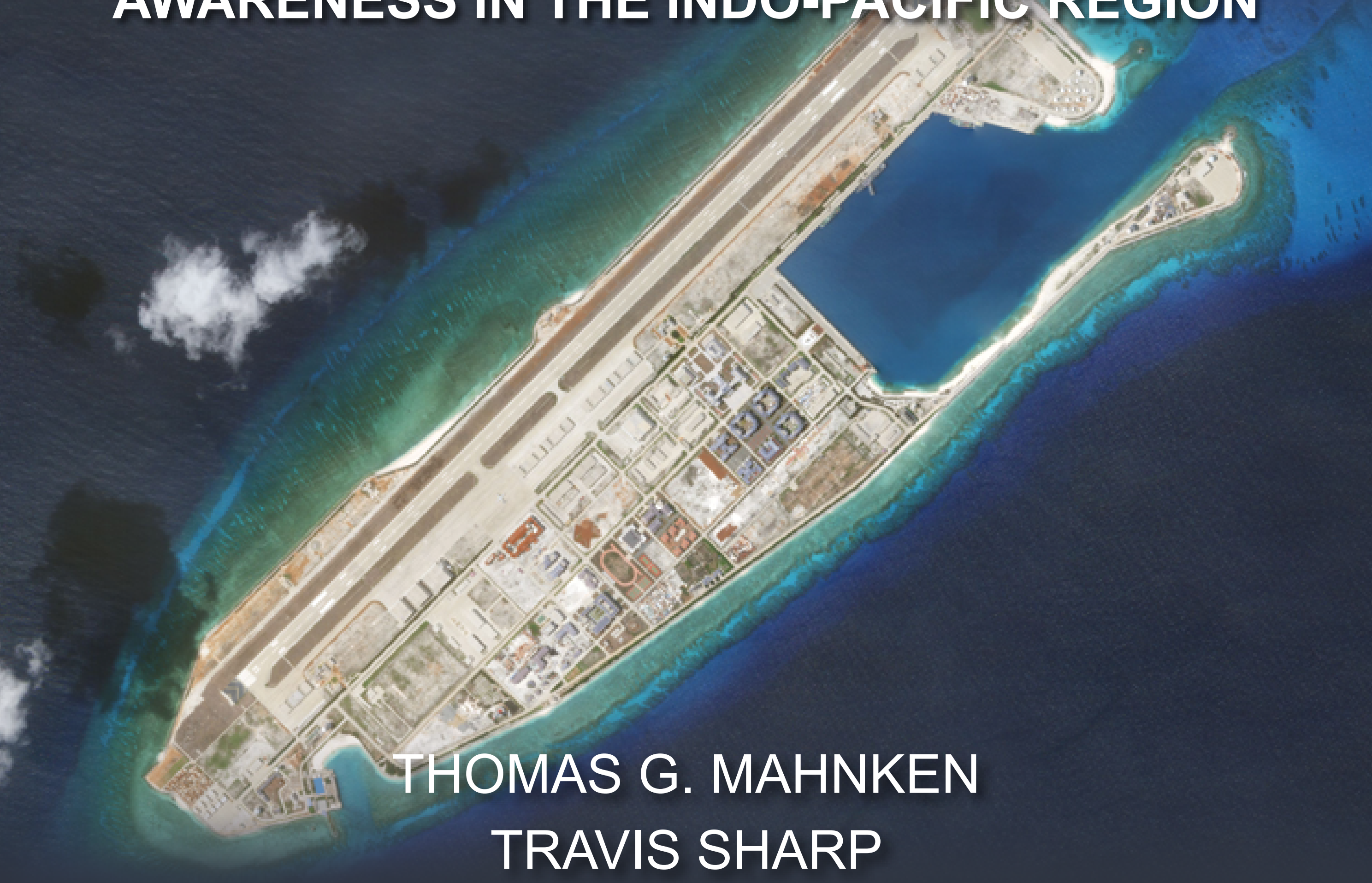
CSBA
Center for Strategic and Budgetary Assessments

IMPLEMENTING DETERRENCE BY DETECTION

INNOVATIVE CAPABILITIES, PROCESSES, AND ORGANIZATIONS FOR SITUATIONAL AWARENESS IN THE INDO-PACIFIC REGION



THOMAS G. MAHNKEN
TRAVIS SHARP
CHRISTOPHER BASSLER
BRYAN W. DURKEE

IMPLEMENTING DETERRENCE BY DETECTION

INNOVATIVE CAPABILITIES, PROCESSES, AND ORGANIZATIONS FOR SITUATIONAL AWARENESS IN THE INDO-PACIFIC REGION

THOMAS G. MAHNKEN

TRAVIS SHARP

CHRISTOPHER BASSLER

BRYAN W. DURKEE

CSBA

Center for Strategic and Budgetary Assessments

2021

ABOUT THE CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS (CSBA)

The Center for Strategic and Budgetary Assessments is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's analysis focuses on key questions related to existing and emerging threats to U.S. national security, and its goal is to enable policymakers to make informed decisions on matters of strategy, security policy, and resource allocation.

