities are spread across a broad spectrum of analytic and operational support entities, whom are common liaison partners with OSI agents in non-permissive environments.

Operating within dual federal LE and CI lanes instead of fragmenting capabilities into separate LE and intelligence activities like sister services, means OSI agents provide DAF commanders a comprehensive opportunity to recognize and respond to viable threats with minimal division of effort. The mission cohesiveness fosters greater information sharing, more precise support to the intelligence community (IC), and tailored capabilities for commanders;

especially those in contested environments. OSI efforts in non-permissive scenarios engage in analytic exchanges or utilize the foreign disclosure process to release sensitive or classified information to host nation security partners. This builds trust, increases informational awareness of potential installation impacts, shapes atmospherics, and provides a means to return operations to host nation control when US and coalition forces depart.

Table 1: MCIO Training & Agent Status Comparison

US Military Service Department	Air Force*	Navy**	Army***
Agency	**OSI**	**NCIS**	**CID**
CITP Training	**X**	**X**	
Civilian Agents	**X**	**X**	**X**
Enlisted Agents	**X**		**X**
Officer Agents	**X**		**X**

* **Includes USSF**
Department of Air Force employs the following non-OSI specialty codes to conduct law enforcement and intelligence:
Air Force: **3P0** Security Forces (non-1811)
1N0 Operations Intelligence
Space Force: **1N0** All Source Intelligence
1N1 Geospatial Intelligence
1N2 Signals Intelligence

** **Includes USMC**
Marine military occupational specialties like OSI and NCIS include:
5811 Military Police
0211 Counterintelligence/Human Intelligence
0212 Technical Surveillance Countermeasures
0231 Intelligence Specialist
0239 Intelligence Analyst

*** **Department of Army** does not send personnel to FLETC
CID officer agents are limited to warrant officers
Army military occupational specialties like OSI and NCIS include:
31D Criminal Investigator (non-1811)
35L Counterintelligence Agent
35M Human Intelligence Collector

The USAF earmarked 500 new manpower billets through 2025[23] for the OSI command. These billets –in support of the NDS– help project the OSI's publicly postured mission "to identify, exploit and neutralize criminal, terrorist and intelligence threats to the USAF, DOD and US Government (USG).[24]" OSI services now extend to the USSF as well, which the USAF was apt to help stand up as a new sister service on December 20, 2019.[25] Sixty days after the USSF inception, BG Bullard reinforced that per SECAF, OSI is the lead LE and CI investigative entity to support USSF.[26] OSI's absorption of USSF support is not expected to substantially impact projected manning, training, funding, or deployment rotations for OSI,[27] although protection of a novel operational domain will require flexible resource and capabilities applications. In a 2016 white paper, General John Hyten warned, if the DOD collectively fails to "adopt new tactics, techniques and procedures…that deter aggression, and if deterrence fails, to enable swift and deliberate action,"[28] then the adversary will close the gap on US competitive advantage.[29] Four years after, Commander, Air Force Space Command commented that USSF's establishment recognizes space as a warfighting domain like the traditionally protected air, land, or sea.[30] DAF cannot afford to delay development of its respective operational environments, and should instead lean into lessons observed from prior conventional conflicts with evolving enemies.

A 2019 study regarding USAF readiness for distributed operations despite a contested domain examined increasingly sophisticated near-peer competitors. Rand suggested US national priorities in the 2018 NDS are quickly transitioning away from stability operations and toward disrupting and overwhelming major adversaries in non-permissive realms.[31] The 2018 NDS prompted senior military leaders to project their respective service needs toward future requirements. DOD objectives were tailored toward expected threat increases from near peer competitors[32] and the department's initial line of effort required an increasingly lethal force,

applicable toward conflict planning and execution via robust military readiness.[33] In spring 2020, the USAF defended its strategy against great power competition[34] to Congress with the Fiscal Year (FY) 2021 presidential budget hearing. Secretary of the AF (SECAF) Barbara Barrett and Chief of Staff of the Air Force, General Dave Goldfein presented a deliberate alignment between the NDS and the USAF of the future, recognizing the link between interconnected global military operations across a span of domains and myriad capabilities.

On February 27, 2020, Secretary Barrett utilized a growing communication medium of senior leaders, where she outlined current USAF priorities via Twitter. SECAF determined that parallel USAF and USSF focus areas can be attributed to the need for "modern, smart, connected, and strong[35]" services to discourage and protect against hostility and preserve liberty and peace.[36] To protect DAF's competitive advantage against near peer threats, OSI senior leadership must communicate preparedness for future war in a way the joint force can understand and leverage. Alignment of OSI priorities with DAF main efforts can reduce ambiguity of OSI as an operational asset and educate commanders on scalable options for conflict plans or missions. In December 2018, OSI released a strategic plan that identified four lines of effort (LOE) to shape the command's future trajectory through 2023. They nest within the DAF priorities (*see Table 2*) and carry an implication of how to apply CI to directly fortify relationships with partners and allies.

Table 2: OSI LOEs Nested within DAF Priorities

Nested Priorities	
DAF	**OSI**
Build the USSF	Develop an exceptional force
Modernize Air & Space Forces We Need	Cost-effectively modernize
Grow Strong Leaders & Resilient Families	Restore readiness
Strengthen our Allies & Partners	Drive innovation; strengthen OSI partnerships

In a 2019 letter to his command, BG Bullard asserted the future OSI force must grow its CI mission, develop a more robust and sustainable force to partner with the defense industrial base, and offensively protect critical and developing technologies across all domains where vulnerabilities and threats exist.[37] Further, the general ascertained that OSI must empower the DAF to "confront and engage peer and near-peer competitors in the regions they look to dominate, counter rogue nations, and continue to battle the global scourge of violent extremism.[38]" To achieve this, OSI agents should consider current CI practices and bolster creative partnerships with other industry, federal and local agencies. One way is through the general's Spartan Citadel initiative to employ approximately ten percent of allocated billets of OSI specialists to reinforce program integrity and protect technology development at contractor facilities.[39] Though physical OSI presence is already an historic practice, future threats from near peer threats with commensurate levels of sensitive information and data suggest OSI agents will need to integrate more closely with myriad partners. Efforts should aim to thwart threats, identify supply chain vulnerabilities, expose insider threat potential from involved teams, and then work to communicate these processes from start to end with DAF commanders.

Arguably, the crux of OSI CI support to force protection (FP) anticipates, hinders, and then counteracts threats[40] for DAF commanders. OSI agents are also authorized to pass relevant intelligence to foreign governments should it be necessary, which is a critical advantage to building partnerships for future coalitions. At USAF inception, OSI support was largely attributed to physical air base defense and defense of ground-based aircraft postured in hostile environments.[41] The evolution of physical threats to aircraft, air bases, and airmen highlighted a deficiency of reliable and actionable intelligence, however. Since commanders can apply OSI CI collections to future domains or emerging threats, the commanders must first understand the

problem they face in order to shape potential solutions and responsibly mitigate risks. Comparative of DOD investigative entities, OSI retains the most flexibility, authorities, and experience to provide valuable CI and federal LE skills in expeditionary and multi-domain environments. OSI agents are the sole DAF CI entity with derived authorities stemming largely from Executive Order (EO) 12333,[42] and empowered by the US Constitution to prudently balance intelligence activities and maintain the integrity of US citizenry rights.[43] Signed into law in 1981, EO 12333 asserts that within the constraints of the law, all judicious ways to seek out and obtain relevant and timely intelligence for the US government must be pursued.[44] Within the lawful bounds of the order, OSI agents capitalize in whatever domain they are operating in to inform DAF commanders using CI activities.

