

Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition

June 4, 2020

Congressional Research Service

<https://crsreports.congress.gov>

R46389



R46389

June 4, 2020

John R. Hoehn,
Coordinator
Analyst in Military
Capabilities and Programs

Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition

The U.S. military could suffer unacceptably high casualties and struggle to win, or perhaps lose, a war against China or Russia. This implication by the National Defense Strategy Commission stands in contrast to the past several decades during which the U.S. possessed military power without equal. Great power competition has returned, marked by Chinese and Russian malign activities occurring below the threshold of armed conflict, an area of competition called the grey zone, while they simultaneously advance warfighting capabilities with increased lethality, range, and speed. The result is the potentially significant erosion of the military advantage possessed by the United States.

A key capability to ensure the U.S. military maintains its dominance is in its intelligence, surveillance, and reconnaissance (ISR) assets. The House and Senate Armed Services Committees have both taken an increasing interest in U.S. military ISR capabilities vis-à-vis China and Russia. The House has emphasized in particular the importance of joint airborne ISR capabilities and established a Future of Defense Task Force to review and assess U.S. defense capabilities to meet emerging threats. The Senate has stressed command and control and both legacy and future ISR systems that can provide tactical forces with targeting data needed to perform their mission within a highly contested environment. Most recently, the House and Senate Armed Services Committees each drafted legislation calling for appropriations to enhance military modernization, to include funding for ISR, in the Indo-Pacific region.

Senior military leaders at the Pentagon are also rethinking modernization priorities to meet the demands of the National Defense Strategy (NDS), and are aiming to build a more lethal force given concerns that China and Russia may surpass the United States in military capability. ISR is one of their modernization priorities. More specifically, the Department of Defense (DOD) aims to connect ISR sensors across all warfighting domains (space, air, land, sea, and cyber) directly with commanders and weapon systems, sharing data at an accelerated speed. This will enable U.S. and allied forces to outthink, outpace, and outmaneuver its adversaries. Congress may consider whether the DOD-wide modernization programs and budget requests for developing advanced sensing capabilities and connecting those sensors to shooters, match the strategies identified in the National Security Strategy (NSS) and NDS.

The current DOD ISR enterprise does not yet possess the readiness to effectively support operations in the grey zone or support combat operations in a highly contested environment, according to senior DOD ISR leaders. To meet the demands of the new global strategic environment, the DOD ISR enterprise intends to shift from a manpower-intensive force optimized for operations within a permissive environment to an automation-intensive force capable of defeating a peer adversary within a highly contested environment. To achieve operational success within a high threat environment, the Services have indicated they would like to invest in resilient and collaborative ISR capabilities that enhance situational awareness, aid rapid decisionmaking, and reliably find, fix, and target elusive targets deep within enemy territory. The objective is to generate an information advantage for U.S. military forces, which is paramount to effective operations both in the grey zone and highly contested environments.

To achieve an information advantage, each military service has highlighted a number of initiatives unique to their specific primary missions and in support of creating an all-domain sensing and sense-making capability. In other words, the aim of the future DOD ISR enterprise is to gain access to data from multiple domains (space, air, land, sea, and cyber); make rapid sense of that data; securely deliver that data to weapons, weapon systems, and commanders; and possess a workforce that can execute its mission in competition and combat, at a pace greater than the enemy. However, each service faces significant challenges with harnessing the exponential growth in data to realize the potential of disruptive technology and shaping the future workforce to employ these warfighting capabilities.

This report offers Congress a conceptual framework for understanding unclassified DOD ISR modernization initiatives for great power competition. Congressional interests include funding levels, strategy, plans, and programs relative to military ISR investments for the new global strategic environment as defined in the NSS and NDS. Congress's decisions on these issues could have significant implications on the U.S. military's competitive advantage versus China and Russia and its ability to compete, deter, and win in this environment.

Contents

Introduction: Evolution into Great Power Competition	1
What Is Intelligence, Surveillance, and Reconnaissance (ISR)?	1
ISR Roles and Responsibilities	3
Intelligence in Military Operations	4
Scoping the Challenge.....	5
Grey Zone	6
Highly Contested Environment.....	7
Rethinking Military Modernization Priorities	8
Connecting Sensors to Shooters.....	9
Joint All Domain Operations (JADO).....	9
Joint All Domain Command and Control.....	10
Congressional Actions on ISR.....	11
ISR Design for Great Power Competition.....	13
Air Force	14
Next Generation ISR Dominance Flight Plan.....	14
ISR Rebalance.....	14
Future Capability Investments	15
Collaborative Sensing Grid.....	17
Air Force Distributed Common Ground System	17
Information Warfare.....	18
Other Views	18
Space Force	19
Space Situational Awareness.....	19
Ballistic Missile Warning System	20
Army	20
ISR Task Force.....	21
Space.....	22
Multi-Domain Sensor System.....	22
Terrestrial Layer System	23
Tactical Intelligence Targeting Access Node	23
Distributed Common Ground System—Army	23
Science and Technology Focus	24
Other Views	24
Navy	25
Information Warfare.....	25
Airborne Platforms.....	25
Surface Vessels.....	25
Data Fusion Technology	26
Human Capital	27
Other Views	27
Marine Corps.....	28
Expeditionary Advanced Base Operations.....	28
Marine Corps ISR Enterprise.....	28
Airborne Platforms.....	29
Surface Vessels.....	29
Data Fusion Technology	29

Information Warfare.....	30
Operationalizing ISR for Great Power Competition	30
Data	30
DOD Data Strategy	31
Challenges with Data Formats	31
Keeping Pace with Data.....	32
Disruptive Technology	33
Human-Machine Teaming.....	34
Cloud Technology	35
Human Capital	35
Shaping the Future ISR Force.....	35
Partnering with Industry and Academia.....	36
Issues for Congress.....	36

Figures

Figure 1. Array of Multi-domain ISR Capabilities.....	3
Figure 2. Joint Intelligence Process	4
Figure 3. China Anti-Access/Area Denial Defensive Layers	8
Figure 4. Joint All Domain Command and Control.....	11
Figure 5. Air Force ISR Rebalance	15
Figure 6. Army Cross-Functional Teams.....	21
Figure 7. Maritime Security and Operational Environment	27
Figure 8. How Much Data Is Generated Every Minute?	33

Contacts

Author Information.....	37
-------------------------	----

Introduction: Evolution into Great Power Competition

The terror attacks on September 11, 2001, followed nearly a decade without major conflict and pushed the U.S. military into counter-terror (CT) and counterinsurgency (COIN) operations aimed at defeating enemies in Afghanistan, Iraq, and other austere locations. However, the 2017 National Security Strategy (NSS) and the 2018 National Defense Strategy (NDS) note that the global strategic environment has changed, and that it is now characterized primarily by competition between the United States and an ascending China, as well as a reemerging Russia. Importantly, this competition is marked by Chinese and Russian malign activities occurring below the threshold of armed conflict while they and other competitors have simultaneously fielded warfighting capabilities with increased lethality, range, and speed. This combination of actions and capabilities, according to the National Defense Strategy Commission, has significantly eroded the military advantage possessed by the United States since the end of World War II in the Pacific and the fall of the Soviet Union in 1991.¹ An operationally important capability associated with this advantage has been U.S. intelligence, surveillance, and reconnaissance (ISR) assets.

What Is Intelligence, Surveillance, and Reconnaissance (ISR)?

“The world is not getting any safer, and espionage remains our first line of defense.”
General Michael V. Hayden²

ISR is a military operation intended to help “decision makers anticipate change, mitigate risk, and shape outcomes.”³ The U.S. Department of Defense (DOD) defines ISR as “an integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations.”⁴ It is at the intersection between military planning, operations, and assessment where intelligence is the product of surveillance and reconnaissance operations.

¹ National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, 2018, December 12, 2019, at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>. The commission was created pursuant to the National Defense Authorization Act of 2017 to examine and make recommendations with respect to the national defense strategy of the United States. More specifically, the commission was charged with formally reviewing the National Defense Strategy (NDS) released by the Department of Defense (DOD) in January 2018, as well as assessing and offering its views on the broad range of issues that informed that strategy. The commission was tasked with reporting its findings to the President, Secretary of Defense, Committee on Armed Services of the House of Representatives, and Committee on Armed Services of the Senate.

² Hayden, Michael V., *Playing to the Edge*, Penguin Books, February 23, 2016.

³ Brown, Jason, *Strategy for Intelligence, Surveillance, and Reconnaissance*, Air University Press, 2014.

⁴ DOD Dictionary of Military and Associated Terms, at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.

Intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.⁵

Surveillance. The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means.⁶

Reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.⁷

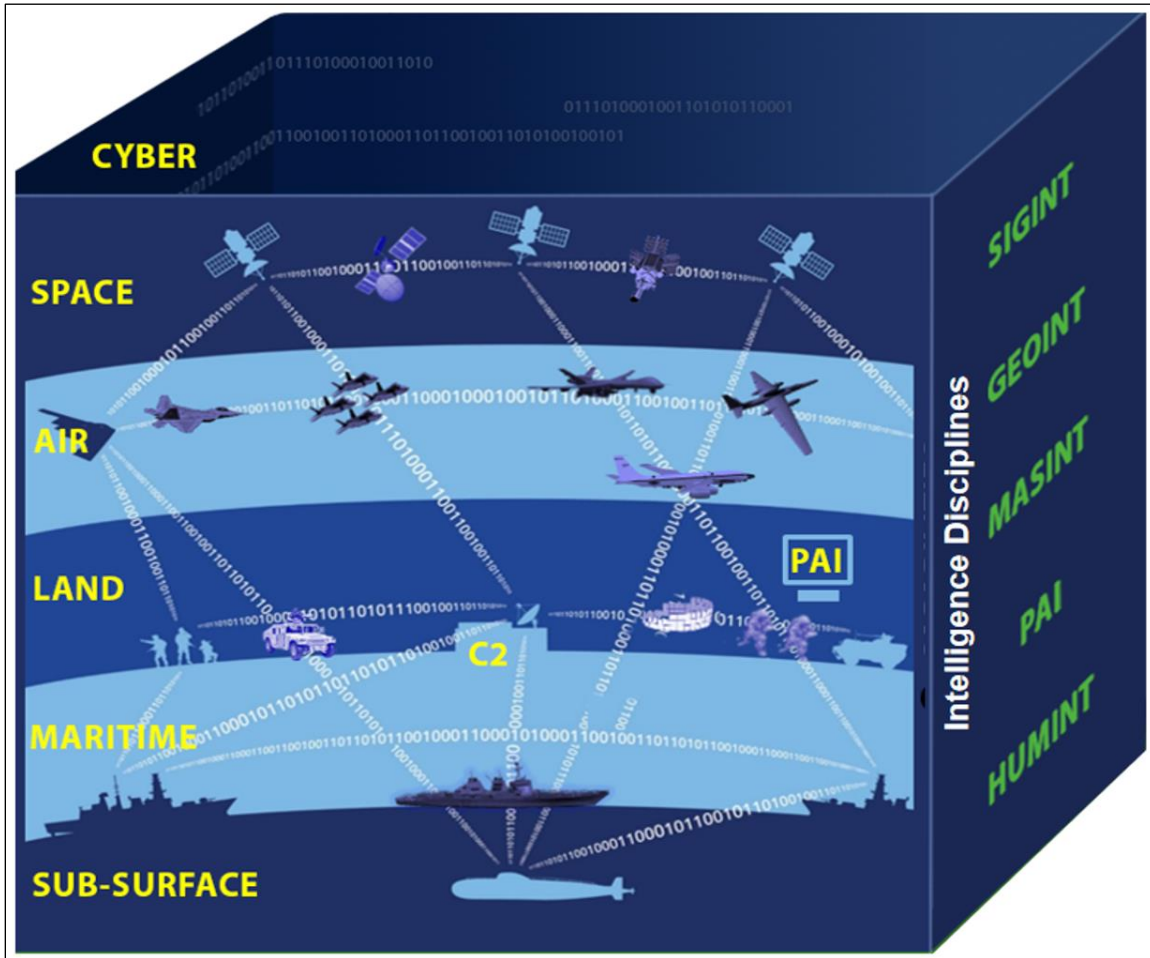
ISR does not imply that the U.S. military senses all activity within a given battlespace. It involves using a wide-array of platforms, sensors, and analytic capacity to create an awareness of adversary capabilities, dispositions, and likely intentions. This awareness, resulting from analysis, is then used by commanders to exercise Command and Control (C2) and decide appropriate measures to utilize available military capabilities.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

Figure I. Array of Multi-domain ISR Capabilities
Data Network, Platforms, Sensors, and Operators



Source: U.S. Air Force.

Notes: A wide variety of platforms (satellites, aircraft, ships, humans, etc.) and sensors (imagery, communications, acoustics, etc.) collect, analyze, and share data, information, and intelligence across multiple warfighting domains. The focus of ISR is on answering a commander's information needs, such as identifying and locating adversary activity and intentions within a given battlespace. Specific intelligence disciplines include but are not limited to Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Measurement and Signatures Intelligence (MASINT), Publicly Available Information (PAI), and Human Intelligence (HUMINT).