ABOUT THE AUTHORS

Thomas G. Mahnken is President and Chief Executive Officer of the Center for Strategic and Budgetary Assessments. He is a Senior Research Professor at the Philip Merrill Center for Strategic Studies at The Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS). He recently served as a member of the Congressionally-mandated National Defense Strategy Commission and as a member of the Board of Visitors of Marine Corps University. His previous government career includes service as Deputy Assistant Secretary of Defense for Policy Planning from 2006–2009, where he helped craft the 2006 Quadrennial Defense Review and 2008 National Defense Strategy. He served on the staff of the 2014 National Defense Panel, 2010 Quadrennial Defense Review Independent Panel, and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. He served in the Defense Department's Office of Net Assessment and as a member of the Gulf War Air Power Survey. He was awarded the Secretary of Defense Medal for Outstanding Public Service in 2009, and the Department of the Navy Superior Civilian Service Medal in 2016.

Travis Sharp is a Fellow at the Center for Strategic and Budgetary Assessments. He directs the defense budget studies program and works to inform policymakers, senior leaders, and the public about issues related to resourcing national security. He also serves as an officer in the U.S. Navy Reserve. He has held positions with academic and policy organizations, including George Washington University's Institute for Security and Conflict Studies, West Point's Modern War Institute, the Office of the Secretary of Defense, the Center for a New American Security, and the Center for Arms Control and Non-Proliferation. His research has appeared in *The Journal of Strategic Studies*, *Policy Sciences*, *Survival*, and *International Affairs*, among other outlets.

Christopher Bassler is Senior Fellow at the Center for Strategic and Budgetary Assessments. He previously served as the Chief Strategy Officer (CSO) for the F-35 Lightning II Joint Program Office (JPO), the Department of Defense's largest acquisition enterprise, responsible for developing and acquiring the most advanced next-generation strike aircraft weapon system for the U.S. Air Force, Marines, Navy, and many allied nations. He also previously served as Deputy Director of the Office of the Senior National Representative (SNR), in the Office of the Chief of Naval Operations, Directorate for Innovation, Technology Requirements, Test & Evaluation (OPNAV N94). Prior to that assignment, he served as the Director of the Naval Science & Technology Cooperation Program at the Office of Naval Research (ONR). Earlier in his career, Dr. Bassler held several positions at the U.S. Navy's Naval Surface Warfare Center, Carderock Division (NSWCCD), leading research projects, design studies, and teams. He has received two Navy Meritorious Civilian Service Awards, one from the U.S. Secretary of the Navy in 2014 and one from the U.S. Chief of Naval Research in 2016. He received the 2014 American Society of Naval Engineers (ASNE) Solberg Award for Research and the 2009 ASNE Rosenblatt Young Naval Engineer Award. He has published over 60 scientific papers and technical reports and has been awarded two U.S. Patents.

Bryan W. Durkee is the 2020/2021 Navy Fellow assigned to the Center for Strategic and Budgetary Assessments as a part of the Federal Executive Fellowship program. He is a current, active duty Navy Captain with over 27 years of service. As an EP-3 pilot, Bryan commanded Task Force SIX SEVEN (CTF-67) where he led the Maritime Patrol and Reconnaissance Forces for U.S. Naval Forces Europe-Africa / U.S. 6th Fleet from 2014 to 2016. He commanded the "Rangers" of Fleet Air Reconnaissance Squadron TWO (VQ-2) from 2010 to 2011 where he led deployed detachments in the 4th and 6th Fleet areas of operations. Throughout his career, he has led and flown reconnaissance missions in support of every geographic combatant command, to include participation in Operations Allied Force, Northern Watch, Enduring Freedom, Iraqi Freedom, New Dawn, Nomad Shadow, Inca Gold, Odyssey Dawn/Unified Protector, Atlantic Endeavor, Joint Forge, and Inherent Resolve.

ACKNOWLEDGMENTS

The authors thank David Zikusoka for his invaluable contributions to an earlier version of this report, as well as a series of anonymous reviewers for their comments and suggestions. They also thank Josh Chang for preparing outstanding graphics and James Mersol for editing and producing the monograph. The analysis and findings presented here are solely the responsibility of the authors. CSBA receives funding from a broad and diverse group of contributors, including private foundations, government agencies, and corporations. A complete list of these organizations can be found on our website at www.csbaonline.org/about/contributors.

Cover Graphic: Satellite imagery of Fiery Cross Reef on May 3, 2020, courtesy of SkySat. CC BY 2.0

Contents

FIGURES

CHAPTER 1

Introduction

The proposition that surveillance reduces the frequency or severity of misbehavior lies at the heart of thinking about deterrence. Deterrence could not meaningfully exist in a world where transgressors believed they could act with impunity because their misdeeds would go unnoticed and thus unpunished.[1] The fear of detection, whether before, during, or after wrongdoing, is necessary for deterrence because detection must precede retaliation, the threat of which persuades a prospective wrongdoer to behave in the first place.

The United States and its allies and partners fear that the Chinese military might act aggressively soon, including acts of coercion that fall below the threshold of armed conflict. In recent months, Chinese belligerence toward Taiwan has quickened policymaker pulses. As Admiral John Aquilino, the commander of U.S. Indo-Pacific Command, testified to Congress in March 2021 about a potential Chinese assault on Taiwan, "this problem is much closer to us than most think."[2] Analysts have debated whether China really intends to attack Taiwan and whether it could do so successfully.[3] Yet these debates do not change the fact that American and allied leaders, possessing the full range of classified intelligence, genuinely worry about near-term Chinese aggression, whether against Taiwan or against territorial features in the South China Sea or East China Sea.