Ensuring protection of aircraft, mobility operations, and aircraft schedules to support ground troops and conduct kinetic missions are among the main concerns for air base commanders engaged in contingency operations. During conflict, the Joint Force Commander designates the Combined Joint Forces Air Component Commander (JFACC) to establish and ensure unity of effort for joint air operations.[45] In theater, the OSI operates in direct support of the JFACC and their priorities, with an emphasis on CI support to FP. The OSI capitalizes on placement and access within the environment and uses CI activities to shape a commander's posture within an operational domain. In current contingency operations of traditional domains for example, the positioning and vulnerability of aircraft remains as critical and pressing a concern as it was during Vietnam. Lessons observed in a 1995 Rand study noted that non-prioritization of air base defense via resource allocation directly resulted in insufficient response to standoff threats.[46] Former OSI command historian Christine Williamson reflected that Operations Enduring Freedom and Iraqi Freedom were the precipice of CI and AT missions, and

their results commanded notice at tactical and strategic levels of USAF echelons.[47] Blended OSI capabilities in an expeditionary capacity provide commanders a substantive crystal ball to understand threats to their forces and assets.

Air Force Instruction (AFI) 71-104 details the significance of OSI's role as the only DAF organization that can conduct CI investigations, operations, collections, and other activities.[48] It mandates that all OSI personnel engaged in conducting CI activities must attend and satisfactorily complete commensurate formal training approved by the DOD or a military department,[49] and this practice is generally aimed to further operations in non-permissive environments in support of FP or strategic measures set forward by the combatant commander. OSI's execution of relevant CI activities still leverage the recognized ground forces and airborne surveillance assets to prioritize threat mitigation and maintain a buffer[50] for DAF assets. In non-permissive environments, unpredictable threats by non-state actors, whom the *International Journal of Intelligence and Counterintelligence* highlight as an unconventional CI threat that the IC must impact through network disruption,[51] is primarily addressed through OSI's proactive and offensive CI efforts. OSI agents appreciate how to frame offensive CI operations in non-permissive environments in order to reveal adversary capabilities, expose their targeting needs, and minimize their operational efficacy[52]" as it relates to FP and strategic IC awareness.

As the DAF re-postures in preparation for future conflict, OSI contributions must also be reviewed for relevancy and at the appropriate level. Technologies and aircraft protection remain the main priority of a superior USAF and the JFACC, which is fortified with CI activities. OSI should inform the JFACC and subordinate commanders directly of CI-based critical findings or operations to allow for timely and appropriate responses. Historically, air base defense endured the majority of damaged aircraft or negative disruptions to air task orders (theater-wide schedule

of sorties to be in the designated airspace within a set timeframe) through infiltration of insider sabotage, harassment from locals, or ground attacks from enemy forces.[53] Air base defense and aerial asset protection were prominent in the early 1990's, which marked a notable shift in modern warfighting. Gulf War observations suggested a distinct advantage to having allies and staging areas near conflict zones, and warned that modern air entities operating in desert locations should be wary of false security from small-unit attacks despite long distances between them and the fight.[54] Since then, ongoing operations in Southwest Asia with a multitude of DOD entities on the ground, sea, or air at any given moment demand commanders increasingly rely on dependable ground and air intelligence. Due in part to OSI's effective management of non-permissive environments using its LE and CI operational authorities, OSI is designed to be a robust and flexible force.[55] Agents turn CI activities into relevant information for commanders to assess risk to their forces and assets. In non-permissive environments, placement and access are integral for reliable information. OTW missions and creative application of informed ground forces and aerial ISR support dedicated to FP can glean actionable intelligence from human sources and official liaison contacts to inform commander decisions. Generally, non-OSI military intelligence or HUMINT collectors are limited in scope and authority by how deeply they can operate in an environment. The additional maneuverability and application of OSI agents provides DAF commanders an in-depth understanding of operational environments instead of simply evaluating atmospherics at superficial levels.

The Post-Cold War transition for the USAF saw an increase in air power requirements in support of national security objectives and contributed to a steep rise of deployments and the semi-permanence[56] of expeditionary operations. Expanded OSI capabilities in support of air base defense and FP despite unrelenting global conflict led OSI planners and commanders to

reconfigure the OSI deployment process to complement USAF deployment air and space expeditionary force (AEF) rotation cycles.[57] The AEF cycle was meant to provide airmen with predictability for when they were eligible for deployment, and consequently support stability[58] for personal life and garrison work. In 1992, a change to OSI's command structure[59] occurred, where the command was divided into geographic districts of field investigations regions, detachments and smaller operating locations aligned with USAF major commands.[60] The effectiveness of this new construct was first stressed with the 1996 Khobar Tower terrorist bombings. OSI determined its command and control construct adequately empowered USAF commanders, and then by summer of 2002, the OSI further refined its deployment model, as it altered agent deployment rotation cycles to better meet USAF deployment requirements[61] in both style and tempo.

From a commander's vantage point, knowing the situation and how to affect the space in pursuit of asset protection is critical. OSI has traditionally shaped physical base defense, starting with a rapid deployment force able to integrate into any environment. The OSI formed an Antiterrorism Specialty Team [AST][62] to deliver USAF commanders a global, rapid-mobility CI/AT capability.[63] Williamson noted how post-September 11, 2001 attacks led to early agent insertions to hostile areas to preempt the arrival of major forces with relevant and reliable threat information; this provided an accurate assessment of USAF vulnerabilities.[64] A 2005 assessment on how best to utilize OSI in future warfare amid global terrorism included the continuance of OSI provision of steady amounts of agents as a bolster.[65] Nearly two decades later, OSI's committed deployed force has settled at nearly a quarter of its agent and specialist population.[66] OSI CI activities can also strengthen diplomacy through meaningful information sharing,[67] which is germane to promoting the White House's National Defense Strategy in spite of

adversarial intentions. OSI activities further assist in shaping the DAF's response evolution to novel conflict scenarios and enemies.

In a 2019 *War on the Rocks* interview, General Goldfein inferred that multi-domain operations would be critical to success in a cyber or space-based conflict.[68] If these complex arenas were challenged, the DAF would need to "simultaneously overwhelm an adversary by converging capabilities at a time and place of [their] choosing.[69]" This approach can be enhanced with early application of OSI CI capabilities, to ensure DAF commanders can make educated battlespace decisions. Commanders can benefit from including agents in the planning, exercise, and mission execution phases of conflict. With a traditional domain such as land or sea, agents have often been a physical presence on the first flight manifests to assess a bare base or new environment for threats. As domains shift and may not require or permit a physical presence, however, OSI is evolving its workforce's technical and creative proficiency through recruitment and training measures. Junior to mid-level applicants with cyber, special operations, intelligence, CI, or foreign language and living experiences[70] are increasingly sought out for OSI service. These focus areas are not meant to detract from law enforcement or legal backgrounds which are important to OSI's overall mission, but instead will bolster OSI competency and creativity to assess and respond to future threats and new contested domains.