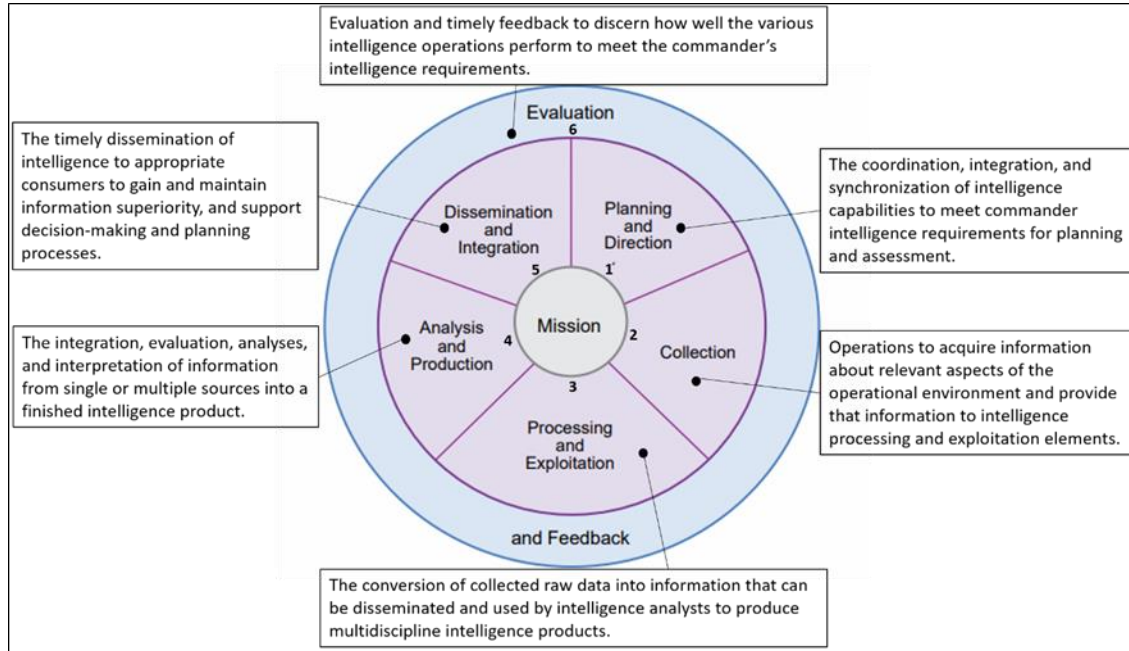
ISR Roles and Responsibilities

According to joint military doctrine, the primary role of intelligence is to provide information and assessments to facilitate mission accomplishment.⁸ For instance, targeting an adversary's long-range missiles is, of course, much easier when U.S. military commanders know where the missiles are. ISR aims to inform commanders to enable decisionmaking, support military planning by anticipating adversary actions and defining the operational environment, warn friendly forces of threats, support deceptive techniques and counter adversary deception, identify

⁸ Joint Chiefs of Staff, Joint Publication 2-0 Joint Intelligence, October 22, 2013.

adversary vulnerabilities, hold targets at risk of being attacked, and assess combat effectiveness.⁹ These roles and responsibilities are accomplished through a detailed joint intelligence process that facilitates an understanding of the wide variety of intelligence operations and their interrelationships.

Figure 2. Joint Intelligence Process



Source: CRS Adaptation from Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, July 5, 2017.

Intelligence in Military Operations

The most important role of intelligence in military operations is to provide commanders with analysis of key aspects of the operational environment to assist them in their decisionmaking process. Using a wide variety of capabilities ranging from above the earth's atmosphere to below the surface of the ocean, ISR sensors collect data on a given area of operations or battlespace in support of a commander's information needs. Such needs may include the location of adversary forces, their warfighting capability, and their intentions. The *collected data* resulting from multiple sources are then analyzed, largely by human operators with support from artificial intelligence, and transformed into *information*. This information creates a narrative on observed activity within the battlespace. Analysts then derive meaning from information, resulting in *intelligence* and generating a picture of adversary activity that answers the commander's information needs and ultimately drives decisionmaking. Furthermore, during the execution of real-time combat operations and in accordance with the direction provided by a commanding officer, ISR provides both targeting data for weapon systems to engage enemy forces and threat data to protect forces.

The following is a simplified, hypothetical example of how ISR operations are conducted in support of a commander's objectives. In order to gain control of the airspace within an operational environment (air superiority), a commander determines the operational objective to

⁹ Ibid.

find, fix, and target enemy air defense systems. Via mission analysis, analysts determine that an adversary mobile air defense system remains un-located, posing a direct threat to aircraft and their achieving air superiority. ISR operators at Command and Control (C2) centers synchronize available intelligence capabilities, assigning collection tasks to appropriate platforms and sensors while also tasking analytic nodes to rapidly make sense of collected data and generate intelligence in support of the commander's requirement to identify and locate the missing air defense system. Platform operators and analysts then collaboratively plan how best to accomplish the commander's intent. The operation begins, and an array of ISR assets, either operating in a single domain or multiple domains, work together to find and fix the missing air defense system. A SIGINT sensor collects data on the air defense system, finding the general location where it is located. Confirming the data, an analyst then shares that data with the C2 center and other ISR sensors, queuing a full-motion video (FMV) sensor to image the location. Within the FMV field of view, imagery analysts fix the air defense system, noting its specific geographic location. Armed with confirmation of the identity and location of the air defense system, the C2 center tasks a strike aircraft to target the air defense system. A strike is conducted, and additional ISR assets are tasked to conduct a damage assessment, confirming that the air defense system no longer poses a threat to achieving air superiority.

This process, largely operating at human-speed, can occur simultaneously or sequentially, taking from several minutes to days to accomplish. The U.S. military's goal for the future is to conduct this process at machine speed, an accelerated pace achieved by employing artificial intelligence and cloud computing. At machine speed, this process can be conducted in seconds to single digit minutes, enabling U.S. and allied forces to outthink, outpace, and outmaneuver its adversary on the battlefield.

Scoping the Challenge

The 2017 NSS stated that China and Russia both seek to assert their influence across the globe with the intent to undermine and supplant American leadership by cleverly operating below the threshold of armed conflict, an area of global competition former Chairman of the Joint Chiefs of Staff, General Joseph Dunford, identified as the grey zone.¹⁰ Recognizing that U.S. national security interests had evolved from terrorism to strategic competition, the 2018 NDS focused DOD's strategy to compete with and deter U.S. great power adversaries by remaining prepared to decisively win a war.¹¹ In support of both grey zone competition and combat operations within a highly contested environment, the challenge for the DOD ISR enterprise is twofold. The first challenge is to develop and field capabilities that can endure a degradation in mission capacity yet remain operational, facilitating collaboration among multiple platforms, sensors, and disruptive technologies. Second, the ISR enterprise must overcome challenges in collecting, analyzing, and sharing an exponential growth in data at machine speed.

¹⁰ General Joseph Dunford, Chairman of the Joint Chiefs of Staff, in testimony before the U.S. Congress, Senate Committee on Armed Services, The Fiscal Year 2020 National Defense Authorization Budget Request from the Department of Defense, 116th Cong., 1st sess., March 14, 2019.

¹¹ Department of Defense, "Summary of the 2018 National Defense Strategy of The United States of America; Sharpening the American Military's Competitive Edge," at <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Grey Zone

Then-Chairman Dunford testified that China and Russia innovatively use the grey zone—the competitive space that resides between peace and war—to pursue strategic gains without provoking a conventional conflict and therefore mitigating the United States’ competitive military advantage.¹² For example, China’s broad lineup of actions include military intimidation, paramilitary activities, information operations, industrial and academic espionage, and economic coercion.¹³ Russia is also an active participant in the grey zone, responsible for employing “military intimidation, weaponization of social media, information and cyber warfare ... and funding proxy groups and political organizations hostile to Western institutions.”¹⁴ General Dunford also surmised that the collective sum of peer adversary actions in the grey zone undermine U.S. alliances and partnerships and the health and stability of democracies, while imposing gradual, and potentially irrevocable, losses on the U.S. strategic position around the globe.¹⁵

Military ISR serves a significant role in supporting grey zone operations. An array of spy satellites, surveillance aircraft and ships, and ground-based collection and analysis centers provide early warning to deny an adversary the opportunity to conduct a surprise strategic attack against the U.S. and its allies, or to confirm incidents involving adversary military intimidation or paramilitary activities. For example, the Chinese Navy shadows and harasses neighbor-state fishing vessels operating in international waters, and Russia has deployed paramilitary units to Libya in support of forces opposing the internationally recognized Libyan government.¹⁶ It also supports readiness via war plan development conducted by U.S. combatant commands and informs development and acquisition of future weapon systems intended to ensure continued U.S. military competitive advantages. Military ISR also complements national intelligence gained by the U.S. Intelligence Community in support of national level policy. Fulfilling these missions helps ensure the U.S. possesses an information advantage over an opposing force and helps strengthen military alliances and partnerships via intelligence sharing and therefore generating transparency and shared awareness on malign adversary actions.

However, grey zone operations may be an area that the U.S. military finds itself ill-prepared to compete effectively in as it attempts to transform stove-piped ISR operations, challenged with

¹² General Dunford, in testimony before the U.S. Congress, Senate Committee on Armed Services, March 14, 2019, described the grey zone as possessing five distinct characteristics: “political influence, economic coercion, use of cyber, information operations, and then military posture.” General Dunford continued, declaring that within the military strategy the “competition in the grey zone is really for our partners,” where the adversary seeks “to undermine the credibility of our alliances and partnerships,” and therefore it is “critical for us to overcome in the information space, overcome in cyber capabilities, and then our military posture the erosion of that relationship we have with our allies.”

¹³ Morris, Lyle J., Mazzar, Michael J., Hornung, Jeffrey W., Pezard, Stephanie, Binnendijk, Anika, Kepe, Marta, “Gaining Competitive Advantage in the Gray Zone,” *RAND Corporation*, 2019, at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf.

¹⁴ Ibid.

¹⁵ General Joseph Dunford, Chairman of the Joint Chiefs of Staff, in testimony before the U.S. Congress, Senate Committee on Armed Services, The Fiscal Year 2020 National Defense Authorization Budget Request from the Department of Defense, 116th Cong., 1st sess., March 14, 2019.

¹⁶ Grady, John, “DOD Official: U.S. Committed to Countering Chinese Military Intimidation in South East Asia,” *USNI News*, August 7, 2018, at <https://news.usni.org/2018/08/07/dod-official-u-s-committed-countering-chinese-military-intimidation-south-east-asia> and Department of Defense, “Russia Deploys Military Fighter Aircraft to Libya,” *U.S. Africa Command*, May 26, 2020, at <https://www.africom.mil/pressrelease/32887/russia-deploys-military-fighter-aircraft-to-l>.

geographic and cyber access to monitor adversary actions and intent, into day-to-day military power projection intended to deter adversaries from pursuing strategic gains.¹⁷ Stove-piped ISR operations generate challenges in both data sharing and creating a comprehensive picture of the operating environment. These challenges are further exacerbated in the grey zone, which is wrought with “deception and misinformation,” as adversary “military and paramilitary measures” are combined with economic statecraft, political warfare, information operations, and other tools. Countering the utilization of these tools is an especially difficult problem in that such use often occurs in the “seams” between DOD and other U.S. departments and agencies, making them all the more difficult to address.¹⁸

Highly Contested Environment

While the NSS and NDS point to a multidimensional great power competition instead of the singular challenge of military conflict with China and Russia, senior DOD ISR leaders have noted that potential military conflicts with either state would significantly challenge the U.S. military’s ISR capabilities.¹⁹ This is because the highly contested environment is defined by sophisticated anti-access/area denial (A2/AD) capabilities, with extended range, increased speed, and enhanced targeting precision. Potential adversary capabilities are designed to create a nonpermissive environment, deny the U.S. military freedom of movement, and mitigate the effectiveness of U.S. combat power within an armed conflict. Both China and Russia have fielded advanced warfighting capabilities to include mobile ballistic missiles, mobile air and coastal defense weapon systems, cyber, stealth aircraft, remotely piloted aircraft, advanced ISR and electronic warfare capabilities; they are also pursuing emerging technologies such as hypersonics, autonomous systems, and artificial intelligence.²⁰ These weapon systems and capabilities may significantly impair the current U.S. ISR enterprise by forcibly denying platforms and sensors both geographic and virtual access to adversary activity and data.

Numerous challenges exist for ISR to successfully operate within a highly contested environment. For example, networks, platforms, sensors, and military personnel must be able to penetrate adversary defenses, collect data, analyze that data and recognize threats and targets, and ultimately share that data with decisionmakers, other sensors, and weapons, at machine-speed.²¹ An inability to collect, analyze, and share data at a speed greater than our adversary will degrade

¹⁷ Pomerleau, Mark, “What the New 16th Air Force Means for Information Warfare,” *C4ISRNet*, October 13, 2019, at <https://www.c4isrnet.com/dod/air-force/2019/10/14/what-the-new-16th-air-force-means-for-information-warfare/>. Within this context, stove-piped intelligence includes collection and analysis of data through a single intelligence discipline (e.g., signals intelligence, geospatial intelligence, human intelligence), and not effectively integrated with other intelligence disciplines, therefore limiting comprehensive and shared situational awareness of the battlespace across the joint force.

¹⁸ National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission*, 2018, December 12, 2019, at <https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf>.

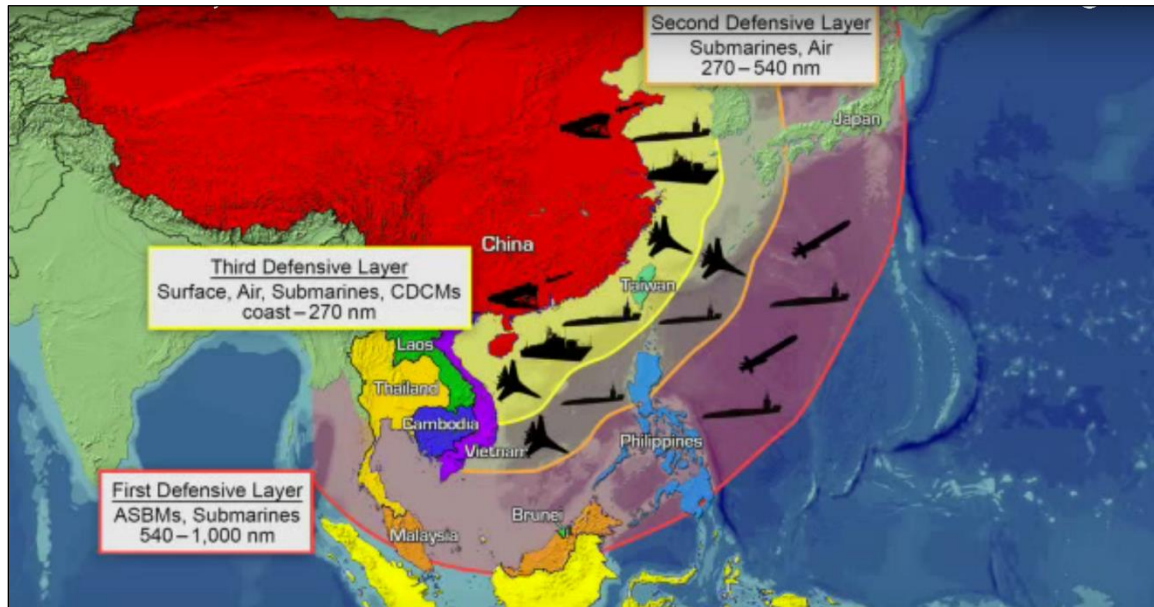
¹⁹ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-I8dt2gL9A>.

²⁰ Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, January 3, 2019, at <http://www.dia.mil/Military-Power-Publications>, and Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, 2017, at <http://www.dia.mil/Military-Power-Publications>.