The United States and its allies and partners can strengthen their near-term deterrence posture against China by increasing Beijing's fear of being detected committing an

[1] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (June 2015), pp. 316–348. During the Cold War, Thomas Schelling and other theorists frequently returned to the idea that bolstering surveillance could strengthen deterrence and preserve peace by supplying accurate information that would help dampen the reciprocal fear of surprise attack. See Thomas C. Schelling, "Arms Control: Proposal for a Special Surveillance Force," *World Politics* 13, no. 1 (October 1960), pp. 1–18.

[2] Robert Burns, "US Military Cites Rising Risk of Chinese Move against Taiwan," *Associated Press*, April 7, 2021, available at https://apnews.com/article/us-military-risk-china-move-against-taiwan-788c254952dc47de78745b8e2a5c3000.

[3] Robert D. Blackwill and Philip Zelikow, "Can the United States Prevent a War over Taiwan?" *War on the Rocks*, March 1, 2021, available at https://warontherocks.com/2021/03/can-the-united-states-prevent-a-war-over-taiwan/.

infraction. To help achieve that objective, this report proposes a refined version of an operational concept, "Deterrence by Detection," previously developed by CSBA.[4] The original concept recommended employing existing non-stealthy long-endurance unmanned aircraft systems (UAS) to surveil key geographic areas in the Western Pacific and Eastern Europe. This report's refined concept focuses on situational awareness in the Indo-Pacific theater as an illustrative scenario, although the concept and analysis have applicability elsewhere.

The report proposes that the United States and its allies strengthen surveillance of potential Chinese military operating areas by:

1. employing the entire spectrum of existing ISR capabilities, not just UAS, supplemented by select investments in key technology enablers;

2. improving ISR processes, primarily by using artificial intelligence (AI) to automate specific collection and processing tasks, to maximize the returns from existing ISR capabilities; and

3. adopting a "neighborhood watch" approach, primarily via adapting existing organizational structures, with additional capacity to conduct coalition situational awareness operations in the Indo-Pacific theater.

The report's central argument is that the United States and its allies should fully leverage existing ISR capabilities by boosting their performance with technology enablers, streamlining processes with AI, and improving regional military coordination. Policymakers should not discard existing ISR platforms prematurely in a rush to buy all-new capabilities, although augmenting the platforms with new capabilities will prove necessary and should support a longer-term evolutionary approach to the architecture. Fully leveraging existing ISR capabilities will strengthen nearer-term deterrence against China while holding down costs, an attractive option given tightening U.S. defense budgets.

Consistently improving existing ISR capabilities will ensure that they remain relevant to the military missions emphasized in the 2018 National Defense Strategy (NDS).[5] Tying existing ISR capabilities to priority NDS missions will prevent policymakers from mistakenly branding them as "legacy" systems suitable for elimination due to perceived operational irrelevance.[6]

[4] Thomas G. Mahnken, Travis Sharp, and Grace B. Kim, *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition* (Washington, DC: Center for Strategic and Budgetary Assessments, April 2020).

[5] Department of Defense (DoD), *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DoD, January 2018).

[6] Thomas G. Mahnken and Christopher Bassler, "What Is a Legacy System? The Key Is Relevance, Not Age," *Defense News*, February 22, 2021, available at https://www.defensenews.com/opinion/commentary/2021/02/22/what-is-a-legacy-system-the-key-is-relevance-not-age/.

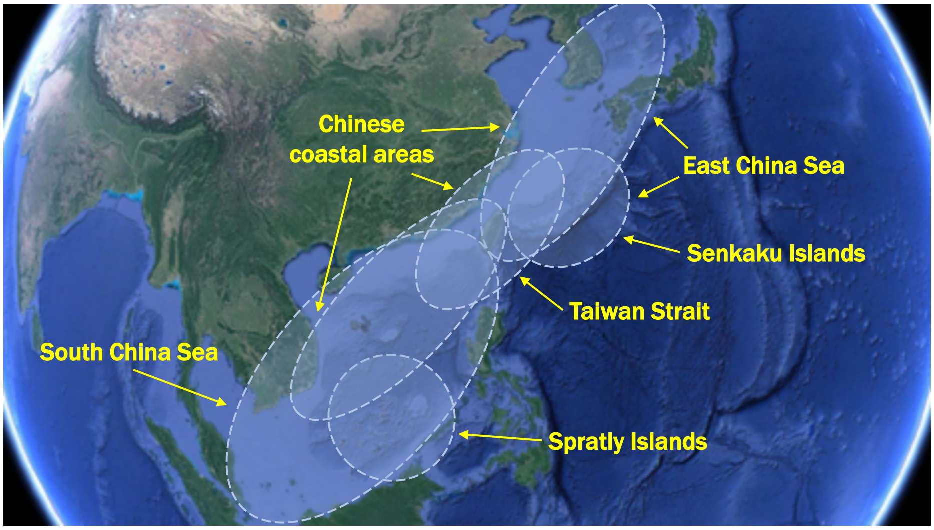
On the contrary, the Department of Defense (DoD) can use existing ISR systems to evaluate new technologies, concepts, and organizations under operational conditions. Existing ISR capabilities can function as a testing ground for building and validating next-generation ISR architectures, providing operationally relevant insights for designing future requirements. In this way, existing ISR systems can help reduce risk in the next generation of ISR capabilities.

This introductory chapter summarizes the original Deterrence by Detection concept and the refinements proposed in this report. It then connects the concept to the larger strategic issue of deterrence timing—the dilemma of whether to prioritize nearer-term deterrence or longer-term deterrence against a rising rival. Finally, it outlines the ensuing chapters to preview what follows.