Department of Air Force Preparation for Multidomain Conflict

OSI units operating in the Middle East during the summer of 2019 provided DAF commanders with a threat assessment of stationary aircraft in contested environments. A sophisticated exercise followed, and for twenty-four consecutive hours,[71] command and control of all aircraft within Central Command's scope transitioned from the Combined Air and Space

Operations Center (CAOC) in Qatar back to domestic soil on a South Carolina base.[72] CAOC officials observed that growing risks coupled with new technologies are prompting US officials to reassess whether some foreign-based operations should instead be home-based.[73] Nearly a week prior to the CAOC operational shift, Gen Goldfein addressed the Air Force Association's annual Air, Space and Cyber Conference about the reality of multi-domain operations. As he laid out to his forces, the USAF must transition from a platform (e.g. specific aircraft) mentality, to one focused on interconnectedness (e.g. human interactions, information sharing, real-time transparency, uniform network capabilities).[74] OSI CI activities give life to the concept of interconnectedness. The offensive and comprehensive approach of agents and their teams help bolster security and inform commanders of players in their battlespace and how to counter an adversary's influence.

OSI operational authorities are retained by the SECAF, although in contested environments they can be employed under the combatant commander for specific missions.[75] In general, the prudent use of OSI agents and their extensive CI authorities manifest from a span of professional staffing, and an appreciation for melding security measures with creative thought. Regardless of operational environments and available resources, agents promote a heterogeneous approach to base defense outside the confines of a defended base perimeter. Safety and integrity inside the wire (ITW) is commensurate with practical understanding and influence of the OTW environment. OSI cannot fully address both ITW and OTW vulnerabilities in hostile territories, so comprehensive and transparent initiatives with traditional security forces and intelligence entities should be fostered. With the majority of OSI deployments to non-permissive environments within Southwest Asia, the Pacific, and Africa, CI collections are intended to serve both a tactical FP initiative and craft a battlespace with ensured freedom of movement or

maneuver for US and coalition partners. Allowance of friendly freedom of maneuver consequently inhibits the same for enemy forces.

OSI's daily actions to protect DAF assets, Airmen, and Space personnel[76] prompts manning and resourcing considerations. Efforts to reinforce the staffing and resiliency of the AST agent will include additional training opportunities, like some traditional Special Forces[77] courses to ensure an adaptable and independent CI asset. Management of the AST has been allocated to OSI's epicenter, or ICON Center as of May 2018.[78] Bred as a command-wide analytic and field agent resource, the ICON Center promotes comprehensive support and capabilities to apply OSI support elements or information toward critical DAF decision points or threat scenarios.[79] The ICON is further designed to support global USAF missions with a team approach divided by geographic or functional missions, although it remains outside of major command or geographic combatant command subordination.[80] This degree of separation facilitates operational objectivity for the agents and thus reduces undue command influence over OSI capabilities and findings. The autonomy of OSI CI activities and their results prevent compromise; if a target is neutralized based off OSI CI collections, the veracity of information and the operation remains valid.

OSI dissects an operational environment beyond its agent support capabilities. This is first reinforced via a talented pool of support staff, to include language and cultural advisors. OSI Agents work alongside Category Two and Three linguists who hold security clearances and have passed CI polygraph examinations to better navigate non-permissive environments with added assurance of agent safety and mission integrity. Typically, each employed linguist has cultural awareness or background in the area of operation to further enhance environmental clarity. Additionally, agent teams operate with in-house targeting analysts who help agents

transform their raw intelligence – usually obtained from human sources – into finalized products for greater IC consumption; generally, through Intelligence Information Reports (IIRs). In 2019 alone, over fifty percent of OSI-published IIRs garnered an evaluation rating from the IC,[81] reinforcing community interest in, and validity of OSI CI collections. This work helps shape contested environments while informing civilian decision makers of realities in the field, sans sensational media reports.

In November 2019, the OSI Commander penned a transition notification. He identified a need to develop the DOD and interagency relationships[82] in alignment with national priorities. Manning allocations have been adjusted in parallel with concerted efforts to cross-pollinate agents and support staff into career-broadening jobs outside of the OSI career field. These staff are to remain informed and in contact with OSI headquarters elements to ensure transparency and networking about information, resources, and capabilities. The cross-pollination is intended to reinforce the breadth of OSI capabilities to senior levels of US military and government channels, as well as focus OSI efforts to meet congressionally mandated requirements and protect the evolving needs of Air Force assets. The task force construct to combat adversaries is effective as well. Combining DAF specialists and their respective authorities or technical expertise expands operational reach and allows for more latitude and creativity in pursuing an enemy. It also provides a more comprehensive sight picture of the operational environment, better informing DAF commanders. The OSI with its customers must dually understand and communicate how CI operations reinforce strategic intent in support of national security objectives and a whole of government approach.

Independent of the doctrinal lifespan of counterinsurgency (COIN) operations, CI collections and human source dynamics still fit into a COIN-based hearts and minds schema.

COIN operations, according to JP 3-24, require combined action with the interagency and inter-organizational coordination of instruments of national power in order to reinforce a host nation's governance and legitimacy.[83] Every collection received is an opportunity to create or fill a priority intelligence requirement for the IC or provide a missing piece for a targeting analyst, and may serve as a trigger for a kinetic operation. Ganesh Sitaraman recognizes that successful COIN is a result of interagency cooperation—between political, military, police, administrative, economic, and cultural actors.[84] A snippet highlighting the danger of non-state actors (NSAs) in a 2009 CI Threat publication explained that the US must balance between sharing intelligence on mutual threats with other governments and militaries, while still protecting its national interests. In practice, liaison is a force multiplier for US interests, yet can also present a concern for CI agents and HUMINT collectors from coalition and US military counterparts. The threat of working with NSAs in non-permissive environments presents challenges in maintaining a power position as a commander. Risk to force or personnel can manifest in many ways. Related to future war in a space domain with NSAs, the threat could begin as the loss of proprietary information from a military research and development project. Next, it could lead to a degradation of DAF systems and resources as the nodes are disrupted, degraded, or destroyed. If forces are present or deploy to mitigate the threat, then an ensuing risk to operations with potential loss of life in its most extreme cases could occur. Extended operations in the Middle East have systemic enemy behaviors where they collect intelligence, materials, and access in order to conduct insider attacks and kill US and coalition partners.

Although the details of future conflict and adversaries remain elusive, proper planning with OSI insight and considerations of available CI collections and IIRs can alleviate some potential for trauma. A way to posture for future conflict damage is to understand the

environment and capabilities of others. OSI remains postured to capitalize on placement and access within environments that are often restricted or not understood. Technological proficiency, human source relationships, and robust targeting analysis provide three ways in which OSI can provide DAF commanders an opportunity to better understand and shape their operational domains. Senior OSI leadership must maintain enough clout with external chain commanders to promote resources, funding, and the support needed to maintain its ability to accurately defend DAF interests and assets worldwide. In a rapidly evolving world, implications from OSI's contributions to thwarting threats are validated with assets such as the AST, multi-specialty task forces, or its recruitment focus to meet near peer challenges in future war scenarios. To what degree OSI's contributions will shape DAF decisions in new environments, however, remains presumptive.

Imagining Future War

As DoD-wide plans are crafted in anticipation of future war, reality suggests US national interests should be assessed against vulnerabilities outlined in the NDS. The US is no longer the atomic juggernaut amid a post-Cold War era of nuclear containment. Instead, global adversaries, many with unstable governance, are refining nuclear arsenals which the DAF is keenly set to deter. A Lawfare Institute book review of *The Future of War* suggests a future enemy's technological advances and how to mitigate the technical problem do not matter.[85] What does matter, is an intellectual and conceptual approach to the future environment of war, because conflict or asset loss will all come down to how best the enemy can outthink the American military commander.[86] History reinforces that the United States' exposure to unexpected

security issues will also not abate,[87] which affects the intelligence analytic posture[88] as the DAF prepares for future war.