²¹ Humans are limited in the speed at which they can process large amounts of data and information in a reasonable time. Automating capabilities, via artificial intelligence, machine learning, and computing power, speeds processing rates far faster than human capabilities. This processing speed is identified as “machine-speed.”

battlespace awareness and command and control (decisionmaking), and will have a negative impact to ensuring U.S. and allied forces have the freedom to attack and the freedom from attack.

Figure 3. China Anti-Access/Area Denial Defensive Layers



Source: LaGrone, Sam, CNO Richardson: Navy Shelving A2/AD Acronym, *USNI News*, October 3, 2016, <https://news.usni.org/2016/10/03/cno-richardson-navy-shelving-a2ad-acronym>.

Notes: Office of Naval Intelligence image. China's anti-access area denial defensive layers consists of multiple capabilities to include, but not limited to, anti-ship ballistic missiles (ASBM), submarines, surface-to-surface missiles, surface-to-air missiles, coastal defense cruise missiles (CDCM), and fighter and bomber aircraft. Operating within this highly contested environment presents a significant challenge for U.S. and allied military forces. Specific challenges for ISR include collecting target-quality data via penetrating and persistent ISR operations, rapidly making sense of that data, and transmitting that data to a commander, weapon, or weapon system to complete the find, fix, target kill chain, at machine speed, of adversary threat systems.

Rethinking Military Modernization Priorities

A number of senior U.S. military leaders are rethinking modernization priorities with an aim to build a more lethal force given concerns that China and Russia may surpass the United States in military capability. One such investment priority is C4ISR.

Investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.²²

Concepts such as Joint All Domain Operations (JADO) and Joint All Domain Command and Control (JADC2) are at the forefront of DOD pursuits to fulfill this priority. Realizing the potential of each concept (i.e., connecting sensors to shooters in real-time) depends upon innovative technological advancements and the development of appropriate joint doctrine and

²² Department of Defense, Summary of the 2018 National Defense Strategy of The United States of America; Sharpening the American Military's Competitive Edge, undated but released January 2018, at <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

operational concepts. The question is whether the DOD-wide modernization programs and budget requests for connecting ISR sensors to shooters match the strategies identified in the NSS and NDS.

Connecting Sensors to Shooters

The U.S. military contends that future conflicts within a sophisticated, highly-contested, A2/AD environment will be won by the side with an information advantage, enabling the ability to outpace, outthink, and outmaneuver adversaries across multiple domains (space, air, land, sea, and cyber).²³ To maintain its information advantage and dominate this new battlefield, the U.S. military is reportedly adopting a network-centric approach (connecting every sensor with every shooter) so that it can move data at machine speed and overwhelm an adversary by attacking from all domains.²⁴ However, the emphasis is placed on the ability to find and fix a target, not necessarily finish the target, according to the Chief of Staff of the Air Force (CSAF), who stated “it doesn’t matter as much what mechanism is used to destroy a target as it is to be able to rapidly locate and characterize it.”²⁵

Joint All Domain Operations (JADO)

ISR is likely to play a central role in new approaches to commanding and communicating in military operations. Initially called Multi Domain Operations and subsequently renamed JADO, senior military officers and defense experts have described this concept as the “new American way of war,” potentially providing the U.S. a significant military advantage “over everybody in the world for a long time.”²⁶ JADO is defined as “operations conducted across multiple domains and contested spaces to overcome an adversary’s (or enemy’s) strengths by presenting them with several operational and/or tactical dilemmas through the combined application” of combat power.²⁷ It describes how the U.S. military can counter and defeat a near-peer adversary capable of contesting the United States in all domains by converging capabilities (space, cyber, nuclear deterrence, transportation, electromagnetic spectrum, missile defense, etc.) across domains, environments, and functions in time and space.²⁸ JADO intends to provide commanders access to an abundance of data, information, and intelligence to support the integration of warfighting

²³ Saltzman, Chance Brig Gen, USAF, *MDC2 Overview*, 2018 C2 Summit, at <https://www.mitre.org/sites/default/files/publications/Special-Presentation-Gen%20Chance-Saltzman%20MDC2%20Overview%20for%20MITRE-June-2018.pdf>.

²⁴ Honorable Heather Wilson and General David Goldfein, Secretary of the Air Force and Chief of Staff of the Air Force, in testimony before the U.S. Congress, Senate Committee on Armed Services, Posture of the Department of the Air Force, 116th Cong., 1st sess., April 4, 2019.

²⁵ Tirpak, John A., “Goldfein says 2021 Budget Buys Connectivity by Accepting Capacity Risk,” *Air Force Magazine*, January 27, 2020, at <https://www.airforcemag.com/goldfein-says-2021-budget-buys-connectivity-by-accepting-capacity-risk/>.

²⁶ Clark, Colin, Gen Hyten on the New American Way of War: All Domain Operations, *Breaking Defense*, February 18, 2020, at <https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/>.

²⁷ U.S. Army, *The U.S. Army in Multi Domain Operations 2028*, December 6, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

²⁸ Ibid. Clark, Colin, Gen Hyten on the New American Way of War: All Domain Operations, *Breaking Defense*, February 18, 2020, at <https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/>.

capabilities across all domains in order to gain physical and psychological advantages, control, and influence over the operational environment.²⁹

Joint All Domain Command and Control

The increased speed and reach of war combined with an exponential growth in data has led the CSAF to advocate for an enhanced command and control (C2) system that will focus on situational awareness, rapid decisionmaking, and the ability to direct forces across all domains.³⁰ In addition, Secretary of Defense Esper recently voiced his support for an advanced C2 system, and Representative Banks of the House Armed Services Committee Future of Defense Task Force highlighted the need for a “sensing, intelligent and distributed command and control environment” to ensure U.S. military forces overmatch any potential adversary.³¹

In addition to FY2020 appropriations of \$100.8 million for JADC2 RDT&E, the CSAF singled out a FY2021 budget request of \$435 million to begin developing architecture and connectivity that “we need to be able to not only connect the Air Force, but to connect the joint force.”³² The Joint Requirements Oversight Council, responsible for achieving consensus across the services regarding acquisition priorities, appointed the Air Force as the lead service for JADC2 technological testing.³³ Recent testing suggests the Air Force intends to pursue the Advanced Battle Management System (ABMS) as a joint architecture foundation for JADC2.

The initial test explored new methods for Air Force and Navy aircraft (F-22, F-35), a Navy destroyer, and Army air defense radar systems plus a mobile artillery system to share data and provide a fuller picture of the operating environment for a C2 element in Florida. According to U.S. military officials, the C2 cell “watched real-time data pour in, and out of, the command cell. They observed information from platforms and people flowing instantly and simultaneously across air, land, sea, and space that provided shared situational awareness updates as events occurred whether the information originated from jets, or passing satellites, or from sea and ground forces on the move.”³⁴

²⁹ Ibid.

³⁰ U.S. Air Force, *CSAF Letter to Airmen*, March 10, 2017, at <https://www.af.mil/News/Article-Display/Article/1108931/csaf-letter-to-airmen/>. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, defines C2 as “The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.”

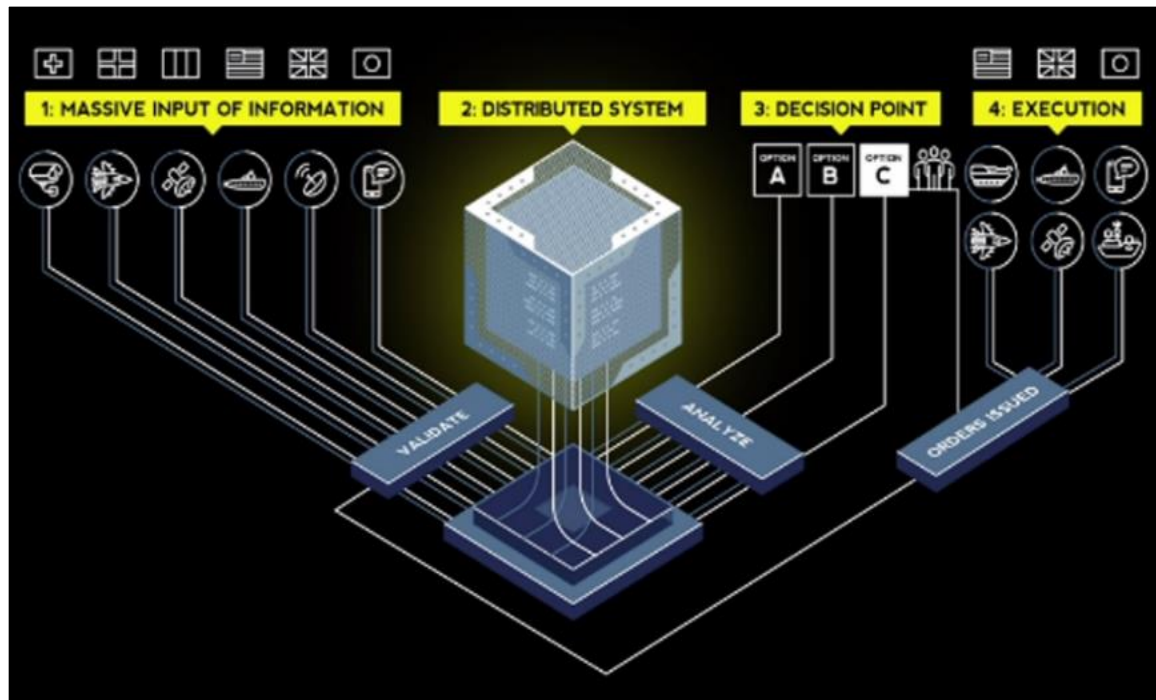
³¹ Mehta, Aaron, Mark Esper on the ‘Big Pivot Point’ That Will Define the 2022 Budget,” *Breaking Defense*, February 10, 2020, at <https://www.defensenews.com/smr/federal-budget/2020/02/10/mark-esper-on-the-big-pivot-point-that-will-define-the-2022-budget/>, and Future of Defense Task Force Hearing: Theories of Victory, October 29, 2019, at <https://armedservices.house.gov/2019/10/future-of-defense-task-force-hearing-theories-of-victory>.

³² Department of Defense, Fiscal Year 2020 Department of Defense Appropriations Act, P.L. 116-93; Department of the Air Force, *FY 2021 Budget Overview*, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/SUPPORT_FY21%20Budget%20Overview_1.pdf?ver=2020-02-10-152806-743; and Naegele, Tobias, “Here’s how USAF Aims to Spend \$30 billion in Legacy Savings,” *Air Force Magazine*, at November 6, 2019, <https://www.airforcemag.com/heres-how-usaf-aims-to-spend-30-billion-in-legacy-savings-2/>.

³³ Hitchens, Theresa, “OSD & Joint Staff Grapple with Joint All Domain Command,” *Breaking Defense*, November 14, 2019, at <https://breakingdefense.com/2019/11/osd-joint-staff-grapple-with-joint-all-domain-command/>.

³⁴ Ibid.

Figure 4. Joint All Domain Command and Control



Source: 2019, Air, Space, and Cyber Conference.

Some analysts take a more skeptical approach to JADC2. They raise questions about technological capabilities and unrealistic ambition of fielding a network that can securely and reliably connect sensors to shooters and support C2 in a lethal, electronic warfare-rich environment.³⁵ Others question who would have decisionmaking authority across domains in JADO and question the human role in making JADC2 decisions in real time.³⁶

Moreover, not all services are convinced ABMS is a scalable solution to connect the entire joint force. Army leaders believe that “ABMS cannot be the sole solution, because it doesn’t account for, in some cases, the scale or the unique requirements of all the other services.”³⁷

Congressional Actions on ISR

Congress has taken an increasing interest in U.S. military capabilities vis-à-vis China and Russia.

The House Armed Services Committee (HASC), in its FY2020 National Defense Authorization Act Committee Report, highlighted both the importance of airborne ISR capabilities in supporting

³⁵ Shattuck, A.J., “The Pipe Dream of (Effective) Multi-Domain Battle,” *Modern War Institute*, March 28, 2017, at <https://mwi.usma.edu/pipe-dream-effective-multi-domain-battle/>.

³⁶ Spears, Will, “A Sailors Take on Multi Domain Operations,” *War on the Rocks*, May 21, 2019, at <https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/>.

³⁷ Freedberg, Sydney J, Jr., “ABMS Can’t be Sole Solution for Joint C2, Army Tells Air Force – Exclusive,” *Breaking Defense*, January 22, 2020, at <https://breakingdefense.com/2020/01/abms-cant-be-sole-joint-c2-solution-army-tells-air-force-exclusive/>.

U.S. military operations worldwide and a significant shortfall in the services taking an integrated approach to modernizing the ISR enterprise.³⁸

The committee understands that responsive, persistent, and precise collection of operational information from the air will continue to provide an asymmetric and decisive advantage to operational commanders and tactical forces. The committee also recognizes that to meet the objectives described in the National Defense Strategy, the Department of Defense must modernize and adapt its ISR operating concepts and joint force [U.S. military) structure to ensure it can maneuver, fight, and prevail in highly contested environments. However, the committee notes that there is an apparent lack of an integrated joint approach to the Department's ISR modernization strategy.³⁹

Furthermore, the HASC launched a new bipartisan Future of Defense Task Force to examine how to maintain the DOD technological edge against Russia and China.⁴⁰ The new group is chartered to “review U.S. defense assets and capabilities and assess the state of the national security innovation base to meet emerging threats and ensure long-term strategic overmatch of competitors.”⁴¹ The effort, which began in October 2019, explores disruptive technologies like artificial intelligence, biotechnology, fifth-generation telecommunications technology (5G), and hypersonic weapons.⁴² Task force findings are expected to be released in May 2020.

In March 2020, the Senate Armed Services Committee (SASC) received posture statement testimony from senior leaders across each of the services, who delineated their FY2021 investment strategies in support of implementation of the NDS. The committee focused on all domain service initiatives to meet the demands of the NDS and great power competition.⁴³ In consideration of potential cuts to aircraft inventory, Ranking Member Reed specifically stated that “any Air Force proposal deserves our careful consideration, but we must consider it against the recent history of abrupt Air Force changes of direction” on several aircraft programs to include the unmanned RQ-4 Global Hawk and MQ-9 Reaper ISR aircraft.⁴⁴ In addition, some Senators focused their questioning on the continued capability of legacy aircraft, the implementation of the Air Force's Next Generation ISR Dominance Flight Plan, and cuts to

³⁸ U.S. Congress, Report of the Committee on Armed Services Committee House of Representatives on H.R. 2500, June 2019, https://armedservices.house.gov/_cache/files/0/f/0fb5f8dd-a7c9-45bd-a187-c20cc2f66ef5/18AAE9B54DC35E2E04FAFAE121D80E5D.fy20-ndaa-committee-report.pdf.