Original Deterrence by Detection Operational Concept

First introduced by CSBA in April 2020, the Deterrence by Detection concept proposed establishing a network of existing non-stealthy long-endurance UAS to maintain real-time, persistent situational awareness in key geographic areas in the Western Pacific and Eastern Europe. In the Western Pacific, the Deterrence by Detection concept envisions establishing a network of UAS to increase coverage of the Taiwan Strait, East China Sea, South China Sea, and coastal areas of mainland China (**Figure 1**). In the Taiwan Strait, UAS would monitor the approaches to Taiwan, provide periodic surveillance of China's coastline, and surveil the waters farther to the east. Nearby in the East China Sea, UAS would continuously monitor the approaches to the Senkaku Islands. Coverage of the South China Sea would remain periodic and include broad coverage of an area of roughly 260,000 nm^2 as well as focused coverage of the Spratly Islands, which stand at the center of multiple territorial claims.

FIGURE 1: WESTERN PACIFIC UAS ORBITS IN DETERRENCE BY DETECTION



Source: CSBA

CSBA analysis showed that implementing Deterrence by Detection would require 46 airframes in the Western Pacific assigned to key geographic areas. The UAS would come from U.S., allied, and partner country inventories and operate in national groups and potentially as part of a coalition network. Western Pacific operations would require allocating additional medium-altitude long-endurance (MALE) UAS from existing inventories to provide persistent presence over the localized flashpoints of the Taiwan Strait, Spratly Islands, and Senkaku Islands. The Western Pacific's ocean environs also would demand allocating additional maritime-optimized high-altitude long-endurance (HALE) UAS from existing inventories. The annual operating cost for the 46 UASs would total approximately $700 million based on Congressional Budget Office figures.[7] Since the aircraft would come from the existing inventory, not from new purchases, the operating cost represents money the United States and its allies would spend anyway to keep the aircraft flying. Split among the United States and its many allies and partners in the Western Pacific, the estimated cost per country should remain affordable relative to the expected security gains.

Allies and partners would play an important role in implementing Deterrence by Detection, both as operators of UAS within regionally focused networks and as consumers of the data they collect. Since Deterrence by Detection would mainly—though not exclusively—rely upon unarmed or defensively configured UAS, the concept would appeal to allies and partners who may be concerned that operating offensively configured UAS from their territories could further exacerbate tensions with China. U.S. allies could invest further in UAS capabilities by increasing the number of existing long-endurance UAS in their inventories, whether they are U.S. made or domestically produced, and by investing in longer-range strategic sensors and resilient command and control (C2). Other countries could also invest in similar capabilities, further enhancing Deterrence by Detection.

The Deterrence by Detection concept rests on two logics: the deterrent effect of surveillance with attribution and the efficiency effect of repurposing existing systems.

- **Deterrence**: A potential adversary will be less likely to attempt an opportunistic act of aggression if it believes the United States and its allies surveil the adversary persistently, particularly if that surveillance captures granular "pattern of life" data on the adversary's military activities. Persistent surveillance raises doubt in adversary leaders' minds that they can prepare for and execute a military operation without being either detected in advance, giving the U.S. alliance time to thwart the operation militarily and diplomatically, or exposed in retrospect, reducing the aggressor's odds of escaping culpability and achieving a *fait accompli*.[8] In addition, existing long-endurance UAS provide a highly

[7] The $700 million figure halves the estimated cost for 92 airframes included in the original report. Mahnken, Sharp, and Kim, *Deterrence by Detection*, pp. ii–iii.

[8] Empirical analyses show that deterrence is more likely to fail when an aggressor believes it can pull off a *fait accompli* successfully. Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), pp. 536–547.

visible signal of the U.S. alliance's commitment to surveillance, in contrast to other surveillance capabilities.

- **Efficiency**: The United States and its allies will conserve resources by repurposing existing UAS to new missions rather than procuring new UAS to perform those roles. Existing UAS mainly have operated over the more permissive battlefields of the Middle East. They would face a highly contested environment during any future conflict involving China. Since the aircraft would primarily perform their missions before the outbreak of major hostilities, however, they do not require stealth capabilities to prove effective. In fact, their very visibility will help bolster deterrence. Furthermore, using existing UAS for persistent, wide-area ISR missions will free up other ISR platforms, both manned and unmanned, to perform other tasks for which they are uniquely suited. Platforms should complement one another to enhance the overall capability of the network. For example, HALE platforms provide important wide-area surveillance that can cue MALE platforms to maintain dwell time through local orbits over targets of interest or more rapidly prosecute them.

Refined Deterrence by Detection Concept

This report builds upon the Deterrence by Detection concept in three ways. First, it broadens the concept to incorporate the full range of existing unmanned ISR capabilities across all domains. Focusing narrowly on existing UAS made sense initially because the systems have assumed symbolic importance in the debate over how the U.S. military should adapt to great power competition.[9] The United States and its allies ought to reap the benefits of the full range of existing unmanned ISR capabilities by making select investments in key technology enablers that can help boost performance without breaking the bank. This approach permits the maximum use of existing forces while also making selective investments to ensure their resiliency. Establishing a multi-domain system of systems for Deterrence by Detection would involve combining existing military assets with increasingly proliferated and available commercial assets.