Conventional intelligence resources do not adapt readily to surprise situations,[89] and instead provide an oft reactive, or defensive assessment of enemy behaviors. OSI on the other hand, provides commanders the distinction of being offensive in nature, as it aims to identify enemy behaviors and trends prior to nefarious incidents. In a current deployed location with adversarial NSAs for example, DAF commanders can leverage OSI's CI capabilities to simultaneously identify tangible threats like an imminent rocket attack, and the details preempting an attack. Such collections can include players involved, their motivations, key nodes of the NSA network, and enemy vulnerabilities making follow-on friendly operations feasible. Some may argue traditional DAF intelligence entities could provide the same details based on conventional analysis of historic trends or knowledge of the general area, yet OSI's CI capabilities are also uniquely bolstered by a law enforcement framework.

The investigator mindset, when applied to CI, allows a full rendition of targeting approaches to shape a battlespace instead of just collecting details of events which already transpired against DAF assets. Within the USAF intelligence community, CI operational experience is one of two job requirements for Major through Colonel ranks where the need for its expertise outweighs the pool of experienced candidates.[90] The OSI can minimize the impact of this gap for DAF commanders, by assisting the DAF intelligence community with CI support. Realistically, some commanders may not be comfortable turning to OSI as an intelligence function if they believe the agency to be a purely law enforcement asset, so transparent liaison with intelligence counterparts is a critical component of informing commanders of OSI's

available CI capabilities. This relational exchange is more important as DAF commanders strive to predict the future and their role in unknown warfare.

As the space domain grows and commercializes, and additional domains evolve as battlespaces, the DAF should fortify its personnel adjustments with a concentration on OSI support. Capable adversaries will increasingly complicate coordinated attacks or perhaps tailor attacks at specific bases,[91] according to Miranda Priebe in a Rand assessment of distributed operations. Elements of the unknown will present an opportunity for risk management and subsequent sets of options to be evaluated by accountable commanders. The study suggests a combined effort toward base defense and FP will meld threat information and mitigation options so that commanders could make informed decision.[92] The researchers even recommended retraining of airmen to enhance their skills beyond their specialty,[93] which notionally could train conventional intelligence assets on CI, for example. While appropriate as a recommendation, the reality of cross training numerous airmen to increase resourcing across operational environments is impractical despite current force re-posturing. An applicable support element, however, is the OSI agent. A commander's decision-making lens can be stretched to better understand the area of responsibility through integration and incorporation of OSI CI activities into planning and operations.

The US Intelligence Community, highlights "collection, analysis, counterintelligence, and covert action,[94]" as the four types of intelligence activities, and are tied to the intelligence cycle according to Jeffrey Richelson. The cycle (see *Table 3*) as employed by OSI agents through talented and diverse personnel and their unities of effort, provide an opportunity for commanders to understand their operational environment (OE) and capitalize on its proactive shaping. Where the distinction from the OSI advantage stems, is in its ability to obtain, analyze, and

operationalize the myriad information that often overwhelms decision makers regarding potential threats to assets and forces. The findings of a 2019 study on how intelligence assessments inform decision-making[95] purported that without an educated evaluation of intelligence, every single droplet of information must be viewed as entirely trustworthy.[96] This would entirely overwhelm commanders and exhaust emergency preparedness to thwart illegitimate threats. OSI agents and analysts are specially trained and operationally experienced to slice through the chafe of those redundant areas of collection and to identify credible aspects of threats and adversary networks to exploit. How this valuable currency is expended remains largely dependent on an individual commander's comfort with risk mitigation and an appreciation for underlying regulations and policies to take innovative yet legal operational risks in contested environments.

A potential, yet underrecognized method to disrupt an enemy's impact on DAF assets and personnel is lawfare as a form of warfare. Arguably, the US government does employ diplomatic lawfare most recognizably via economic sanctions on near peer adversaries, yet it has not been codified as a national security strategy nor recognized widely as a viable military tool. Lawfare can be associated with an array of definitions and examples, but for the purpose of this paper and in the context of OSI CI activities, may simply describe a tool to achieve a DAF commander's desired end state in support of FP or asset management. Major General Charlie Dunlap, USAF, retired, penned lawfare as the "strategy of using – or misusing – law as a substitute for traditional military means to achieve a warfighting objective.[97]" Dunlap then narrowed enemy use of lawfare into two sections: first, battlefield tactics to affect US operations[98] such as insurgent use of human shields which could affect DAF kinetic strike support, and second, wielding control over US legal systems to affect the US military.[99] The second tactic can be seen in the currently developing International Criminal Court (ICC) decision

to conduct an investigation into potential US war crimes from Afghanistan.[100] This not only affects global perception of US adherence to rule of law in war, but it has potential to strain ally relationships and resourcing if the US takes the unprecedented route of sanctioning the ICC in retaliation,[101] or if the findings are unfavorable toward US military activities and personnel.

Perception shaped by an adversary and its effect on DAF resource allocation requires early and nuanced intervention with host nation and allied security counterparts to preempt negative fallout. *Lawfare: Law as a Weapon of War* framed a US predisposition to believe nothing is absolute, and consequently can be shaped to include strategic and agile resourcing[102] at the forefront of all military planning. Orde Kittrie contends law is simply a prominent tool in warfare and how each combatant wields control over the law as an actual tool shapes a tangible outcome.[103] Lawfare, then can be inserted into various types and levels of disputes[104] to shape the battlespace, and OSI professionals can likewise be inserted to accomplish the same for DAF interests. Translated to traditional operational domains, these acts can be manifested via liaison relationships OSI holds with host nation security partners to bolster local judiciary practices or LE-inspired information exchanges. Potential to shape an operational environment by motivating counterpart best practices in evidence collection, interview methodology, and early warning identifiers can reinforce host nation law enforcement legitimacy and stabilize the environment. These CI applications lessen an adversary's impact on DAF assets and personnel.

Recommendations and Best Practices

The OSI must actively promote its growing preparedness for future war. Its impactful CI operations can increasingly benefit DAF commanders from their seamless application of blended authorities and operational mobility. Some current best practices impacting global expeditionary

endeavors start in garrison, where OSI units are tenants to a host wing. The wing commander – generally also the installation commander – is not in charge of the tenant OSI yet should rely on the OSI for any federal LE or CI matters of concern. At installations where Contingency Response (CR) Forces are present, OSI generally has AST personnel allocated to assist with exercise or operational deployments. A scalable entity, the CR Groups can support any contingency, worldwide.[105] In an ideal world, sans fiscal, personnel, and other general constraints, OSI would be able to attend every exercise or deployment. The reality is OSI cannot physically cover all phases of planning and mission execution. In practice, OSI ICON leadership entities should be involved in routine CR planning sessions at higher headquarter levels to communicate relevant AST capabilities and guidance, regardless of whether a physical body can be allocated toward individual missions. This would not only boost an awareness of OSI expeditionary capabilities but would bolster professional relationships between the base leadership and agent teams from top-down communication and influence. OSI can also consider its involvement in the JPP structure to ensure it can be easily leveraged.