³⁹ Ibid. The joint force consists of all the U.S. military services and branches: Army, Navy, Air Force, Marine Corps, and Space Force.

⁴⁰ Gould, Joe, “Congressional Task Force to Examine Long Term Defense Strategy for Russia, China,” *Defense News*, October 22, 2019, at <https://www.defensenews.com/congress/2019/10/22/moulton-banks-helm-new-future-of-defense-task-force/>.

⁴¹ Ibid.

⁴² Ibid.

⁴³ U.S. Congress, Opening Statement of U.S. Senator James Inhofe, Chairman, Senate Armed Services Committee, To receive testimony on the posture of the Department of the Army in review of the Defense Authorization Request for Fiscal Year 2021, March 26, 2020, at https://www.armed-services.senate.gov/imo/media/doc/Inhofe_03-26-20.pdf, and Opening Statement of U.S. Senator Jack Reed, Ranking Member, Senate Armed Services Committee, To receive testimony on the posture of the Department of the Army in review of the Defense Authorization Request for Fiscal Year 2021, March 26, 2020, at https://www.armed-services.senate.gov/imo/media/doc/Reed_03-26-20.pdf.

⁴⁴ U.S. Congress, Stenographic Transcript Before the Committee on Armed Services, *Hearing to Receive Testimony on Posture of The Navy in Review of the Defense Authorization Request for Fiscal Year 2021 and the Future Years Defense Program*, United States Senate, March 4, 2020, https://www.armed-services.senate.gov/imo/media/doc/20-07_03-03-2020.pdf, and Stenographic Transcript Before the Committee on Armed Services, *Hearing to Receive Testimony on Posture of The Air Force in Review of the Defense Authorization Request for Fiscal Year 2021 and the Future Years Defense Program*, United States Senate, March 3, 2020, https://www.armed-services.senate.gov/imo/media/doc/20-07_03-03-2020.pdf.

unmanned ISR programs across the services. They also focused on the need to ensure that command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR) systems can provide tactical forces with targeting data needed to perform their mission within a highly contested environment.⁴⁵

Moreover, in April 2020, Representative Mac Thornberry, ranking member of the HASC, released a discussion draft chartering an Indo-Pacific Deterrence Initiative, calling for \$6.09 billion in FY2021 to be spent in the Indo-Pacific region on a number of defense capabilities to include ISR programs.⁴⁶ The draft legislation called for \$378.6 million to “enhance indications and warning, sensor packages, the development of future intelligence, surveillance and reconnaissance platforms, and interoperable processing, exploitation, and dissemination architectures for the United States Indo-Pacific Command.”⁴⁷ The aim of this effort is to “enhance U.S. deterrence of China, similar to what the European Deterrence Initiative has done for Europe against Russia.”⁴⁸ Similarly, SASC member Senator Tom Cotton proposed the Forging Operational Resistance to Chinese Expansion (FORCE) Act.⁴⁹ The proposal calls for providing the DOD an additional \$6.1 billion to “regain the advantage in the Indo-Pacific” and \$9.2 billion to support military modernization for great power competition.⁵⁰

ISR Design for Great Power Competition

At the Military Service Intelligence Priorities Panel of the 2019 Intelligence & National Security Alliance Summit, Army, Air Force, and Navy intelligence leaders discussed the comprehensive challenges facing military intelligence in the new global strategic environment. They concluded that the current DOD ISR enterprise and associated operational concepts are not yet postured to contend with great power competition.⁵¹ The ISR enterprise’s focus on CT and COIN since

⁴⁵ Ibid. Senator Hawley specifically asked General David H. Berger, USMC Commandant, “From an ISR and C2 standpoint, what would you say, General, are the most important programs for ensuring that Marine Corps fire units have the targeting data they need to perform the sea denial mission?” The General responded, “I do not care where I get my fire data solution from or what ISR platform. I just need the data.”

⁴⁶ U.S. Congress, House Armed Services Committee Republicans, *Fact Sheet: Thornberry Indo-Pacific Deterrence Initiative*, at <https://republicans-armedservices.house.gov/sites/republicans.armedservices.house.gov/files/IPDI%20Fact%20Sheet%20.pdf>.

⁴⁷ U.S. Congress, House Committee on Armed Services, *Indo-Pacific Deterrence Initiative Draft Discussion*, 116th Cong., 2nd sess., April 15, 2020, at <https://republicans-armedservices.house.gov/sites/republicans.armedservices.house.gov/files/IPDI%20Legislation.pdf>.

⁴⁸ U.S. Congress, House Armed Services Committee Republicans, *Fact Sheet: Thornberry Indo-Pacific Deterrence Initiative*, at <https://republicans-armedservices.house.gov/sites/republicans.armedservices.house.gov/files/IPDI%20Fact%20Sheet%20.pdf>.

⁴⁹ U.S. Congress, Cotton FORCE Act Surges \$43 Billion to Thwart Chinese Military Aspirations in Indo-Pacific, at https://www.cotton.senate.gov/files/documents/Package%20IV%20Summary_FINAL.pdf.

⁵⁰ Ibid. According to Sen. Cotton’s proposal, the \$6.1 billion to regain the advantage in the Indo-Pacific is intended to fund joint force lethality, force design and posture, strengthen allies and partners, exercises, experimentation, and innovation, and logistics and security enablers. The \$9.2 billion intends to support naval lethality, air superiority, ground overmatch, and missile defense, and advanced technology. Although the draft bill does not specifically address intelligence, surveillance, and reconnaissance (ISR), focus areas that intend to regain an advantage in the Indo-Pacific and increase military capabilities for great power competition could also support ISR modernization. The summary of the bill text is available at https://www.cotton.senate.gov/files/documents/Package%20IV%20Summary_FINAL.pdf.

⁵¹ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-18dt2gL9A>. According to <https://www.insaonline.org/about>, INSA is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. The INSA Military Service Priorities panelists discussed the importance of collaboration across military branches in order to have

September 11, 2001, has generated an ISR capability and process designed for operations in a permissive environment, where the U.S. military controlled the timing and tempo of operations at relatively minimal risk. Given adversary advancements in mobile A2/AD weapon systems, the U.S. military now aims to develop and field a resilient ISR enterprise that can execute digital-age intelligence operations at machine speed.

The primary aim shared by the service intelligence chiefs is to shift from a manpower-intensive, permissive environment force to an automation-intensive, high-threat environment force that is cost-effective, can reliably find and fix elusive targets, and can enable an interoperable U.S. military to gain and maintain the information advantage across the grey zone and highly contested environments.⁵² Common themes across the services describing the future DOD ISR enterprise are joint all-domain operations, an overwhelming abundance of data, disruptive technology, and human capital. However, each service faces significant challenges with harnessing data to realize the potential of disruptive technology and shaping the future workforce to employ these warfighting capabilities.

Air Force

Next Generation ISR Dominance Flight Plan

In 2018, the Secretary of the Air Force and the CSAF approved the Next Generation ISR Dominance Flight Plan 2018-2028. This document acknowledged that the current Air Force ISR enterprise was not positioned to meet the full intent of the NDS, and that potential adversaries' development of advanced threat capabilities highlights seams and gaps of past ISR investments, which were focused on CT and COIN operations.⁵³ The ISR Dominance Flight Plan reorients the Air Force ISR enterprise from a manpower-intensive capability designed for Cold War and CT/COIN operations, toward an enterprise operating at machine speed within a potentially high-threat environment.

The full aim of the ISR Dominance Flight Plan is to meet NDS intent by increasing the role of emerging and disruptive technology and analytic expertise in the development of new ISR capabilities. The Air Force contends that it will achieve this through two major efforts: (1) generating a balanced ISR enterprise designed to operate within the grey zone and highly contested environments, and (2) deploying new tools and trained airmen resulting in increased readiness and lethality.⁵⁴

ISR Rebalance

The Air Force Deputy Chief of Staff for ISR and Cyber Effects Operations teamed with the Air Force Studies, Analyses, and Assessments directorate and two federally funded research and development centers to generate an ISR rebalance review. The review intended to provide recommendations aimed at transforming the current CT/COIN focused enterprise toward a set of capabilities consisting of updated, legacy-manned aircraft and new classified platforms and sensors able to operate successfully against U.S. great power competitors.⁵⁵ An initial assessment

the most effective integration of emerging technologies and innovative warfare.

⁵² Ibid.

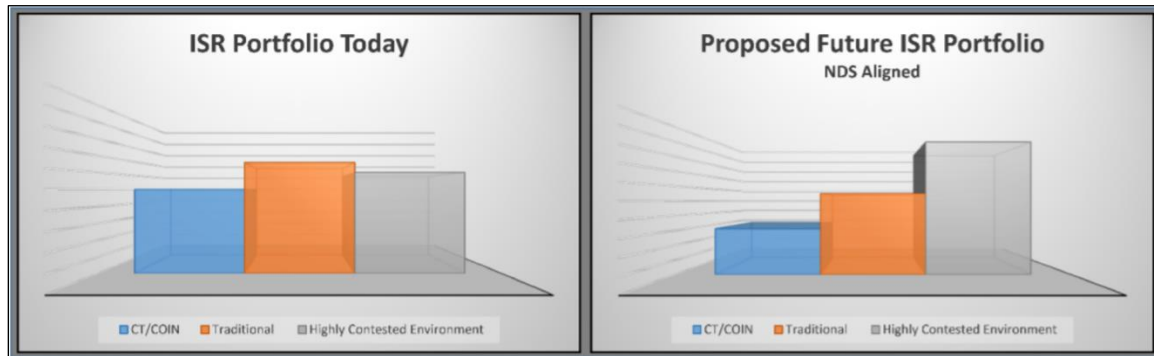
⁵³ U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

⁵⁴ Ibid.

⁵⁵ Based on author discussions with Kenneth Bray, Headquarters Air Force, ISR and Cyber Effects Operations, Acting

was concluded in 2018, with focus on geospatial intelligence capabilities; an additional assessment consisting of broader options is currently underway.⁵⁶

Figure 5. Air Force ISR Rebalance



Source: U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

Notes: To position the Air Force ISR enterprise to generate an information advantage, the ISR Dominance Flight Plan outlines Air Force resources for future investments. The ISR Rebalance Review aims to realign specific investments in CT/COIN capabilities toward assets more appropriate for operations within the grey zone and combat operations within a highly contested environment.

Future Capability Investments

Future capability investments, called “pathways” by the Air Force, intend to drive change and increase readiness and lethality via 10 unique initiatives. The first pathway, *Disruptive Technologies/Opportunities*, is highlighted by three initiatives.⁵⁷

- **Machine Intelligence (MI).** MI is about human-machine teaming. The goal of this initiative is to create a system in which intelligence analysts use artificial intelligence/machine learning (AI/ML) to learn new insights, ask new questions, and discover and implement new solutions.⁵⁸
- **Data Strategy.** This effort aims to ensure Air Force ISR data are discoverable, accessible, interoperable with joint data systems, and secure. A data strategy will directly support automation and serves as the foundation for effective MI.⁵⁹
- **Agile Capability Development (ACD).** ACD intends to rapidly develop and field new capabilities and technologies at the precise point in time of need the speed of via prototyping, experimenting, and software development.⁶⁰

In support of this pathway, ISR Modernization and Automation Development was appropriated \$19 million in FY2020, and the Air Force requested an additional \$19.3 million for FY2021, both

Associate Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations, and Chris Moore, Headquarters Air Force, Studies, Analyses and Assessments, Operations Research Analyst, May 29, 2019.

⁵⁶ Ibid.

⁵⁷ U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

⁵⁸ Ibid. The DOD AI Strategy defines AI as “the ability of machines to perform tasks that normally require human intelligence.” Machine learning, a subfield of AI, allows for machines to learn from data.

⁵⁹ Ibid.

⁶⁰ Ibid.

to support RDT&E of algorithmic warfare (AI/ML, deep learning, computer vision) and to automate ISR analyst workflows.⁶¹ This investment will directly tackle the challenge of analysts spending 80% of their time searching for data and 20% making sense of the data.⁶²

In pursuit of the second pathway, *Bolster Lethality & Readiness*, the Air Force states that the service “requires multi-role, cross-domain ISR collection in order to win in the highly contested environment.”⁶³ The Air Force anticipates future investments in “ultra-high/ultra-persistent/ultra-fast air assets (hypersonics, directed energy, long-endurance balloons), penetrating, persistent ISR, space operations, publicly available information, and cyber operations.”⁶⁴ This pathway is highlighted by five initiatives.

1. **High Altitude.** This initiative intends to “migrate away from less capable, traditional ISR systems, and reprioritize” toward survivable and “interoperable capabilities.”⁶⁵
2. **Penetrating, Persistent, and Multi-role Remotely Piloted Aircraft.** This initiative intends to “repurpose and retool traditional ISR capabilities” with disruptive technology that can successfully penetrate adversary airspace, undetected and provide persistent collection on the battlespace.⁶⁶
3. **ISR From/For Space Operations.** This initiative aims to provide “enhanced persistence, resilience, maneuverability, and flexibility” for “future space-based capabilities” to include “U.S. government owned, allied, and commercial space systems.”⁶⁷ It includes generating ISR from the space domain to support joint operations and generating intelligence to support U.S. Space Force operations.
4. **Publicly Available Information (PAI).** With the “global rising use of social media,” PAI is quickly becoming an increasingly important source of battle space information, providing insights into adversary intent, capability, and operational execution.⁶⁸
5. **ISR From/For Cyberspace Operations.** ISR-informed cyber capabilities will support lethal and nonlethal actions.⁶⁹ They include generating ISR from the cyber domain to support joint operations and producing intelligence to support offensive and defensive cyber operations.

⁶¹ U.S. Congress, Fiscal Year 2020 Department of Defense Appropriations Act, P.L. 116-93, and U.S. Air Force, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Air Force, Justification Book Volume 3b of 3, Research, Development, Test & Evaluation, Air Force, Vol-III Part 2, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIb%20-%20updated.pdf?ver=2020-02-12-125427-660.

⁶² U.S. Air Force, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Air Force, Justification Book Volume 3b of 3, Research, Development, Test & Evaluation, Air Force, Vol-III Part 2, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIb%20-%20updated.pdf?ver=2020-02-12-125427-660.

⁶³ U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ Ibid.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Ibid.