Second, the report deepens the Deterrence by Detection concept by going beyond ISR capabilities and identifying ISR processes—specifically collection and processing—that could be improved via AI-enabled automation to maximize the returns provided by existing ISR capabilities. Making small investments to improve suboptimal processes would allow these capabilities to reach their full potential and potentially reduce the manpower associated with maintaining those capabilities, freeing up funds to invest in new technologies. Improving processes to offload certain complex tasks to machines would also cost far less than buying entirely new capabilities and would promote tighter integration between the United States and its allies.

[9] Andrew Metrick, "Bad Idea: UAVs Aren't Usable in Contested Environments," Center for Strategic and International Studies, December 4, 2017, available at https://defense360.csis.org/bad-idea-uavs-contested-environments/.

Third, the report proposes an organizational structure for implementing the Deterrence by Detection concept. Applying the neighborhood watch concept, Deterrence by Detection would combine information derived from the full range of existing ISR capabilities with enabling technologies and concepts, including the proposed AI-enabled improvements to intelligence collection and processing. Regional multi-domain fusion centers would provide the core of the Deterrence by Detection neighborhood watch. The centers would support the foundational principles of the United Nations Convention on the Law of the Sea (UNCLOS) for open and transparent maritime security.

Tying Concept to Strategy: Dilemma of Deterrence Timing

The Deterrence by Detection concept ties into a larger strategic issue. The United States faces a dilemma as it evaluates options for adjusting its deterrence posture toward China. The same dilemma has confronted other great powers who faced a rising rival and operated under constrained resources: should a great power emphasize strengthening its deterrence posture in the nearer term, when its rival is less powerful but perhaps more impetuous militarily, or in the longer term, when it is more powerful but perhaps less impetuous militarily?[10] Put differently, when is the optimal time to confront a rising rival with peak deterrence: now or later?

The dilemma exists for two reasons. First, deterrence adjustments entail opportunity cost in the sense of foregone opportunities. A dollar spent conducting a large-scale exercise to maintain current readiness is a dollar that cannot be spent researching technologies that will propel future long-range missiles. The reverse also holds true: Funds committed to improving nearer-term deterrence, which potentially lowers the probability of conflict today when the rising rival is weaker, become unavailable for improving longer-term deterrence, which potentially raises the probability of conflict tomorrow when the rising rival is stronger.

Second, deterrence adjustments entail risk in the sense of an investment's actual performance lagging its projected performance. As one example, a U.S. deterrence posture oriented toward futuristic weaponry might fail to overawe a Chinese leader predisposed to viewing U.S. legacy forces as the *sine qua non* of military power.[11] As another example, bolstering U.S. military strength today might unintentionally signal hostile future intent if

[10] For discussion of how the psychology of time horizons affects coercion, see Ronald R. Krebs and Aaron Rapport, "International Relations and the Psychology of Time Horizons," *International Studies Quarterly* 56, no. 3 (September 2012), pp. 530–543.

[11] The two best empirical analyses of this hypothesis are Barry M. Blechman and Stephen S. Kaplan, eds., *Force without War* (Washington, DC: The Brookings Institution, 1978); and David E. Johnson, Karl P. Mueller, and William H. Taft, *Conventional Coercion Across the Spectrum of Operations: The Utility of U.S. Military Forces in the Emerging Security Environment* (Santa Monica, CA: RAND Corporation, 2003).

China earnestly seeks security, triggering a security dilemma in which every move triggered a rival countermove, reducing net security for both.[12]

Policymakers cannot easily avoid the dilemma of deterrence timing. Military planners might seek to smooth or balance risk over time, avoiding what they might consider a false choice between prioritizing deterrence now or later. Yet democratic political leaders face an omnipresent near-term consideration, i.e., winning reelection, which incentivizes them to privilege today over tomorrow.[13] The fierce urgency of "now" felt by politicians attenuates a democracy's ability to spread risk smoothly over time.

Strategic intelligence might push decision makers toward nearer-term deterrence or longer-term deterrence if it pinpointed a period of peak danger. Yet intelligence professionals know that such assessments prove fraught, not least because the assessments often disagree about the peak danger period. The focus of Marine Corps planning documents on reshaping the force for a potential conflict in 2030 versus the focus of Air Force planning documents on its operating concepts in 2035 illustrates the point.[14] Additionally, policymakers frequently distrust strategic intelligence assessments or react to them too slowly.[15]

Reliance on allies to carry greater shares of the collective deterrence burden, whether now or later, might inform when to prioritize one's own efforts. Yet democracies typically ally with other democracies, meaning allied governments suffer from the same politics-driven present bias that disrupts balancing risk over time. Allies also frequently view potential threats and appropriate responses somewhat differently, placing each ally in the precarious position of wagering its own security on its allies' present and future actions.[16] In sum, the United States will continue to face the dilemma of deterrence timing as it adjusts its defense policy toward China in the years ahead.

How Deterrence by Detection Limits Cost and Risk

The refined Deterrence by Detection concept balances nearer-term and longer-term deterrence—thereby easing the dilemma of deterrence timing—by limiting cost and risk. In terms of cost, the concept employs existing ISR capabilities rather than requiring new platform purchases, thereby minimizing the large opportunity costs associated with new

[12] A classic assessment is Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978), pp. 167–214.

[13] Authoritarian leaders worry about retaining power, too. Bruce Bueno de Mesquita et al., *The Logic of Political Survival*, first paperback edition (Cambridge, MA: The MIT Press, 2005).

[14] U.S. Marine Corps, *Force Design 2030* (March 2020), available at https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460; and U.S. Air Force, *Air Force Future Operating Concept: A View of the Air Force in 2035* (September 2015), available at https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.