The Joint Planning Process (JPP) is an established way for OSI to highlight its capabilities for operational use to deployed commanders in wartime or peace. Meant to allocate military activities in support of national objectives[106] properly, the JPP aids commanders and their planners to shape their planning actions, recognize a shared mission and commander's intent, and then create effective strategies and orders.[107] CI can be interlaced at each of the seven steps (*See Table 3*). JP 3-0 further outlines DOD intelligence capabilities, resources, and persons may be used for CI.[108] Currently, the joint approach to incorporate CI is detailed in JP 2-0. It affirms, "CI should be factored in whenever US intelligence or national security capabilities are

deployed or when we are targeted by our adversaries." As multiple domains begin to be analyzed for future war, so too should OSI consider ways to publicize their support to the JPP.

Table 3: OSI Integration to the Joint Planning Process and the Intelligence Process

Joint Planning Process*	OSI CI Functions**	Intelligence Process***
Planning Initiation	Collection	Planning & Direction
Mission Analysis	Analysis & Production	Collection
Course of Action (COA) Development	Investigations	Processing & Exploitation
COA Analysis & Wargaming	Operations	Analysis & Production
COA Comparison		Dissemination & Integration
COA Approval	Functional Services	*- All steps are centered around a mission, and tied to evaluation and feedback*
Plan or Order Development		

* As derived from Joint Publication 3-0
** As derived from Joint Publication 2-0
*** As derived from Joint Publication 2-01

The range of CI possibilities (*See Table 4*) with an agent deployment can span from standing up a bare base to supporting an enduring base in contested environments. Agents can be inserted into any environment to conduct a threat assessment and evaluate physical air base defense, cyber concerns, and vulnerabilities to aircraft. Vulnerabilities to the supply chain and suspicious activities ITW are also relevant, yet generally fall to military intelligence teams due to OSI force constraints. Due to COIN doctrine as touched on earlier, OSI agents can creatively apply CI collections to friendly force operational patrols, build target packages for host nation military and law enforcement service, and conduct information sharing with host nation intelligence and security officials to build comprehensive targeting data. The data can then be acted on using organic ISR capabilities to shape a commander's desired end state. What has not yet been extensively developed is a method to thwart adversary action from a hybrid of multi-domain environments or the newly formalized physical space domain.

Table 4: OSI Examples via the Joint Planning Process

CI Nuances per Joint Planning Process	
CI is*	**OSI can**
Offensive: Adversary penetration and deception	Use 9Q specialists or cyber specialists, but not standard/non-specialized OSI agent
Defensive: Protection of vital US national security related information from being obtained or manipulated by an adversary's intelligence organizations, activities, and operations	Conduct FP; supply chain risk mitigation; execute CI investigations; counter technical and cyber threats; conduct CI operations
* As derived from JP 2-0	

The 2019 Space Threat Assessment from the Center for Strategic and International Studies outlines early on the immense threat to the US via its lack of security for satellites and control of the domain.[109] Although deploying special agents into outer space in the immediate future is unlikely, OSI still has the opportunity to shape risk mitigation and operational plans which affect DAF interests and assets. Many of the nations highlighted as threats in the NDS are also "developing, testing, and fielding a range of counterspace weapons that threaten to deprive [the US] of the many economic and military advantages we derive from space,[110]" per Jim Cooper of the US House of Representatives. OSI should consider its restructure and dual support to USSF to consider immediately embedding agents and specialized support staff to the USSF Headquarters, like its placement of subject matter experts throughout the Joint Staff, Air Staff, and key interagency and partner agencies. The core functions of OSI CI may continue to evolve with advancements in technical expertise and personnel experience.

Evolution of forces is underway for DAF as well. Former SECAF Heather Wilson along with Gen Goldfein instituted the Air Force Warfighting Integration Capability (AFWIC), meant to capitalize on a wide berth of experience and ingenuity within the DAF to develop future force

tangible solutions.[111] OSI can readily insert its capabilities within any level of the AFWIC to assist with understanding the adversary and the operational domain first, so the solutions can be relevant and timely. Collective reflections from earlier cited Rand studies posit that the USAF has historically achieved greater resource and finance allocations than sister services due to their advanced technological capabilities and convincing anecdotes of air superiority to win wars. The space domain's leadership simply need the best potential force capable of flexibly addressing threats. AFWIC proposes using the five military services and their respective domains as a joint force tool[112] (*See Table 5*). While OSI has some expeditionary ISR capabilities, the true input is its blend of agents, analysts, defenders, and support personnel shaping a battlespace using CI activities. These can be incorporated into the AFWIC multi-domain command and control function[113] which will take intelligence and affect strategic and operational planning and missions. Like space integration, OSI should also embed agents and subject matter experts into the AFWIC planning teams and organizational structure. The opportunity with AFWIC to insert OSI into the emerging operations construct is critical to counterbalance emerging unknowns because DAF senior leaders should have every operational advantage through an understanding of vulnerabilities and enemy capabilities to shape their decisions.

Table 5: OSI Integration to the AFWIC Operating Construct

AFWIC Emerging Operational Concept*		
Service	**Domains**	**OSI Involvement**
Air Force	Air, Cyber	CI Awareness Briefings, Information/Product Sharing, Operations/Missions, Onsite SMEs
Space Force	Space, Cyber	
Navy	Sea, Cyber	Liaison, Information/Product Sharing, Combined Operations/Missions
Marine Corps	Sea, Land, Air, Cyber	
Army	Land, Air, Cyber	
* As derived from AFWIC Emerging Concept Graphic		

Conclusion

OSI is a DAF decision-maker's most robust defense in understanding evolving threats to their respective operational environment. OSI shapes and protects US national security interests, and as an agency is prepared to advocate best practices for future service chief decisions. Despite myriad threats the DAF will continue to face, CI is a vital aspect of warfighting. Actions to ensure DAF future wars planning, policy, and operational efforts hold CI considerations at the forefront of their efforts are critical as near peer threats continue to evolve and threaten U.S. national interests. The OSI should continue to highlight its relevancy for asset and technology protection within the senior levels of the DAF and continue to strategically invest subject matter experts at key staff billets. OSI's historic relevance and its outlined force design efforts bolster DAF preparedness for a multi-domain future fight. Continued relationship cultivation and incorporation of CI activities into planning and deployment schemas – regardless of impacted domains – need to be advertised and repeated. OSI must codify its place in the joint planning process and ensure it expands best practices as a vital counterbalance to increasing near peer threat competition. Globally, OSI's combination of its premier personnel along with resources, capabilities, and skills shape DAF defense and is repeatable to address new enemies and domains. OSI's CI authorities and especially its CI support to FP activities provide more operational latitude than what traditional DAF intelligence and law enforcement entities can provide, and OSI can supplement traditional DAF intelligence community gaps in CI training and experience. OSI can help illuminate the obscurity of future war, affect any multi-domain conflict, and enhance DAF commander desired end states. Creativity and courage are means to bolster the DAF against future adversaries, and OSI is a CI-capable force poised to support DAF commanders in future war triumph.