To support this pathway, the Air Force FY2021 budget request aims to fund aircraft and sensor upgrades to the unmanned RQ-4 Global Hawk Block 40 wide-area surveillance platform and the manned RC-135 Rivet Joint signals intelligence platform.⁷⁰ The Air Force also plans to eliminate some antiquated ISR assets and operations, and to retire 24 Global Hawk Block 20/30 aircraft and reduce 10 unmanned MQ-9 combat air patrols.⁷¹ Furthermore, the Air Force no longer plans to purchase the MQ-9 beyond FY2020.⁷² This suggests the Air Force may continue to employ the U-2 as its primary high-altitude, multi-intelligence platform, and that it may already have a follow-on, unmanned platform ready to replace the MQ-9 in the coming years.

The final pathway, *Foundational Capabilities*, focuses on workforce development and outreach to industry and academia to drive culture change across the ISR enterprise.⁷³ This pathway is highlighted by two initiatives.

1. **Human Capital.** This initiative focuses on force development and talent management of ISR Airmen with the intent to recruit, develop, and retain a highly capable and competitive workforce.⁷⁴
2. **Partnerships.** This initiative acknowledges that the Air Force must partner with global, commercial, academic, scientific, service, and international partnerships to achieve the ISR Flight Plan vision.⁷⁵

Collaborative Sensing Grid

The Collaborative Sensing Grid is a data-centric network of multidomain platforms, sensors, disruptive technologies, and airmen that are interconnected and working together to provide ISR across an operating environment. Designs for the sensing grid call for a resilient, penetrating, and persistent capability that employs manned and unmanned platforms equipped with disruptive technologies capable of collecting, fusing, and linking commanders to real-time information, plus cueing data from sensors-to-sensors and weapons to support rapid targeting of the adversary.⁷⁶

This initiative is aligned with the Air Force's development of the Advanced Battle Management System, the network intended to support Joint All Domain Command and Control and enable sensor-to-shooter operations.

Air Force Distributed Common Ground System

Given the exponential growth in data, the Air Force is rethinking how it conducts intelligence processing, exploitation, analysis, and dissemination. The primary entity responsible for this mission is the Air Force Distributed Common Ground System (AF DCGS). AF DCGS "employs a global communications architecture that connects multiple intelligence platforms and sensors"

⁷⁰ Department of the Air Force, *FY 2021 Budget Overview*, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/SUPPORT/FY21%20Budget%20Overview_1.pdf?ver=2020-02-10-152806-743.

⁷¹ U.S. Air Force, *The Department of the Air Force FY21 Budget: Air and Space Force Design for Great Power Competition*, undated but released February 2020.

⁷² Cohen, Rachel, S., "Abrupt end to MQ-9 Production Surprise General Atomics," *Air Force Magazine*, February 26, 2020, at <https://www.airforcemag.com/abrupt-end-to-mq-9-production-surprises-general-atomics/>.

⁷³ U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

⁷⁴ Ibid. The term *Airmen* encompasses the entirety of the Air Force workforce to include officers, enlisted and Department of the Air Force civilians.

⁷⁵ Ibid.

⁷⁶ Ibid.

with Airmen charged with generating near-real time intelligence.⁷⁷ The weapon system is undergoing a modernization effort from a closed, proprietary based capability to a government-owned open architecture framework that allows AF DCGS analysts to contend with data growth by capitalizing on AI/ML and cloud computing.⁷⁸ Ongoing modernization aims to speed exploitation via automation and advance human-machine teaming to support analysis. AF DCGS was appropriated \$25 million for RDT&E, \$116 million for procurement in FY2020, totaling \$141 for FY2020.⁷⁹ The Air Force requested an additional \$158.9 million for FY2021 to support development and procurement of its new open architecture network, hardware, and software capabilities in support of ongoing CT/COIN and grey zone operations, and in preparation to deliver intelligence in a highly contested fight.⁸⁰

Information Warfare

To contend with the cognitive challenge from the exponential growth in data presented by the new global strategic environment, the Air Force created its first Information Warfare command organization, known as 16th Air Force (16 AF), Air Forces Cyber.⁸¹ The change is aimed at modernizing the Air Force for a new approach to warfare; one Air Force official described it as shifting from one of attrition to cognition.⁸² The command consolidates a series of capabilities and disciplines, to include ISR wings, cyber wings, a weather wing, and reconnaissance wings encompassing assets like the RQ-4 Global Hawk and U-2 spy plane to provide a more integrated and synchronized information warfare capability.⁸³

Other Views

Some analysts have taken a skeptical view of whether the Air Force is serious about ISR. The service culture arguably “values ISR significantly below fighters and bombers,” although ISR is identified as one of five service core missions.⁸⁴ The other core missions are air and space superiority, rapid global mobility, global strike, and command and control. Analysts are concerned that service leaders will “fall back on an organizational culture and history that does

⁷⁷ U.S. Air Force, *Air Force Distributed Common Ground System*, October 13, 2015, <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/>.

⁷⁸ Brigadier General Gagnon, Gregory and Lt Col Smagh, Nishawn, “How ISR Airmen Can Work Together for Persistent ISR,” *C4ISRNet*, October 8, 2019, at <https://www.c4isrnet.com/opinion/2019/10/08/how-airmen-can-work-together-for-persistent-isr/>.

⁷⁹ Fiscal Year 2020 Department of Defense Appropriations Act, P.L. 116-93.

⁸⁰ U.S. Air Force, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Air Force, Justification Book Volume 3b of 3, Research, Development, Test & Evaluation, Air Force, Vol-III Part 2, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIb%20-%20updated.pdf?ver=2020-02-12-125427-660.

⁸¹ Pomerleau, Mark, “What the New 16th Air Force Means for Information Warfare,” *C4ISRNet*, October 13, 2019, at <https://www.c4isrnet.com/dod/air-force/2019/10/14/what-the-new-16th-air-force-means-for-information-warfare/>.

⁸² Ibid.

⁸³ Ibid. The 557th Weather Wing is the lead Air Force meteorology center. It provides environmental information and awareness in support of the Air Force, Joint Force, combatant commands, and the Intelligence Community.

⁸⁴ Stiegel, Robert, “Is the Air Force Serious About Intelligence, Surveillance, and Reconnaissance?,” *War on the Rocks*, June 25, 2019, at <https://warontherocks.com/2019/06/is-the-air-force-serious-about-intelligence-surveillance-and-reconnaissance/>.

not value the ISR mission or capabilities,” and “divert resources from combat-proven ISR capabilities” to support funding for additional fighter and bomber aircraft.⁸⁵

The Air Force’s vision for a next-generation ISR enterprise depends on disruptive technologies, perhaps even leaps in capability, to enable a smaller pool of airmen to sift through an exponential increase in data while being expected to generate a greater amount of actionable intelligence. One such leap is the application of AI/ML, but the Intelligence Community and DOD are “still awaiting solid results” from AI/ML.⁸⁶ Air Force analysts understand that achieving the lofty vision of a collaborative sensing grid cannot be reached without harnessing the promise of AI/ML and cloud computing technology.

Space Force

The Air Force ISR Dominance Flight Plan was published prior to the establishment of the U.S. Space Force, and therefore incorporated ISR From/For Space Operations within its strategy. This is a significant challenge and area of investment for the U.S. military as China and Russia have both initiated significant investments in their space and counter-space capabilities to mitigate U.S. advantages in the space domain.

Space Situational Awareness

Space Situational Awareness (SSA) is the intelligence driven capability to detect, track, and identify objects in earth orbit. The space domain has become increasingly congested and contested, and to ensure effective SSA, “sensors need access to intelligence” in order to prepare the Space Force to fight and win in the space domain and support operations in other domains.⁸⁷ SSA serves as the foundation for U.S. space control via surveillance of space objects and activities by gathering intelligence on adversary space operations. When paired with sensors and information integration capabilities within the SSA Space Surveillance Network, SSA systems can surveil objects in orbit to provide early warning for satellite attack, space treaty monitoring, and technical intelligence gathering.⁸⁸ SSA is a significant capability improvement as the U.S. military is increasingly dependent upon space for intelligence, position, navigation, and timing capabilities; communications capabilities; and missile warning capabilities. The Space Force requested \$44.8 million for FY2021 to support RDT&E of SSA.⁸⁹

⁸⁵ Ibid.

⁸⁶ Ibid.

⁸⁷ Salinas, Erin, “Space Situational Awareness is Space Battle Management,” Air Force Space Command, May 16, 2018, at <https://www.afspc.af.mil/News/Article-Display/Article/1523196/space-situational-awareness-is-space-battle-management/> and CRS Report R43353, *Threats to U.S. National Security Interests in Space: Orbital Debris Mitigation and Removal*, by Steven A. Hildreth and Allison Arnold.

⁸⁸ U.S. Air Force, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Air Force, Justification Book Volume 1 of 1, Research, Development, Test and Evaluation, Space Force, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=2020-02-11-083608-887.

⁸⁹ Ibid.

Ballistic Missile Warning System

The Space Force requested \$2.3 billion in FY2021 RDT&E funding for the development of a next-generation Overhead Persistent Infrared (OPIR) ballistic missile warning system.⁹⁰ This amount represents nearly an \$800 million increase above FY2020 appropriations.⁹¹ The FY2021 request intends to develop the next generation of survivable space-based missile warning OPIR platforms.⁹² The Space Force contends that this program will deliver improved missile warning capabilities that are more survivable against emerging Chinese and Russian threats.⁹³

Army

According to the Army, JADO intends to provide commanders access to an abundance of data, information, and intelligence to support the integration of warfighting capabilities across all domains in order to gain physical and psychological advantages, control, and influence over the operational environment.⁹⁴ In effort to achieve JADO capabilities, the Secretary of the Army and the Chief of Staff of the Army established eight Cross Functional Teams (CFT) to drive requirements development and modernization of Army warfighting capabilities.⁹⁵

⁹⁰ Ibid.

⁹¹ Ibid.

⁹² Ibid. The FY2021 request intends to implement the direction of the Joint Requirements Oversight Council Memorandum (JROCM) 130-17, dated December 21, 2017.

⁹³ Ibid.

⁹⁴ U.S. Army, *The U.S. Army in Multi Domain Operations 2028*, December 6, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

⁹⁵ U.S. Army, *Army Directive 2017-24 (Cross-Functional Team Pilot In Support of Materiel Development)*, October 6, 2017, at https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6101_AD2017-24_Web_Final.pdf.

Figure 6. Army Cross-Functional Teams

Source: U.S. Army, "Army Directive 2017-24 (Cross-Functional Team Pilot In Support of Materiel Development)," October 6, 2017, at https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6101_AD2017-24_Web_Final.pdf.

Notes: Army Directive 2017-24 established the Cross Functional Teams. The CFTs are led by U.S. Army Futures Command, which is responsible for driving requirements development and modernization.

ISR Task Force

The ISR Task Force, established in 2019 and led by the Deputy Chief of Staff for Intelligence, Lieutenant General Scott Berrier, performs a complimentary and enabling role to the CFTs by providing intelligence capabilities and resources to support them.⁹⁶ Its mission is to explore "established requirements for intelligence operations within a multi domain operating environment and develop sensors, concepts and techniques," with emphasis on executing JADO against a peer adversary within a highly contested environment.⁹⁷ As the task force's work progresses, it will also aim to capitalize on complimentary capabilities across the U.S. military and the Intelligence Community.

Lieutenant General Berrier and the ISR Task Force have identified four modernization priorities as the service transitions its focus from COIN/CT operations toward great power competition: (1) space, (2) multidomain sensing system, (3) terrestrial layer system (TLS), and (4) Tactical Intelligence Targeting Access Node (TITAN). Together these capabilities are designed to connect sensors to shooters and enable execution of joint all domain operations.⁹⁸

⁹⁶ Amble, John, "Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier," *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

⁹⁷ Ibid.

⁹⁸ Ibid.

Space

The Army's first modernization initiative, space, is a joint effort between the Army and the National Reconnaissance Office (NRO). The plan calls for use of NRO prototype satellites for tasking and direct downlink of ISR assets operating in low earth orbit.⁹⁹ The current intent is to inform requirements development, improve partnerships, and inform future investments for capabilities that will provide persistent and penetrating satellite-based geospatial and signals intelligence coverage of adversary actions to spark Army intelligence operations in support of long-range fires and maneuver.¹⁰⁰ The pursuit of low earth orbit ISR satellites for operations within a highly contested environment suggests the Army plans to field a considerable number of platforms, some of which may even be designed as cost-effective, attributable capabilities that can be reused or employed as expendable resources. An \$86.8 million line item is budgeted for this effort in FY2021.¹⁰¹

Multi-Domain Sensor System

Operating in the air domain and led by the Army Intelligence and Security Command, the Multi-Domain Sensor System (MDSS) is pursuing manned and unmanned aerial systems capable of operating at high and medium altitudes.¹⁰² Aircraft would employ various geospatial, full-motion video and technical intelligence sensors to identify targets and advanced signals deep in enemy territory and drive long-range precision targeting.¹⁰³ According to the Commander of the Army Intelligence Center of Excellence, the service wants "smart sensors that are tied down to shooters to close that gap to when we see the enemy to when we kill the enemy."¹⁰⁴ Future platform options for MDSS include high-altitude maneuverable balloons, gliders, and a joint effort with the Navy on the P-8 Poseidon program.¹⁰⁵ Sensor options include synthetic aperture radar and moving target identification sensors enabled with AI that can rapidly and reliably identify enemy movements to enable rapid targeting of prioritized targets.¹⁰⁶ A \$52 million line item is budgeted for MDSS in FY2021 to launch sensor development and prototyping.¹⁰⁷

⁹⁹ Based on CRS discussions with John J. Strycula and William Frederick, Army G2 ISR Task Force, December 20, 2019.

¹⁰⁰ Amble, John, "Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier," *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹⁰¹ U.S. Army, Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, Army, Justification Book of Research, Development, Test, and Evaluation, Army RDT&E, Budget Activity 4, accessed February 12, 2020, at https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/rdte/RDTE_BA_4_FY_2021_PB_RDTE_Vol%202_Budget_Activity_4.pdf.

¹⁰² Amble, John, "Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier," *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹⁰³ Ibid.

¹⁰⁴ Pomerleau, Mark, "The Army Targets Systems to 'see' 1000 miles," *C4ISRNet*, April 2, 2019, at <https://www.c4isrnet.com/c2-comms/2019/04/02/the-army-targets-systems-to-see-1000-miles/>.