[15] Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, DC: Brookings Institution Press, 1982).

[16] Mancur Olson, Jr. and Richard Zeckhauser, "An Economic Theory of Alliances," *The Review of Economics and Statistics* 48, no. 3 (August 1966), pp. 266–279.

acquisitions. Implementing the concept will require paying operating costs to maintain existing systems but not paying development and procurement costs to field new systems. Therefore, implementing the concept should not require any major spending increases above the current budgetary programs of record, except for some targeted investments in specific technology enablers and process improvements. By minimizing the need for funding increases while still strengthening surveillance in the Indo-Pacific region, Deterrence by Detection conserves resources to invest in longer-term deterrence while simultaneously fortifying nearer-term deterrence. In short, Deterrence by Detection aims to let the United States and its allies have their cake and eat it too by reinforcing nearer-term deterrence without undermining longer-term deterrence.

Over time, the aging of existing ISR systems may cause their operating costs to grow excessively, incurring higher opportunity costs. At that point, the United States and its allies should retire the systems and field next-generation replacements in accordance with the typical modernization process. Ideally, the United States and its allies would field the new systems before the costs became unaffordable. The report's argument, however, is that policymakers should not discard existing ISR capabilities prematurely in a rush to buy all-new capabilities due to a mistaken belief that existing capabilities cannot help deter China. The Deterrence by Detection concept illustrates that existing ISR capabilities will remain operationally relevant in the Indo-Pacific region for the foreseeable future.

In terms of risk, the Deterrence by Detection concept concerns the observational aspect of deterrence, not its retaliatory aspect. Most risks stem from the latter. To revisit the previous examples, a robust surveillance posture is required to deter Chinese leaders regardless of whether they regard futuristic U.S. weaponry or legacy U.S. forces as the more credible threat. Additionally, bolstering surveillance of areas outside a rival's territory, such as adjacent international waters, signals less of a hostile future intent than alternative deterrence options such as fielding offensive weaponry.[17] Chinese leaders could attempt to portray increased surveillance as hostile, particularly if they labeled it a precursor to offensive action.[18] On balance, however, it seems unlikely to provoke escalatory security dilemma dynamics. After all, the United States and China currently conduct extensive surveillance, but it has not consistently led to escalation. By strengthening the observational activities undergirding deterrence, not the subsequent retaliatory activities, Deterrence

[17] The same cannot be said of surveilling a rival's territory. As John Lewis Gaddis noted, "There was, to be sure, little in the history of great power rivalries to suggest that nations might willingly allow potential adversaries to reconnoiter their territories," although the United States and Soviet Union did develop regimes that permitted such reconnaissance. John Lewis Gaddis, "The Evolution of a Reconnaissance Satellite Regime," in Alexander L. George, Philip J. Farley, and Alexander Dallin, eds., *U.S.-Soviet Security Cooperation: Achievements, Failures, Lessons* (New York: Oxford University Press, 1988), p. 353.

[18] Mark J. Valencia, "US-China Race for Surveillance Supremacy in South China Sea Risks a Needless Clash," *South China Morning Post*, May 14, 2021, available at https://www.scmp.com/comment/opinion/article/3133329/us-china-race-surveillance-supremacy-south-china-sea-risks-needless.

by Detection improves nearer-term deterrence but sidesteps the risks of misjudging or provoking potential Chinese responses that could erode longer-term deterrence.

The primary risk of Deterrence by Detection concerns the possibility that existing ISR capabilities cannot provide sufficient surveillance, in terms of coverage and duration, of Chinese military activities to uphold deterrence. For instance, consider a scenario in which China conducted military movements in a deliberate attempt to probe whether the United States and its allies could detect the activity. If Chinese leaders received no indication that the U.S. alliance detected their moves, they might infer that their activity went unobserved. They might then gain confidence that they could execute such movements without triggering a U.S. or allied response during a future assault.

Since neither ISR systems nor the humans directing them are foolproof, military planners can never eliminate the risk of detection failure, even with persistent coverage of a particular geographic area. However, the United States and its allies can use information disclosures, public statements, and other tools to reduce Chinese leaders' confidence in their ability to evade detection, thereby reducing their willingness to attempt military action. To draw an analogy with nuclear arms control verification, the United States and its allies should aspire not to perfect detection but effective detection, such that if China moved "in any militarily significant way, we would be able to detect the violation in time to respond effectively and, thereby, deny […] the benefit of the violation."[19] Effective detection represents a realistic goal for Deterrence by Detection.

Chapter Roadmap

The chapters ahead further develop these themes. Chapter 2 discusses how planners can leverage military and selected commercial assets fielded today to begin integrating a multi-domain system of systems to deliver persistent ISR, influence adversary behavior, and enhance common understanding among allies and partners in the Indo-Pacific region. Chapter 3 contends that harnessing AI to improve existing ISR processes will maximize the returns from existing ISR capabilities, fueling the Deterrence by Detection operational concept. Chapter 4 ties everything together by proposing a neighborhood watch approach to maintaining situational awareness in the Indo-Pacific theater. Finally, Chapter 5 concludes by summarizing the implications for policy and future research. The Appendix profiles some of the existing systems that would support the near-term implementation of the Deterrence by Detection architecture.

[19] Paul H. Nitze, "Security Challenges Facing NATO in the 1990s," remarks to the Nobel Institute's Leangkollen Seminar, Oslo, Norway (Washington, DC: Department of State, February 1989), p. 4.