Acronyms

AEF	Air and Space Expeditionary Force
AFI	Air Force Instruction
AFWIC	Air Force Warfighting Integration Capability
AST	Antiterrorism Specialty Team
AT	Antiterrorism
BG	Brigadier General
CAOC	Combined Air and Space Operations Center
CI	Counterintelligence
CID	Criminal Investigation Command
CITP	Criminal Investigator Training Program
COA	Course of Action
COIN	Counterinsurgency
CR	Contingency Response
CSAF	Chief of Staff of the Air Force
DAF	Department of the Air Force
DOD	Department of Defense
DON	Department of the Navy
EO	Executive Order
FLETC	Federal Law Enforcement Training Centers
FP	Force Protection
FY	Fiscal Year
HUMINT	Human Intelligence
IC	Intelligence Community
ICC	International Criminal Court
ICON	Investigations, Collections, and Operations Nexus
IIR	Intelligence Information Report
ISR	Intelligence, Surveillance, and Reconnaissance
ITW	Inside the Wire
JFACC	Joint Force Air Component Commander
JP	Joint Publication
JPP	Joint Planning Process
LOE	Lines of Effort
MCIO	Military Criminal Investigation Organization
NCIS	Naval Criminal Investigative Service
NDS	National Defense Strategy
NSA	Non-State Actor
OSI	Office of Special Investigations
OTW	Outside the Wire
SECAF	Secretary of the Air Force
SME	Subject Matter Expert
USAF	US Air Force
USG	US Government
USMC	US Marine Corps
USSF	US Space Forces

Endnotes

[1]Office of Special Investigations, “In Remembrance of Fallen OSI Heroes,” Fallen Agents, accessed March 7, 2020,

https://www.osi.af.mil/About/Fallen-Agents/.
[2] Terry L. Bullard, "Our Command's Future, The AFOSI We Need," News Commentaries, November 21, 2019, https://www.osi.af.mil/News/Commentaries/Display/Article/2023439/our-commands-future-the-afosi-we-need/.
[3] US Department of Defense, "Our Story," *Defense.gov*, accessed March 7, 2020, https://www.defense.gov/Our-Story/.
[4] US Department of Defense, "Our Priorities," *Defense.gov*, accessed March 7, 2020, https://www.defense.gov/Our-Story/.
[5] The White House, *Summary of the 2018 National Defense Strategy of the United States of America (*Washington, DC, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[6] *United States Air Force Posture Statement: Fiscal Year 2021 President's Budget Request: Hearing before the US Senate Armed Services Committee*, 116th Cong., 2 (March 3, 2020) (statement of The Honorable Barbara Barrett, Secretary of the Air Force and General David L. Goldfein, Chief of Staff, United States Air Force).
[7] Secretary of the Air Force Public Affairs, "The Air Force We Need: 386 operational squadrons," September 17, 2018, https://www.af.mil/News/Article-Display/Article/1635070/the-air-force-we-need-386-operational-squadrons/.
[8] Valerie Insinna, "US Air Force's top officer talks about the budget and why he won't drop the 386-squadron goal," *Defense News.com*, February 24, 2020, https://www.defensenews.com/digital-show-dailies/air-warfare-symposium/2020/02/24/us-air-forces-top-officer-talks-about-the-budget-and-why-he-wont-drop-the-386-squadron-goal/.
[9] Annex 3-10, "Threats to the Air Force Mission," Force Protection, last modified November 19, 2019, 17, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-10/3-10-D07-FORCE-Threats.pdf.
[10] Annex 3-10, Force Protection, 17.
[11] *The National Security Act of 1947*, 88th Cong., Public Law 253, ch. 343 (July 26, 1947), S. 758, 5, https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf.
[12] Office of Special Investigations, "Fact Sheet," About OSI, last modified August 4, 2017, https://www.osi.af.mil/About/Fact-Sheets/Display/Article/349945/air-force-office-of-special-investigations/.
[13] S. Rebecca Zimmerman, Kimberly Jackson, et.al., *Movement and Maneuver: Culture and the Competition for Influence Among the US Military Services*, xv, (Santa Monica, Ca: Rand Study, 2019), https://www.rand.org/pubs/research_reports/RR2270.html.
[14] Zimmerman and Jackson, Movement and Maneuver, xix.
[15] US Department of Defense. *Joint Security Operations in Theater*, JP 3-10 (Washington, DC: Department of Defense, July 25, 2019), III-10, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_10.pdf?ver=2019-07-31-083752-333.
[16] Zimmerman and Jackson, Movement and Maneuver, xix.
[17] OSI, Fact Sheets, 1.
[18] Department of Homeland Security, "Federal Law Enforcement Training Centers Partner Spotlight: The Air Force Office of Special Investigations," last modified March 4, 2019, https://www.fletc.gov/press-release/2019/03/04/air-force-office-special-investigations.
[19] DHS, FLETC Spotlight: OSI, 1.
[20] US Air Force, "Fact Sheet," Security Forces – 3P0X1, last modified September 1, 2006, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104599/security-forces-3p0x1/.
[21] US Air Force, "Careers Detail," Enlisted Operations Intelligence, accessed March 7, 2020, https://www.airforce.com/careers/detail/operations-intelligence.
[22] David H. Berger, *Force Design 2030*, Commandant of USMC Vision for the Future, March 2020, 7, https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460.
[23] Bullard, Our Command's Future: OSI We Need, 1.
[24] OSI, Fact Sheets, 1.
[25] *United States Air Force Posture Statement: FY21 Budget Request*, 116th Cong., 2, SECAF and CSAF.
[26] Bullard, email to the OSI Command, February 20, 2020.
[27] Bullard, telephone conversation with the author, April 21, 2020.
[28] John E. Hyten, "Space Mission Force: Developing Space Warfighters for Tomorrow," (white paper, US Air Force Space Command, 2016), 3, also available online at: https://www.afspc.af.mil/Portals/3/documents/White%20Paper%20-%20Space%20Mission%20Force/AFSPC%20SMF%20White%20Paper%20-%20FINAL%20-%20AFSPC%20CC%20Approved%20on%20June%2029.pdf?ver=2016-07-19-095254-887.
[29] Hyten, Space Mission Force: Developing Space Warfighters for Tomorrow, 3.