¹⁰⁵ Based on CRS discussions with John J. Strycula and Major William Frederick, Army G2 ISR Task Force, December 20, 2019.

¹⁰⁶ Ibid.

¹⁰⁷ U.S. Army, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Army, Justification Book of Research, Development, Test, and Evaluation, Army RDT&E, Budget Activity 4, accessed February 12, 2020, at https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/rdte/RDTE_BA_4_FY_2021_PB_RDTE_Vol%202_Budget_Activity_4.pdf.

Terrestrial Layer System

Led by the Army Intelligence Center of Excellence, the Terrestrial Layer System (TLS) aims to modernize current ground-based signals intelligence collection systems to converge with electronic warfare and cyber into a combined set of Information Warfare capabilities.¹⁰⁸ Senior Army intelligence officials state that TLS “should be able to not only sense the environment but employ some type of action such as electronic attack or cyber capability.”¹⁰⁹ Employed by military intelligence, electronic warfare units and cyber-electromagnetic activities teams at the Brigade Combat Team level, TLS is projected to be fielded on vehicles, enabling mobility, a necessary attribute to optimize system survivability in a highly contested environment.¹¹⁰ In FY2021, a \$22.8 million line item is budgeted for TLS to support RDT&E of component level technologies such as antennas, radios, software architectures plus signals, electronic warfare, and cyber modernization.¹¹¹

Tactical Intelligence Targeting Access Node

To leverage the abundance of multidomain data collected via Space, MDSS, and TLS, as well as by commercial, Joint and Intelligence Community partners, the Army is pursuing development of the Tactical Intelligence Targeting Access Node (TITAN). The Army intends that TITAN serve as a ground-based intelligence system designed to rapidly process data and disseminate targetable intelligence directly to tactical weapon systems deployed across the battlefield, and generate situational awareness for battlefield commanders.¹¹² This AI/ML-assisted mobile intelligence ground station will shorten find, fix, and target timelines by tying deep sensing to Army long-range precision strike options to defeat A2/AD threats and provide standoff to optimize survivability of soldiers and warfighting capabilities.¹¹³ A \$30 million line item is budgeted to build two prototypes in FY2022, followed by system fielding in FY2023 and FY2024.¹¹⁴

Distributed Common Ground System—Army

According to Lieutenant General Berrier, the Army is also emphasizing improving analytic capabilities and data management. “We can have the most pristine sensors in the world,” he said, “and if you don’t have the right analytics and cloud computing to sort all that data you are in

¹⁰⁸ Amble, John, “Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier,” *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹⁰⁹ Pomerleau, Mark, “The Army Wants to Build a Better Signals Intelligence Force,” *C4ISRNet*, July 19, 2018, at <https://www.c4isrnet.com/intel-geoint/2018/07/19/the-army-wants-to-build-a-better-signals-intelligence-force/>.

¹¹⁰ Ibid.

¹¹¹ U.S. Army, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Army, Justification Book of Other Procurement, Army Communications and Electronics Equipment, Budget Activity 2, accessed February 12, 2020, at https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/Procurement/OPA_BA_2_FY2021_PB_Other_Procurement_BA2_Communications_and_Electronics.pdf.

¹¹² Amble, John, “Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier,” *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹¹³ Ibid.

¹¹⁴ U.S. Army, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Army, Justification Book of Research, Development, Test, and Evaluation, Army RDT&E, Budget Activity 4, accessed February 12, 2020, at https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/rdte/RDTE_BA_4_FY_2021_PB_RDTE_Vol%202_Budget_Activity_4.pdf and Amble, John, Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier, *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

trouble.”¹¹⁵ The Army possesses its own Distributed Common Ground System capability, called DCGS-Army (DCGS-A), a legacy platform developed before the terror attacks on September 11. However, this program will serve as the foundation for “capability drops,” or small bundles of capability upgrades that take advantage of agile acquisition, resulting in the opportunity to field enhanced analytic tools and improved data management more quickly.¹¹⁶ The first capability drop focuses on delivering DCGS-A enhancements for the battalion. It will increase mobility by replacing roughly 500 pounds of equipment with three laptops, which act as servers connected to the intelligence architecture, to support analytic and intelligence planning functions.¹¹⁷ The second capability drop is designed to fix the data problem. The Army currently possesses 13 disparate databases across multiple theaters and is aiming to consolidate data, using joint data standards, into three cloud ready nodes in the Pacific, Europe, and in the United States.¹¹⁸ This provides an opportunity to improve data access, maximize AI/ML capabilities, and speed advanced analytics to support sensor to shooter operations. In FY2020, the Army received appropriations for \$28.8 million in RDT&E and \$166.6 million in procurement funds to support DCGS-A.¹¹⁹ A \$199.6 million line item is budgeted for the program in FY2021, which includes a \$30.6 million program reduction.¹²⁰

Science and Technology Focus

To leverage emerging technologies, accelerate modernization, and support pursuit of Army ISR Task Force lines of effort, the Army G-2 established science and technology focus areas to continually refine industry, government, and academia’s understanding of Army Intelligence areas of interest. The focus areas include a foundation rooted in data, information, and knowledge, collection assets, analysis, automation, interoperability, and training.¹²¹

Other Views

Notably missing from the list of Army CFT priorities is ISR. Although “intelligence” is listed within the fourth priority, the Army emphasis is on network modernization, development of a command post common environment, and mobility and survivability. General John Murray, commander of Army Futures Command, stated, “I get criticized all the time because we don’t have an [intelligence cross-functional team],” which led to the creation of the Army ISR Task Force.¹²² The lack of a dedicated ISR CFT may negatively affect the Army’s initiative to develop and field the platforms and sensors necessary to generate target-quality data for long-range precision fires and other associated Army warfighting functions.

¹¹⁵ Amble, John, “Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier,” *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹¹⁶ *Ibid.*

¹¹⁷ *Ibid.*

¹¹⁸ *Ibid.*

¹¹⁹ Fiscal Year 2020 Department of Defense Appropriations Act, P.L. 116-93.

¹²⁰ U.S. Army, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Army, Justification Book of Research, Development, Test, and Evaluation, Army RDT&E, Budget Activity 4, accessed February 12, 2020, at https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2021/Base%20Budget/rdte/RDTE_BA_4_FY_2021_PB_RDTE_Vol%202_Budget_Activity_4.pdf.

¹²¹ Amble, John, “Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier,” *Modern War Institute*, October 25, 2019, at <https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/>.

¹²² Tressel, Ashley, “Army has new ISR Task Force,” *Inside Defense*, May 7, 2019, at <https://insidedefense.com/insider/army-has-new-isr-task-force>.

Navy

Information Warfare

Over the past decade, the Navy has arguably generated the most mature Information Warfare capability among the services. Organized around the core concept of information, naval intelligence and information technology supports the Navy's Information Warfare priorities of battlespace awareness, assured C2, integrated fires, and cyber.

According to Rear Admiral Steven Parode, Director, Navy Warfare Integration Directorate, Office of the Chief of Naval Operations, naval intelligence aims to support the service's Information Warfare implementation plan and build on the service's previous analytic expertise to ensure U.S. forces possess advantageous battlespace awareness across the maritime domain.¹²³ To support ISR sensors/processor development, the Navy requested \$280 million for FY2021, down from \$342 million requested and \$357 million appropriated in FY2020.¹²⁴

Airborne Platforms

The Navy continues its transition away from manned airborne ISR platforms and is expanding its inventory of unmanned airborne ISR platforms. The EP-3E ARIES II, a manned ISR platform responsible for signals intelligence collection, will be replaced by the MQ-4C Triton. The MQ-4C, a long-endurance, high-altitude platform akin to the Air Force RQ-4 Global Hawk, will assume the signals intelligence mission in FY2022 and continue to execute its wide area maritime surveillance mission.¹²⁵ However, the current budget submission reflects an MQ-4C production pause in FY2021 (\$150.5 million) and FY2022 (\$95.7 million), deferring further procurement of the multi-intelligence capable platform and sensor configuration until FY2023 (\$624.9 million).¹²⁶

Surface Vessels

For surface ships, the Navy requested \$66.3 million in FY2021 to fund procurement of six Ship Signals Exploitation Equipment systems (SSEE); this funding will also support procurement of electronic warfare capabilities.¹²⁷ SSEE is designed to enhance the signals intelligence capabilities of its surface fleet aiding in detection, collection, processing, and display of adversary communications and actions in the battlespace.¹²⁸ The Navy is also investing in surface unmanned capabilities such as Large and Medium Unmanned Surface Vehicles, which are designed to carry

¹²³ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-I8dt2gL9A>.

¹²⁴ U.S. Navy, *Department of the Navy FY 2021 President's Budget*, February 10, 2020, at https://www.secnave.navy.mil/fmc/fmb/Documents/21pres/DON_Press_Brief.pdf.

¹²⁵ U.S. Navy, *Highlights of the Department of the Navy FY 2021 Budget, Office of Budget – 2020*, February 10, 2020, at https://www.secnave.navy.mil/fmc/fmb/Documents/21pres/Highlights_book.pdf.

¹²⁶ U.S. Navy, *Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Justification Book Volume 1 of 3 Aircraft Procurement, Navy Budget Activities 01–04*, at https://www.secnave.navy.mil/fmc/fmb/Documents/21pres/APN_BA1-4_BOOK.pdf.

¹²⁷ U.S. Navy, *Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Justification Book Volume 2 of 5 Other Procurement, Navy BA 02*, February 2020, at https://www.secnave.navy.mil/fmc/fmb/Documents/21pres/OPN_BA2_BOOK.pdf.

¹²⁸ *Ibid.*

various payloads to include ISR sensors.¹²⁹ The service requested \$21.5 billion for modernization, a 5.1% increase in funding for FY2021, aimed at investing in emerging technology such as unmanned platforms and AI that can connect the force and support intelligence.¹³⁰

Data Fusion Technology

Naval intelligence, partnered with the Chief of Naval Research, also has a focus on developing and fielding AI/ML capabilities. The service's focus is on data and the integration of emerging technologies with an emphasis on getting machines to plow through massive amounts of structured and unstructured data.¹³¹ An emerging AI capability, called Minotaur and designed by Johns Hopkins Applied Physics Laboratory, is an automated intelligence correlation processor that can be installed on platforms or in control stations to analyze data derived from multiple sensors across domains.¹³² Fielded on a handful of deployed platforms, Minotaur may prove supportive of large-scale navy Information Warfare and information superiority needs within a vast and active maritime security and operational environment. It can automatically optimize data collection against an object or target, and enable an analyst to quickly filter and prioritize data by varying characteristics such as size, speed, direction, and location of an object or target.¹³³ This set of features enables real-time data fusion, at machine speed, to find and fix adversary targets and support rapid decisionmaking by commanders. Minotaur received \$5 million in FY2020 appropriations, and the Navy requested an additional \$5 million in FY2021 procurement funds.¹³⁴

¹²⁹ CRS Report R45757, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, by Ronald O'Rourke.

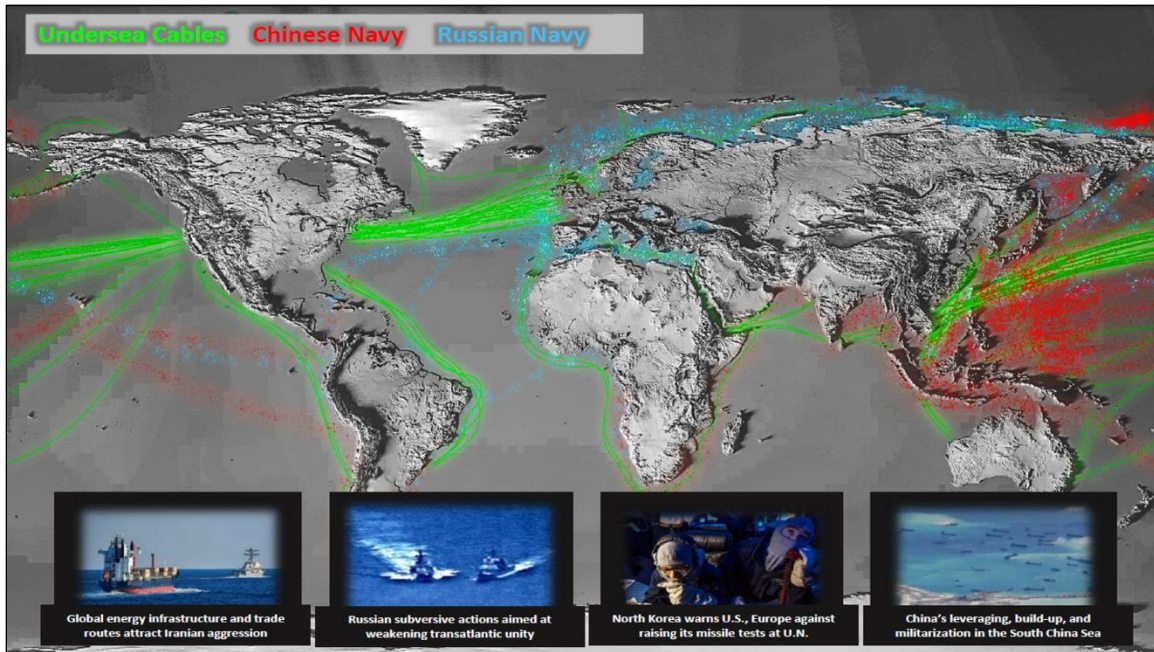
¹³⁰ *Ibid.*

¹³¹ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-I8dt2gL9A>.

¹³² Anderson, Sharon, "Delivering Decisive Understanding to the Commander," *DON CIO*, April-June 2016, at <https://www.doncio.navy.mil/mobile/ContentView.aspx?ID=7899&TypeID=21>.

¹³³ *Ibid.*

¹³⁴ U.S. Navy, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Justification Book Volume 2 of 5 Other Procurement, Navy BA 02, February 2020, at https://www.secnv.navy.mil/fmc/fmb/Documents/21pres/OPN_BA2_BOOK.pdf.

Figure 7. Maritime Security and Operational Environment

Source: U.S. Navy, *Department of the Navy FY2021 President's Budget*, undated but released February 2020, at https://www.secnav.navy.mil/fmc/fmb/Documents/21pres/DON_Press_Brief.pdf.