CHAPTER 2

Establishing a Multi-Domain System of Systems

The United States and its allies and partners should strengthen surveillance of nefarious activities, from illegal fishing to intimidation and coercion to military preparations, by networking existing ISR platforms in key operating areas and augmenting their capabilities with select investments in technology enablers. These investments should aim to expand the integration, distribution, and consumption of data that this persistent, long-dwell, multi-domain system of systems will produce. This approach seeks to maximize the return on investment from assets and platforms that have already been developed and are currently operating. Such a multi-domain system of systems approach will yield a better understanding of Chinese military activities in the Western Pacific and beyond.

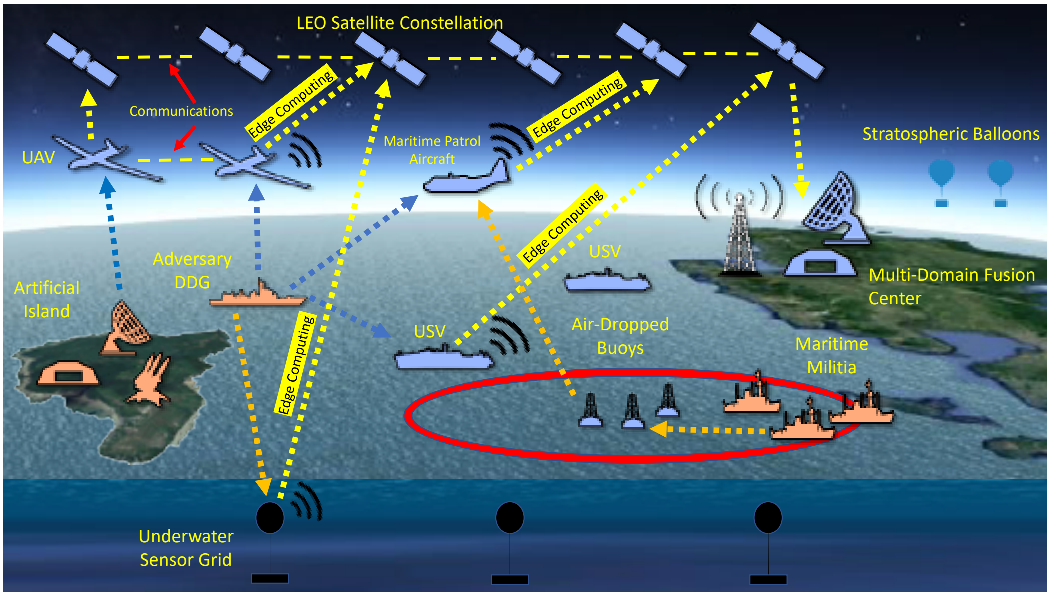
As detailed in the Appendix, a multi-domain system of systems would include both existing military assets and increasingly proliferated and available commercial assets. These systems, spanning the air, maritime, and space domains, include military UASs and balloons, unmanned surface vessels, buoys and gliders, undersea research networks, and space-based commercial and small satellite payloads.

Expanding the ISR Capabilities Included in Deterrence by Detection

The Deterrence by Detection concept focused initially on existing UAS due to their prominence in contemporary debates about America's defense posture. However, the logics of deterrence and efficiency embodied in the original concept also apply to ISR capabilities in other physical domains. The United States and its allies ought to get the full benefit from existing ISR capabilities, making select investments in key technology enablers to boost their performance without large additional expenditures in funding, manpower, and time. Multi-domain ISR strengthens resilience through a system of systems approach. By creating and maintaining an open ecosystem, the United States, its allies, and key partner nations can use existing platforms, integrated into a multi-domain approach, and layer in additional commercial collections.

The keys to operationalizing Deterrence by Detection are fusing various data streams and disseminating the resulting information efficiently and securely. Making the information as accessible as possible will increase coordination among allies. A combination of systems will create a suite of capabilities to discover the ground truth about adversary activities, even in the face of dedicated efforts to obscure them. Fielding an integrated system of systems that uses self-forming, self-healing, ad-hoc mesh networks would allow friendly forces to communicate and exfiltrate data even in the face of an adversary's attempts to interfere with the network's operations.[20]

FIGURE 2: IMPLEMENTING DETERRENCE BY DETECTION WITH EXISTING SYSTEMS



Source: CSBA

This multi-domain system of systems can provide persistent coverage of areas of interest, becoming part of the strategic and operational environment over time. Through persistent data collection, the system of systems can establish patterns of life and provide tipping and cueing for other platforms. The architecture will enable increased data collection and absorption, helping U.S. and allied leaders and operational commanders detect changes and monitor complex situations as they unfold. It will also help observe these activities

[20] Versions of these technologies have been fielded and used operationally for nearly a decade. Key elements include logic protocols to self-default to backup systems and pathways when a preferred option (e.g. SATCOM) is no longer available for a period of time.

more clearly to allow leaders to calibrate the deployment of personnel and platforms against China's Fabian strategy of incursions into international and sovereign territories.

A wide array of sensors and corresponding platforms will contribute to the broader mission of developing persistent situational awareness, with assets both collaborating and specializing in covering specific domains and executing specific tasks. A discussion of the existing platforms that could support the architecture for the Deterrence by Detection concept appears in the Appendix.