[30] US Air Force Space Command, "Quote: General Jay Raymond, Commander, Air Force Space Command," Air Force Space Command Home, https://www.afspc.af.mil/.
[31] Miranda Priebe, Alan J. Vick, et. al. *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, (Santa Monica, Ca: Rand Study, 2019), 99, https://www.rand.org/pubs/research_reports/RR2959.html.
[32] The White House, NDS, 1.
[33] The White House, NDS, 5.
[34] *United States Air Force Posture Statement: FY21 Budget Request*, 116th Cong., 2, SECAF and CSAF.
[35] Secretary of the Air Force Barbara Barrett (@SecAFOfficial), "Our priorities can be summed up simply. We need a modern, smart, connected, and strong @usairforce and @SpaceForceDoD to deter and defend against aggression and to preserve precious freedom and peace. We have that in the United States Department of the Air Force today," Twitter post, February 27, 2020, 14:48, https://twitter.com/SecAFOfficial/status/1233116822322532353
[36] Barrett, Department of Air Force Priorities, 14:48.
[37] Bullard, Our Command's Future: OSI We Need, 3.
[38] Bullard, Our Command's Future: OSI We Need, 3.
[39] Bullard, Our Command's Future: OSI We Need, 1.
[40] Air University Press, ed. Shannon W. Caudill, "Dissipating the Fog of War: Improving Intelligence Support to Air Base Defense," in *Defending Air Bases in an Age of Insurgency*, vol. 2. (Maxwell AFB: Air University Press, March 2019), 335, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0154_Caudill_Defending_Air_Bases_In_An_Age_Of_Insurgency_Vol_II.pdf.
[41] Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases*, (Santa Monica, Ca: Rand Study, 1995), https://www.rand.org/pubs/monograph_reports/MR553.html.
[42] US Department of Defense, *Counterintelligence*, Air Force Instruction 71-101 v4, July 2, 2019, 5, https://fas.org/irp/doddir/usaf/afi71-101v4.pdf.
[43] US President, Executive Order, "United States Intelligence Activities, Executive Order 12333," *Executive Orders*, 12333, December 4, 1981, https://www.intelligence.senate.gov/sites/default/files/laws/amended12333.pdf.
[44] DOD, EO 12333, 1.
[45] US Department of Defense. *Joint Air Operations*, JP 3-30 (Washington, DC: Department of Defense, July 25, 2019), x, https://fas.org/irp/doddir/dod/jp3_30.pdf
[46] Vick, Snakes in the Eagle's Nest, 108.
[47] Christine E. Williamson, "The Air Force Office of Special Investigations: Postured for the Future." *Air and Space Power Journal* XIX, no. 2 (Summer 2005), 23.
[48] DOD, AFI 71-101v4, 5.
[49] DOD, AFI 71-101v4, 5.
[50] Vick, Snakes in the Eagle's Nest, 108.
[51] Justin R. Harber, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors," *International Journal of Intelligence and Counterintelligence* 22, no.2, (2009), 228, https://www.tandfonline.com/doi/full/10.1080/08850600802698200.
[52] Harber, Unconventional Spies: The CI Threat from NSAs, 228.
[53] Vick, Snakes in the Eagle's Nest, 109-110.
[54] Vick, Snakes in the Eagle's Nest, 64.
[55] DOD, AFI 71-101v4, 15-24.
[56] David A. Deptula, "Air Force Transformation: Past, Present, and Future," *Aerospace Power Journal* 15, no. 3 (Fall 2001), 87, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-15_Issue-1-4/Fall2001.pdf.
[57] Williamson, OSI: Postured for the Future, 26.
[58] Deptula, Air Force Transformation, 87.
[59] Deborah Kidwell, "Steadfast Values Through the Years, AFOSI 2019 Fact Book," *Global Reliance* 45, no. 2 (Summer 2019), 6.
[60] Kidwell, Steadfast Values Through the Years, 6.
[61] Williamson, OSI: Postured for the Future, 26.
[62] Antiterrorism Specialty Team (AST) and Special Missions Branch (SMB) labels have been interchangeable over time, with the same intent of providing USAF commanders a rapid mobility entity.
[63] Williamson, OSI: Postured for the Future, 24.
[64] Williamson, OSI: Postured for the Future, 24.
[65] Williamson, OSI: Postured for the Future, 24.

[66] Williamson, OSI: Postured for the Future, 25.
[67] The White House, *The National Security Strategy of the United States of America*, (Washington, DC, 2017), 33, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.
[68] David L. Goldfein, "How is the Air Force Adapting to Great Power Competition?" War on the Rocks, podcast audio transcript, June 5, 2019, 1-18, https://warontherocks.com/2019/06/wotr-podcast-how-is-the-air-force-adapting-to-great-power-competition/.
[69] Goldfein, How USAF is Adapting to Great Power Competition, 8.
[70] Steven Carmical, email message to author, March 17, 2020.
[71] Adam Taylor, "Air Force Shifts Middle East Command Center from Qatar to South Carolina," Washington Post, September 29, 2019, https://www.stripes.com/news/air-force/air-force-shifts-middle-east-command-center-from-qatar-to-south-carolina-1.601074.
[72] Taylor, Air Force Shifts Middle East Command Center, 2.
[73] Taylor, Air Force Shifts Middle East Command Center, 5.
[74] Charles Pope, "Goldfein Details Air Force's Move Toward a 'Fully Networked,' Multi-Domain Future," Secretary of the Air Force Public Affairs, September 17, 2019, 2, https://www.af.mil/News/Article-Display/Article/1963310/goldfein-details-air-forces-move-toward-a-fully-networked-multi-domain-future/.
[75] DOD, AFI 71-101v4, 5.
[76] Williamson, AFOSI: Postured for the Future, 28.
[77] Williamson, AFOSI: Postured for the Future, 24.
[78] Air Force Office of Special Investigations, "AFOSI ICON Center Informs, Engages, Enhances Globally, AFOSI 2019 Fact Book," *Global Reliance* 45, no. 2 (Summer 2019), 8, https://www.osi.af.mil/Portals/29/2019%20Fact%20Book%20PDF.pdf?ver=2019-10-04-145748-687.
[79] OSI, ICON Center, 8.
[80] OSI, ICON Center, 8.
[81] AFOSI, AFOSI 2019 Fact Book, 24.
[82] Bullard, The AFOSI We Need, 1.
[83] US Department of Defense, *Counterinsurgency*, JP 3-24 (Washington, DC: Department of Defense, April 24, 2018), III-5, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_24.pdf.
[84] Ganesh Sitaraman, "Counterinsurgency, the War on Terror, and the Laws of War," *Virginia Law Review* 95 (2009), 1776, https://www.virginialawreview.org/volumes/content/counterinsurgency-war-terror-and-laws-war.
[85] Michael Neiberg, "Predicting War," Lawfare blog, June 19, 2018, https://www.lawfareblog.com/predicting-war.
[86] Neiberg, Predicting War, 5.
[87] Brien Alkire, Abbie Tingstad, et. al. *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, (Santa Monica, Ca: Rand Study, 2016), 28, https://www.rand.org/pubs/research_reports/RR1330.html.
[88] Alkire and Tingstad, Future of AF Intelligence Analysis, 28.
[89] Alkire and Tingstad, Future of AF Intelligence Analysis, 28.
[90] Marygail K. Brauner, Hugh G. Massey, et. al. *Improving Development and Utilization of US Air Force Intelligence Officers*, (Santa Monica, Ca: Rand Study, 2009), 35, https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR628.pdf.
[91] Priebe and Vick, Distributed Operations in Contested Environment, 97.
[92] Priebe and Vick, Distributed Operations in Contested Environment, 97.
[93] Priebe and Vick, Distributed Operations in Contested Environment, 97.
[94] Jeffrey T. Richelson, *The US Intelligence Community* (New York, NY: Taylor and Francis, 2018), 2, https://www.taylorfrancis.com/books/9780429494321.
[95] Daniel Irwin and David Mandel, Improving Information Evaluation for Intelligence Products, (2019) *Intelligence and National Security*, Vol. 34, No. 4, 503, https://www.tandfonline.com/doi/abs/10.1080/02684527.2019.1569343.
[96] Irwin and Mandel, Improving Information Evaluation for Intelligence Products, 517.
[97] Orde F. Kittrie, *Lawfare: Law as a Weapon of War* (New York: Oxford Press, 2016), 2.
[98] Orde F. Kittrie, "Lawfare and US National Security," *Case Western Reserve Journal of International Law* 43 (2011), 396, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1779562##.
[99] Kittrie, Lawfare and US National Security, 397.
[100] Peter E. Harrell, "Could the US Sanction the International Criminal Court?" *Lawfare blog*, March 9, 2020, https://www.lawfareblog.com/could-us-sanction-international-criminal-court.
[101] Harrell, Could the US Sanction the ICC, 1.
[102] Kittrie, Law as a Weapon of War, 33.
[103] Kittrie, Law as a Weapon of War, 35.