Human Capital

To ensure sailor readiness, the Navy has emphasized investments in human capital in order to produce a digital age workforce. The Navy intends to address this critical need by producing “an agile, trained, and intelligent workforce” able to “sense, collect, understand, and act decisively.”¹³⁵ To reach this goal, the Navy is emphasizing digital age training at all levels, beginning at basic training and extending to those sailors and marines pursuing advanced academic degrees.¹³⁶ In addition to training and educating its workforce for the digital age, the Navy intends to generate an “ecosystem of digital innovation centers” and to integrate the “information environment into all its career paths” as information superiority underpins all naval operations in the future.¹³⁷ The digital “innovation centers will bring together teams of Sailors and Marines to develop solutions through user-centered design in Development-Security-Operations with known tools and libraries,” much like the Air Force Kessel Run initiative.¹³⁸

Other Views

Some analysts argue that while the Navy has placed added emphasis on Information Warfare, the funding requests to advance the necessary capabilities have not matched this emphasis. Analysts argue that “Information Warfare requirements usually end up ‘bolting on’ to existing programs”

¹³⁵ U.S. Navy, Information Warfare Community, at https://www.public.navy.mil/bupers-npc/enlisted/community/crypto_it/Pages/default.aspx.

¹³⁶ U.S. Navy, *Department of the Navy Information Superiority Vision*, February 21, 2020, at <https://news.usni.org/2020/02/21/department-of-the-navy-information-superiority-vision>.

¹³⁷ Ibid.

¹³⁸ Ibid.

and are “not included in initial requirements capability documents, or they are the first things sacrificed when cuts are made.”¹³⁹ The message the Navy is sending is that Information Warfare matters doctrinally but not fiscally.¹⁴⁰ This may prove a challenging obstacle to overcome as the Navy, not dissimilar from the other services, is a platform-centric service.

Marine Corps

Expeditionary Advanced Base Operations

The objective of the future Marine Corps operational concept, Expeditionary Advanced Base Operations (EABO), is to “mitigate peer competitors’ anti-access/area denial capability by creating a more survivable, resilient, and persistent forward-postured force.”¹⁴¹ This forward-postured force, which would be located on allied and partnered territory or seized terrain, is designed to have a “deterrent effect” capable of holding adversary targets at risk via long-range fires.¹⁴² Inherent in executing long-range fires is the need to find and fix targets for engagement, a central role for ISR.

Establishing a contemporary Marine Corps vision, the Commandant of the Marine Corps, General David H. Berger, published his planning guidance in 2019. It addresses the criticality of ISR by recognizing that “a likely vision of warfare centers on the recon/counter-recon contest. This demands an agile, stealthy, tactical system employing forces that are able to locate, target, and fire precisely first.”¹⁴³

Marine Corps ISR Enterprise

The Marine Corps ISR Enterprise (MCISRE) is the “mechanism, via personnel, equipment, and processes, that merges disparate nodes of the Marine Corps intelligence effort” into a cohesive set of capabilities designed to support decisionmaking.¹⁴⁴ In support of the commandant’s planning guidance, the Marine Corps Director of Intelligence is drafting the MCISRE 2025 strategy. The strategy aims to pursue innovation and disruptive technologies to accelerate capability development of the MCISRE.¹⁴⁵ MCISRE integrates data, information, and intelligence to aid decisionmaking, and aims to promote a culture that embraces technology and human-machine teaming, allowing for decisionmaking at machine speed that will outpace and outthink any

¹³⁹ Captain Butera, Tony, “Navy Information Warfare Needs More Resources – and Command at Sea,” *U.S. Naval Institute*, January 2019, at <https://www.usni.org/magazines/proceedings/2019/january/navy-information-warfare-needs-more-resources-and-command-sea>.

¹⁴⁰ Ibid.

¹⁴¹ U.S. Marine Corps, *2019 Marine Corps Aviation Plan*, at <https://www.aviation.marines.mil/portals/11/2019%20avplan.pdf>.

¹⁴² Ibid.

¹⁴³ U.S. Marine Corps, *Commandant’s Planning Guidance*, July 17, 2019, at https://www.marines.mil/Portals/1/Publications/Commandant's%20Planning%20Guidance_2019.pdf?ver=2019-07-17-090732-937.

¹⁴⁴ U.S. Marine Corps, Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise, <https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/MCISRE/>.

¹⁴⁵ U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise*, at <https://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/MCISRE/>.

threat.¹⁴⁶ Short of a published MCISRE strategy, the Marine Corps has pieced out a general ISR vision to support EABO and pursue fulfilling the requirements of the NDS.

The Marine Corps' ISR design is predominantly aimed at developing a networked capability of manned aircraft, unmanned aircraft, and unmanned surface vessels to support decisionmaking and cue rapid targeting of adversary forces. It also possesses a reliance on unmanned Navy MQ-4C Triton area surveillance capabilities, plus joint and Intelligence Community collection and analytic capabilities.¹⁴⁷ The Corps is also teaming with the Navy on unmanned large and medium surface vessels for ISR.

Airborne Platforms

According to the 2019 Marine Corps Aviation Plan, the F-35 will play a significant role in supporting and conducting long-range fires, by employing its sophisticated sensors for collection, data fusion, and targeting across the force.¹⁴⁸ In addition, unmanned systems will serve an increasingly important role, providing both cost-effective, persistent surveillance and reconnaissance capabilities for collection deep in enemy territory, and smaller, expendable unmanned aircraft systems (UAS) for the close and mid-range fight, while also supporting rear area EABO security requirements.¹⁴⁹ The Corps requested \$24.9 million in FY2021 procurement funds to support its modernization of unmanned air systems for intelligence.¹⁵⁰

Surface Vessels

The Marine Corps is teaming with the Navy to invest in surface unmanned capabilities, such as Large and Medium Unmanned Surface Vehicles, which are designed to carry various payloads to include ISR.¹⁵¹

Data Fusion Technology

The Aviation Plan also identifies a key enabling capability composed of AI/ML and cloud technology, called the Tactical ISR Processing, Exploitation, and Dissemination System (TIPS) Block 3. TIPS aims to “fuse information collected from unmanned aircraft with information from other off board data systems” and serve as a “digitally interoperable hub for the collection, cataloguing and storage of full motion video, multi-intelligence sensor data, topological data, and target information.”¹⁵² Future iterations of TIPS Block 3 will use advanced algorithms to analyze the vast amount of data as it is collected and autonomously cue operators to defined areas of interest, suggesting an emphasis on developing a data strategy, edge computing, cloud

¹⁴⁶ Ibid.

¹⁴⁷ Telephone conversation between the author and Mark Costner, Headquarters Marine Corps Intelligence Department Marine Air Ground Task Force Branch, January 30, 2020.

¹⁴⁸ U.S. Marine Corps, *2019 Marine Corps Aviation Plan*, at <https://www.aviation.marines.mil/portals/11/2019%20avplan.pdf>.

¹⁴⁹ Ibid.

¹⁵⁰ U.S. Navy, *Supporting Exhibits (M-1, O-1, P-1, R-1 & C-1) Department of the Navy FY 2021 Budget*, Office of Budget-2020, January 22, 2020, at https://www.secnav.navy.mil/fmc/fmb/Documents/21pres/Supp_Book.pdf.

¹⁵¹ CRS Report R45757, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, by Ronald O'Rourke.

¹⁵² U.S. Marine Corps, *2019 Marine Corps Aviation Plan*, at <https://www.aviation.marines.mil/portals/11/2019%20avplan.pdf>.

technology, and AI/ML capabilities for operating within an integrated information environment.¹⁵³

Information Warfare

Lieutenant General Lori Reynolds, the Marine Corps Deputy Commandant for Information, has prioritized network modernization and all domain ISR for the future Marine Corps information environment.¹⁵⁴ Network modernization will adopt AI and incorporate “a mobile cloud” capability. All domain ISR modernization will cover a “range of capabilities” by incorporating new AI/ML tools and using new intelligence sources, to include publicly available information and intelligence support to space and cyber.¹⁵⁵ These capabilities will be integrated within a series of “Marine Expeditionary Force Information Groups,” which will serve as the Marine’s focal point for all information warfare capabilities within a deployed force.¹⁵⁶ Furthermore, the Marines will integrate its Information Groups with the “U.S. Navy’s distributed maritime operations concept” with the intent to “deter, frustrate the adversary’s understanding,” and enable naval power projection against an adversary.¹⁵⁷

Operationalizing ISR for Great Power Competition

The military services have highlighted a number of focus areas to ensure ISR rapidly delivers decision-quality and target-quality insights to support operational planning, operations, and assessment. Common elements within each service’s ISR modernization revolve around data, disruptive technology, and human capital while remaining dependent upon a data-centric architecture that connects sensors to shooters. Simply stated, the DOD ISR enterprise intends to gain access to all domain data; make rapid sense of that data; securely deliver that data to weapons, weapon systems, and commanders; and ensure a workforce that can execute its mission in the grey zone and highly contested environments at a pace greater than the enemy.

Data

“Data is the currency of future warfare, and we must be able to fight at the speed the future will demand.”¹⁵⁸

General David L. Goldfein, USAF

Data, a critical strategic, operational and tactical asset, is the foundational element to generating intelligence. National security experts advocate that the ability to harness the power of data is

¹⁵³ Ibid.

¹⁵⁴ Strout, Nathan, “The Marine Corps’ 4 Priorities in the Information Environment,” *C4ISRNet*, January 6, 2020, at <https://www.c4isrnet.com/information-warfare/2020/01/06/the-marine-corps-4-priorities-in-the-information-environment/>.

¹⁵⁵ Ibid.

¹⁵⁶ Pomerleau, Mark, “The Navy and Marines want an Integrated Force for Information Warfare,” *C4ISRNet*, December 5, 2019, at <https://www.c4isrnet.com/information-warfare/2019/12/05/the-navy-and-marines-want-an-integrated-force-for-information-warfare/>.

¹⁵⁷ Ibid. The U.S. Navy’s Distributed Maritime Operations concept and the Marine Corps’ Expeditionary Advanced Base Operations build on the vision of distributed lethality to connect ships, submarines, aircraft, and satellites in networks to inform command and control elements and connect sensors with shooters.

¹⁵⁸ General David L. Goldfein, Chief of Staff of the Air Force, “Fireside Chat with General David L. Goldfein,” Center for New American Studies, Washington, DC, January 20, 2020.

fundamental to building and deploying the most effective military in the world.¹⁵⁹ Data is not scarce in military ISR. However, DOD faces significant challenges with harnessing the power of data and making sense of all the data collected. Three contributing factors include (1) lack of a DOD data strategy, (2) data formats leading to limitations in data discovery, and (3) contending with the sheer abundance of data generated across the globe.

DOD Data Strategy

To address the first challenge, DOD continues to develop its department-wide data strategy, which may be approved very soon by Defense Secretary Esper.¹⁶⁰ The strategy will address policies, guidance, processes, and tools to generate data that is discoverable, accessible, usable, and trusted.¹⁶¹ According to Thomas Sasala, the Navy's Chief Data Officer, the strategy will focus on "managing and governing information and data by organization or by programs or systems" by grouping "information together and managing like information as a dataset" across "12 information domains."¹⁶² Examples of information domains are "medical information, legal information, and financial management."¹⁶³ However, Congress may consider whether the DOD data strategy includes ISR data and is interoperable with data generated from the intelligence community. Once the strategy is published, the services will execute their implementation plans.

Challenges with Data Formats

Data formats are not standardized, neither within a service, across the services, nor between the elements of the intelligence community. Data exists in both structured and unstructured formats and includes various intelligence disciplines (e.g., geospatial intelligence, signals intelligence, human intelligence), publicly available information (such as social media), and operational data (F-35, carrier strike group).¹⁶⁴ In addition, the data are stored across numerous information technology systems at varying classification levels leading to added challenges with discovering high value data relative to a particular problem set.

Adding to the complexity, each intelligence organization has developed its own unique lexicon for its data. For example, two analysts possessing different training and expertise, and operating under differing organizational standards, may both reference a Russian missile differently. One will identify the missile as an SS-27, the other may call it an intercontinental ballistic missile. They are both correct, but the lack of data standardization and specificity impedes discovery, research, and analytics. These factors lead an analyst to spend 80% of their time searching for

¹⁵⁹ The White House, *National Security Strategy*, December 18, 2017, at <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

¹⁶⁰ Doubleday, Justin, "Congress Shift 'Chief Data Officer' Away from CMO's Office as Pentagon Finalizes Data Strategy," *Inside Defense*, January 6 2020, at <https://insidedefense.com/daily-news/congress-shifts-chief-data-officer-away-cmos-office-pentagon-finalizes-data-strategy>.

¹⁶¹ U.S. Navy, Chief Information Officer Data Strategy, at <https://www.doncio.navy.mil/TagResults.aspx?ID=23>.

¹⁶² Sasala, Thomas, "Interview with Thomas Sasala, DON Chief Data Officer Talks about Building an Enterprise Data Architecture," *CHIPS*, January-March 2020, at <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=13186>.

¹⁶³ *Ibid.*

¹⁶⁴ Structured data is highly organized and formatted in a way so it is easily searchable in relational databases. Unstructured data has no predefined format or organization, making it much more difficult to collect, process, and analyze.

data and 20% of their time making sense of the data, negatively affecting analyst attempts to discover high-value data in order to generate rapid and accurate insights.¹⁶⁵

Keeping Pace with Data

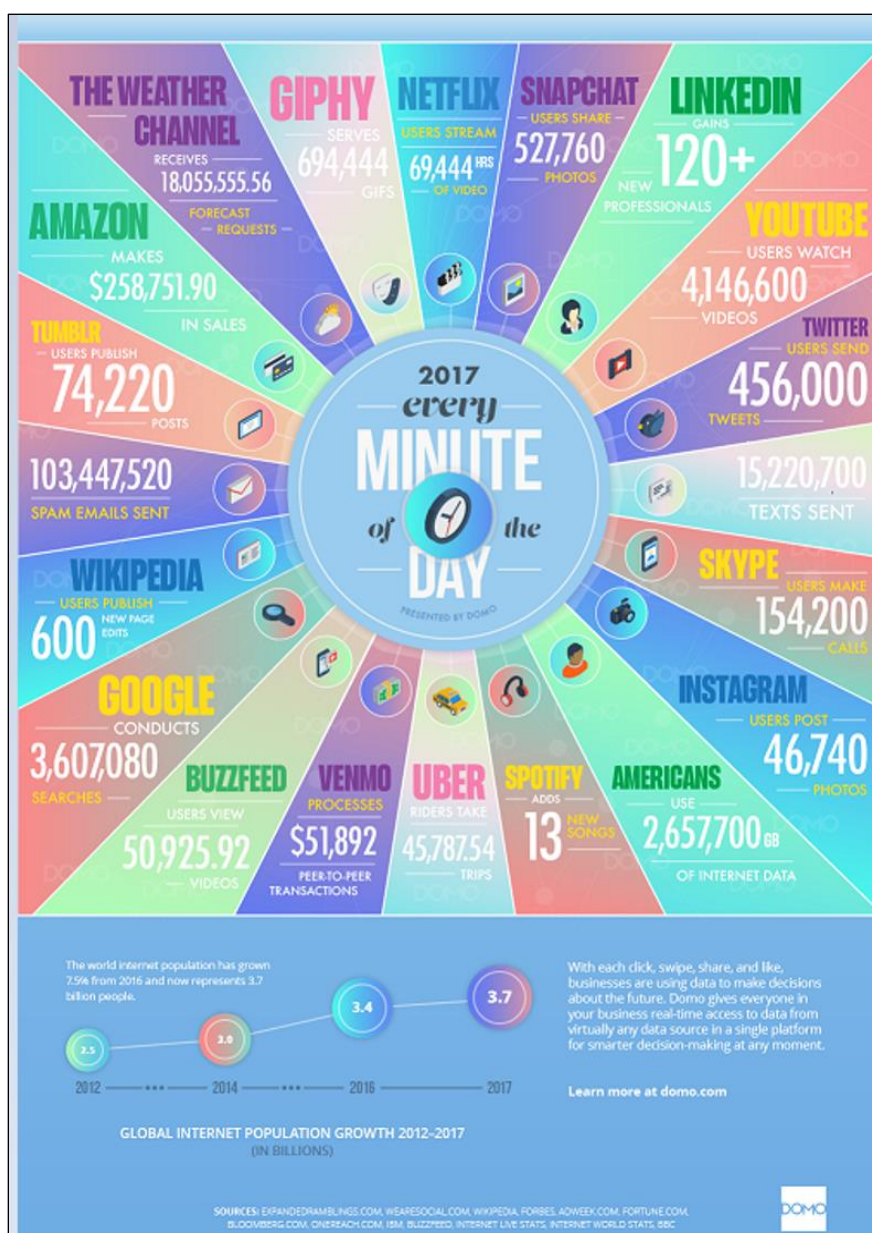
Across the globe, the volume of data has doubled every two years since 2014, and all signs point to its continued exponential growth.¹⁶⁶ In 2017, the Pentagon collected 22 terabytes of data per day and the 3.7 billion users across the globe produced 2.5 quintillion bytes of data per day.¹⁶⁷ Intelligence analysts are contending with having access to too much data, which can have a debilitating effect when attempting to discover high-value data in order to generate insights, especially rapidly. It is this challenge that has led DOD toward developing disruptive technology, such as AI/ML, that allows for human-machine teaming to ultimately help analysts make sense of the tidal wave of data.

¹⁶⁵ U.S. Air Force, Department of Defense Fiscal Year (FY) 2021 Budget Estimates, Air Force, Justification Book Volume 3b of 3, Research, Development, Test & Evaluation, Air Force, Vol-III Part 2, February 10, 2020, at https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIb%20-%20updated.pdf?ver=2020-02-12-125427-660.

¹⁶⁶ International Data Corporation, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, April 2014, at <https://www.emc.com/leadership/digital-universe/2014iview/index.htm>.

¹⁶⁷ Mehta, Aaron, "Pentagon Tech Advisers Target How the Military Digests Data," *Defense News*, April 6, 2017, at <https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/> and DOMO, *Data Never Sleeps 5.0*, at https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1.

Figure 8. How Much Data Is Generated Every Minute?



Source: DOMO, *Data Never Sleeps 5.0*, https://www.domo.com/learn/data-never-sleeps-5?aid=ogsm072517_1&sf100871281=1.

Notes: Data in this chart are current as of 2017. In 2017, 90% of all data was created in the previous two years—2.5 quintillion bytes of data per day.

Disruptive Technology

Artificial intelligence is the sum of data, algorithms, and computing power.¹⁶⁸ Algorithms can automate tasks for a variety of intelligence functions and speed intelligence processes across the

¹⁶⁸ CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler.

spectrum of conflict. However, significant advances in AI/ML and cloud technology may be needed to achieve the DOD's vision for all domain sensor-to-shooter operations.

Human-Machine Teaming

To maintain pace with the demands for intelligence, former Deputy Director of National Intelligence Sue Gordon stated that “we are going to have to make machines integrated into all of our processes.”¹⁶⁹ This perspective mirrors that of DOD ISR leaders who have advocated for human-machine teaming technology to provide the force better scalability, capacity, flexibility, and collaboration. Efforts to advance computing development and training initiatives will give ISR analysts the time and data they need to become more precise and effective in their analysis on warfighter problems.¹⁷⁰

A prime example of DOD efforts to produce disruptive technology and enable human-machine teaming is Project Maven. Launched in 2017, Project Maven has led the DOD's AI/ML development of computer vision algorithms to improve target characterization and identification of objects within full-motion video and imagery. In addition, Project Maven is pursuing capabilities to support perception, natural language processing, recognition, and classification detection and tracking of objects.¹⁷¹ DOD has suggested that such AI-enhanced tools could allow human analysts to process up to two to three times as much data within the same time period, providing more time-sensitive targeting data and a reduction of collateral damage and civilian casualties.¹⁷² Project Maven received \$221 million dollars in FY2020 appropriations, and DOD requested \$800 million for FY2021 RDT&E to support both Project Maven and the Joint Artificial Intelligence Center.¹⁷³

Rear Admiral Parode also suggested a concerted focus on developing human-machine interfaces that spark and capture an analyst's intellectual curiosity by captivating their interest while simultaneously not creating a training burden.¹⁷⁴ Such interfaces may be able to capitalize on human-machine interface technology produced by commercial video game companies. However, a significant challenge exists with algorithm development and the fielding of AI/ML capabilities: trust must be earned. Commanders and operators alike must gain trust and confidence in an algorithm's performance. Much the same way the U.S. military gains trust and confidence in its junior workforce, training, exercise, and experimentation will provide opportunities to gain trust and confidence in AI/ML performance.

¹⁶⁹ Corrigan, Jack, “Spy Agencies Turn to AI to Stay Ahead of Adversaries,” *Nextgov*, June 27, 2019, at <https://www.nextgov.com/emerging-tech/2019/06/spy-agencies-turn-ai-stay-ahead-adversaries/158081/>.

¹⁷⁰ U.S. Air Force, *Next Generation ISR Dominance Flight Plan 2018-2028*, July 24, 2018.

¹⁷¹ Stone, Adam, “The Pentagon's top AI Official explains ‘Computer Vision’,” *C4ISRNet*, September 13, 2019, at <https://www.c4isrnet.com/thought-leadership/2019/09/13/the-pentagons-top-ai-official-explains-computer-vision/>.

¹⁷² CRS Report R45392, *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, coordinated by Andrew Feickert.

¹⁷³ Fiscal Year 2020 Department of Defense Appropriations Act, P.L. 116-93 and Department of Defense, “Defense Budget Overview: Irreversible Implementation of the National Defense Strategy,” *Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer*, May 13, 2020, at https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf.

¹⁷⁴ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-18dt2gL9A>.

Cloud Technology

Cloud technology is likely the only way to achieve the enormous computing power required to run AI/ML tools at the scale of America's defense and intelligence operations.¹⁷⁵ Lieutenant General Jack Shanahan, who leads the Pentagon's Joint Artificial Intelligence Center, stated that DOD AI efforts will be limited until its own enterprise cloud platform is up and running.¹⁷⁶ Data, algorithms, and computer power must all come together for intelligence analysts to capitalize on the potential AI/ML can play in helping human analysts make sense of the immense amount of data collected. In addition, these same capabilities must also come together for the U.S. military to achieve a sensor-to-shooter network in support of joint all domain operations, according to senior defense leaders.¹⁷⁷

Human Capital

“All of our investments in data science, machine learning, and artificial intelligence are designed to unleash the incredible talent of the individual Marine.”¹⁷⁸

General David H. Berger, USMC

Shaping the Future ISR Force

To harness the power of data, algorithms, computer power, and networked operations, the services are pursuing changes to workforce culture, recruiting, force development, talent management, and retention.¹⁷⁹ The changes are intended to ensure military readiness for digital age military operations in the grey zone and in highly contested fights. This is a significant challenge for all services, as each competes for a small pool of potential servicemembers who possess the aptitude and skill sets to advance the DOD's use of data and disruptive technology.

U.S. military ISR leaders are pursuing a competency-based assessment, recruitment, and training methodology. Competency examples include critical thinking capacity plus skill sets and tradecraft possessed, and then shaping intelligence operators with specific training and education designed to improve necessary competencies. This process is not new to the military; the services have long screened its members for unique skill sets that support specific functions.

What is new is the emphasis on human-machine teaming with AI/ML in mind, to include initiatives such as the Air Force's computer language initiative. The initiative rewards airmen with data skills the same way the services compensate troops with proficiency in languages like Arabic and Farsi.¹⁸⁰ The goal is to attract and retain airmen the services need for their increasing

¹⁷⁵ Corrigan, Jack, “Spy Agencies Turn to AI to Stay Ahead of Adversaries,” *Nextgov*, June 27, 2019, at <https://www.nextgov.com/emerging-tech/2019/06/spy-agencies-turn-ai-stay-ahead-adversaries/158081/>.

¹⁷⁶ Konkel, Frank, “Without JEDI, Pentagon's Artificial Intelligence Efforts May be Hindered,” *Nextgov*, March 29, 2019, at <https://www.nextgov.com/it-modernization/2019/03/without-jedi-pentagons-artificial-intelligence-efforts-may-be-hindered/155934/>.

¹⁷⁷ Hitchens, Theresa, “New Joint Warfighting Plan Will Help Define ‘Top Priority’ JADC2: Hyten,” *Breaking Defense*, January 29, 2020, at <https://breakingdefense.com/2020/01/new-joint-warfighting-plan-will-help-define-top-priority-jadc2-hyten/>.

¹⁷⁸ U.S. Marine Corps, *Commandant's Planning Guidance*, July 17, 2019, at https://www.marines.mil/Portals/1/Publications/Commandant's%20Planning%20Guidance_2019.pdf?ver=2019-07-17-090732-937.

¹⁷⁹ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-18dt2gL9A>.

¹⁸⁰ Vanden Brook, Tom, “Artificial Intelligence: Young Officer Mike Kaanan Helping Air Force Lead the Charge,”

reliance on technology.¹⁸¹ However, the challenges with human capital does not end at the young operator executing the mission. Senior DOD leaders must also be educated on the importance of data and both the possibilities and limitations of cloud computing and AI/ML. Education at the senior level will help DOD leaders ask the tough questions on design, architecture, and integration, and determine where to invest money for science and technology and RDT&E.

According to Lieutenant General Shanahan, “We need far more national security professionals who understand what this technology can do or, equally important, what it cannot do.”¹⁸² Furthermore, “We desperately need more people who grasp the societal implications of new technology, who are capable of looking at this new data-driven world through geopolitical, international relations, humanitarian and even philosophical lenses.”¹⁸³

Partnering with Industry and Academia

To achieve these goals, the services are partnering with industry and academia. With industry, the military is not only pursuing AI/ML development, but pursuing optimal human-machine interfaces tuned to produce human enjoyment, much like a video game, according to Rear Admiral Parode.¹⁸⁴ In addition, the military has much to learn from academia on how young American’s are learning in the digital age, and then using that data to optimize military training and education at its technical training courses.¹⁸⁵

Issues for Congress

Potential policy and oversight issues for Congress include the following:

DOD Modernization. Do DOD-wide modernization programs and budget requests for developing advanced sensing capabilities, and connecting those sensors to shooters, match the strategies identified in the National Security Strategy and National Defense Strategy?

Defense Funding Levels. In response to the current global strategic environment and DOD emphasis on Joint All Domain Operations and Joint All Domain Command and Control, should military intelligence funding levels in coming years be increased, reduced, or maintained at about the current level?

DOD Doctrine Development. In response to the global strategic environment, what efforts are underway to develop joint and service military doctrine for ISR in support of Joint All Domain Operations within both the grey zone and highly contested environments?

Operational Concept Development. Are U.S. military services moving at the appropriate speed in their efforts to develop new operational ISR concepts in response to the global strategic environment? What are the potential merits of these new operational ISR concepts, and what

USA Today, March 31, 2019, at <https://www.usatoday.com/story/news/politics/2019/03/29/air-force-pushing-artificial-intelligence-ai-research/1907314002/>.

¹⁸¹ *Ibid.*

¹⁸² U.S. Navy, *Joint Artificial Intelligence Center Director Tells Naval War College Audience to ‘Dive in’ on AI*, December 12, 2019, at https://www.navy.mil/submit/display.asp?story_id=111692.

¹⁸³ *Ibid.*

¹⁸⁴ Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at <https://www.youtube.com/watch?v=6-I8dt2gL9A>.

¹⁸⁵ *Ibid.*

steps are the services taking in terms of experiments and exercises to test and refine these concepts?

Data. What is the DOD data strategy and when will it be published? How and when will the services implement the strategy? Will the strategy address ISR data? If so, will it emphasize data interoperability between services and mission areas (i.e., intelligence and operational data)?

Service Interoperability. To what degree are the U.S. military services coordinating ISR interoperability with other services? How will the services connect their unique data architectures?

Human Capital. Do the services have the necessary human capital, resources, funding, and skill sets to design, acquire, integrate, test, evaluate, and field AI/ML for future DOD ISR operations? How are each of the services changing technical training in their school houses to ensure development of a digital age workforce?

Joint All Domain Command and Control. What is the relative priority for JADC2 compared with other major DOD programs? What role will humans have in the decision to engage if sensors are linked to shooters in real time?

Innovation and Speed in Defense Acquisition Policy. What are the impacts of Section 804 Authorities on DOD ISR innovation and acquisition? Is it supporting service needs? Are there any pitfalls with Joint Staff and Office of the Secretary of Defense-Staff oversight aimed at joint interoperability? What else does DOD need to drive ISR innovation across the department?

Effects of COVID-19 Response and Recovery Efforts. What impact might COVID-19 response and recovery efforts have on military ISR funding requests across the Future Years Defense Program? What effect might COVID-19 have on potential ISR funding intended to support the Indo-Pacific and European Defense Initiatives?

Author Information

John R. Hoehn, Coordinator
Analyst in Military Capabilities and Programs

Acknowledgments

This report was originally written by Nishawn S. Smagh during his military fellowship with the Congressional Research Service.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.