[104] Kittrie, Law as a Weapon of War, 35.
[105] US Air Force Doctrine, *Appendix C: Air Mobility Support and Contingency Response Elements,* Annex 3-17 Air Mobility Operations, (June 28, 2019), 85, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-17/3-17-D42-Appendix-3-Response.pdf.
[106] DOD, JP-3-0, II-5.
[107] DOD, JP-3-0, II-5.
[108] DOD, JP-3-0, III-12.
[109] Todd Harrison, Kaitlyn Johnson, et.al., "Space Threat Assessment 2019," *A Report of The CSIS Aerospace Security Project* (April 2019), https://aerospace.csis.org/space-threat-assessment-2019/.
[110] Harrison and Johnson, et.al., 2019 Space Threat Assessment, IV.
[111] Air Force Warfighting Integration Capability, "About Us," accessed March 7, 2020, https://www.afwic.af.mil/About-Us/.
[112] Air Force Warfighting Integration Capability, "Emerging Concept," last modified August 29, 2019, https://www.afwic.af.mil/Portals/72/Images/Emerging_Concept_Image_large.png?ver=2019-08-29-123628-143
[113] AFWIC, Emerging Concept, 1.

Bibliography

Alkire, Brien, Abbie Tingstad, et. al. *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*. Santa Monica, Ca: Rand Study, 2016, https://www.rand.org/pubs/research_reports/RR1330.html.

Air Force Office of Special Investigations. "AFOSI 2019 Fact Book." *Global Reliance* 45, no. 2 (Summer 2019), 3-8.

Air University Press, ed. Shannon W. Caudill. "Dissipating the Fog of War: Improving Intelligence Support to Air Base Defense." In *Defending Air Bases in an Age of Insurgency*, vol. 2, 251-264. Maxwell AFB: Air University Press, March 2019.

https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0154_Caudill_Defending_Air_Bases_In_An_Age_Of_Insurgency_Vol_II.pdf.

Berger, David H. *Force Design 2030*. Commandant of USMC Vision for the Future, March 2020, https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460.

Brauner, Marygail K., Hugh G. Massey, et. al. *Improving Development and Utilization of US Air Force Intelligence Officers*. Santa Monica, Ca: Rand Study, 2009, https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR628.pdf.

Deptula, David A. "Air Force Transformation: Past, Present, and Future," *Aerospace Power Journal* 15, no. 3 (Fall 2001), 87.

Harber, Justin R. "Unconventional Spies: The Counterintelligence Threat from Non-State Actors," *International Journal of Intelligence and Counterintelligence*, 22, no.2, (2009), 221-236, https://www.tandfonline.com/doi/full/10.1080/08850600802698200.

Harrison, Todd and Kaitlyn Johnson, et.al. "Space Threat Assessment 2019." *A Report of The CSIS Aerospace Security Project* (April 2019). https://aerospace.csis.org/space-threat-assessment-2019/.

Hyten, John E. "Space Mission Force: Developing Space Warfighters for Tomorrow." White Paper, US Air Force Space Command, June 29, 2016. Available online at: https://www.afspc.af.mil/Portals/3/documents/White%20Paper%20-%20Space%20Mission%20Force/AFSPC%20SMF%20White%20Paper%20-%20FINAL%20-%20AFSPC%20CC%20Approved%20on%20June%2029.pdf?ver=2016-07-19-095254-887.

Irwin, Daniel and David Mandel. "Improving Information Evaluation for Intelligence Products." (2019), *Intelligence and National Security* 34, no. 4 (2019), 503-525, https://www.tandfonline.com/doi/abs/10.1080/02684527.2019.1569343.

Kidwell, Deborah. "Steadfast Values Through the Years." *Global Reliance* 45, no. 2 (Summer 2019), 6.

Kittrie, Orde F. *Lawfare: Law as a Weapon of War*. New York: Oxford Press, 2016.

Kittrie, Orde F. "Lawfare and US National Security." *Case Western Reserve Journal of International Law* 43, (2011), 393-421, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1779562##.

Priebe, Miranda, Alan J. Vick, et. al. *Distributed Operations in a Contested Environment:*

Implications for USAF Force Presentation. Santa Monica, Ca: Rand, 2019, https://www.rand.org/pubs/research_reports/RR2959.html.

Richelson, Jeffrey T. *The US Intelligence Community.* Reprint of the 2016 New York edition, 2018. https://www.taylorfrancis.com/books/9780429494321.

Sitaraman Ganesh. "Counterinsurgency, the War on Terror, and the Laws of War." *Virginia Law Review* 95 (2009), https://www.virginialawreview.org/volumes/content/counterinsurgency-war-terror-and-laws-war.

The White House. *The National Security Strategy of the United States of America*. Washington, DC, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

The White House. *Summary of the 2018 National Defense Strategy of the United States of America.* Washington, DC, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

US Air Force Doctrine. *Annex 3-10, Force Protection.* November 19, 2019. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-10/3-10-D07-FORCE-Threats.pdf.

US Air Force Doctrine. *Appendix C: Air Mobility Support and Contingency Response Elements*. Annex 3-17 Air Mobility Operations, June 28, 2019. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-17/3-17-D42-Appendix-3-Response.pdf.

US Congress. House. *The National Security Act of 1947.* 88th Cong., Public Law 253, ch. 343 (July 26, 1947), S. 758. https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf

US Department of Defense. *Counterintelligence*. Air Force Instruction 71-101 v4, July 2, 2019. https://fas.org/irp/doddir/usaf/afi71-101v4.pdf.

US Department of Defense. Joint Intelligence. JP 2-0. Washington, DC: Department of Defense, October 22, 2013, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.

US Department of Defense. Joint and National Intelligence Support to Military Operations. JP 2-01. Washington, DC: Department of Defense, July 5, 2017, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_01_20170705v2.pdf.

US Department of Defense. Joint Operations. JP 3-0. Washington, DC: Department of Defense, October 22, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

US Department of Defense. Joint Security Operations in Theater. JP 3-10. Washington, DC: Department of Defense, July 25, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_10.pdf?ver=2019-07-31-083752-333.

US Department of Defense. Counterinsurgency. JP 3-24. Washington, DC: Department of Defense, April 25, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_24.pdf.

US Department of Defense. Joint Air Operations. JP 3-30. Washington, DC: Department of Defense, July 25, 2019, https://fas.org/irp/doddir/dod/jp3_30.pdf.

US President, Executive Order. "United States Intelligence Activities, Executive Order 12333." *Executive Orders*, 12333 (December 4, 1981). https://www.intelligence.senate.gov/sites/default/files/laws/amended12333.pdf.

Vick Alan. *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases.* Santa Monica, Ca: Rand, 1995), https://www.rand.org/pubs/monograph_reports/MR553.html.

Wayne Amann. "New Strat Plan 'gets back to LE roots.'" *Global Reliance* 45, no. 1 (Spring 2019), 3-4, 28.

Williamson, Christine E. "The Air Force Office of Special Investigations: Postured for the Future." *Air and Space Power Journal* XIX, no. 2 (Summer 2005), 23-28.

Zimmerman, S. Rebecca, Kimberly Jackson, et.al. *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services*. Santa Monica, Ca: Rand, 2019, https://www.rand.org/pubs/research_reports/RR2270.html