Key Enablers: Integrating Existing Platforms with Urgency

Several enabling technologies will play a key role in increasing the value of existing platforms. All the technologies discussed below already exist and are in varying stages of fielding. These critical enablers include:

- Line-of-sight communications, such as laser communications, among and between layers to allow large amounts of data to move quickly;
- Computing at the tactical edge to support a distributed and multi-level tasking, collection, processing, exploitation, and dissemination (TCPED) architecture featuring both multi-static, sensing within and across domains and ad-hoc mesh networks; and
- Artificial intelligence and machine learning (AI/ML) approaches to allow a single crew to identify multiple targets and control multiple orbits of systems, inverting much of the current operational paradigm of large ground crews and operators for each individual system.[21]

Line-of-Sight Communications

High-capacity line-of-sight communications, including laser communications systems, can quickly transfer large amounts of data among platform nodes, whether within domains or across them, and back to fusion centers or control nodes. Optical-based communications such as digital screen displays (or digital semaphore technology) can include liquid crystal display screens displaying QR codes.[22] Platforms with electro-optical (EO) sensors and equipped with QR code readers can then read the information, including encrypted messages, intelligence, and tasking revisions.[23]

[21] Enhancements to some operational systems have reportedly allowed one ground station crew of operators and processors to scale up from supporting a single system to now supporting five orbits simultaneously, with technical feasibility and plans calling for achieving even higher ratios of ground station crews to orbits in the near future.

[22] Andy Lucas et al., *Digital Semaphore: Using QR Code Signaling for Robot and Fleet Use* (Monterey, CA: Naval Postgraduate School, June 1, 2013), pp. 5, 11–12.

[23] Ibid., pp. 27–29.

Distributed Computing

Computing power will need to perform processing, exploitation, and dissemination (PED) of the data collected for users, preparing that data in standard and actionable formats. Cloud and edge-based computing approaches can help satisfy these demands. By combining onboard portable edge computing with an infrastructure-intensive backbone of high-powered server farms, analysts can leverage advanced analytics, deep learning, and artificial intelligence previously unavailable to users outside the scientific supercomputing community. Individual systems and platforms within a Deterrence by Detection multi-domain system of systems must blend onboard processing power with data transmission pathways and bandwidth, with fusion occurring across multiple assets and domains and at key geographic locations.

One example of extensible, portable edge-computing applications is the current Air Force Research Lab (AFRL) effort with industry to develop and integrate flight-capable, podded high-performance computing (HPC) capabilities.[24] By handling complex AI and ML tasks onboard a long-endurance UAS, systems like AFRL's Agile Condor (described further in Chapter 3) can process, exploit, and disseminate collections with minimal or no human intervention. Such systems also can reduce overall capacity demand on communications networks, allowing only collections of interest, also known as reduced-form raw data, to be forwarded to other nodes in the architecture and eventually to human operators. Notably, AFRL seeks to make the processing capability of HPC pods available to other collection platforms within communication range, including other UAS and satellites. A future Deterrence by Detection system of systems that includes HPC could reduce the overall computational burden and resulting data transmission requirements across the system of systems.

Artificial Intelligence and Machine Learning

Machines can help reduce the TCPED burden generated from wide-area, high-resolution, continuous collection, especially using pattern-recognition machine learning algorithms. A breakthrough moment in the AI field occurred in January 2012 when a Canadian researcher entered his algorithm, AlexNet, into the ImageNet Large-Scale Visual Recognition Challenge.[25] AlexNet used a neural network approach to recognize and classify visual images at a speed much faster than ever achievable by human users. Using machine learning algorithms for pattern recognition and change detection, especially from persistent long dwell times, can reduce the number of analysts required and allow them to pursue

[24] SRC, "Agile Condor High-Performance Embedded Computing," accessed April 23, 2021, available at https://www.srcinc.com/products/intel-collection-and-analysis/agile-condor-high-performance-embeded-computing.html; and Frank Wolfe, "Testing Begins for Condor Pod to Enable AI-Powered MQ-9 Reaper Targeting," September 14, 2020, available at https://www.aviationtoday.com/2020/09/14/testing-begins-condor-pod-enable-ai-powered-mq-9-reaper-targeting/.

[25] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton, "ImageNet Classification with Deep Convolutional Neural Networks" *Advances in Neural Information Processing Systems* 25, no. 2 (January 2012), pp. 1097–1105.

higher-value tasks while monitoring developments identified by the algorithms. Algorithms can also aid in the fusion process to strip particular identifiers from data sets, making them source agnostic for some users while retaining some metadata for interrogation if required. Permissions-based security access can also help partition elements of the Deterrence by Detection system of systems to various users who may wish to consume outputs from the distributed, multi-domain architecture. Lastly, fusion algorithms can combine multiple data streams from different layers and nodes in the architecture to achieve optimal awareness based on available platforms and locations.

Conclusion

Integrating the constellation of systems that already exist will provide an immediate opportunity to leverage existing capabilities and operate tailored persistence on demand. By leveraging key parts of the force structure, the United States and its allies will create an overall system of systems architecture that is not only persistent and extensible but also adaptable. Operations and experimentation will help inform the design of future elements, including platform-agnostic payloads (such as multi-function UAS pods or containerized systems for marine platforms) and payload-agnostic platforms in which sufficient space, weight, power, cooling footprint, and established interfaces will allow for customization when desired.

CHAPTER 3

Improving ISR Processes by Incorporating Artificial Intelligence

Many technology leaders have predicted that artificial intelligence (AI) "will revolutionize the practice of intelligence," as stated in the March 2021 final report by the National Security Commission on Artificial Intelligence (NSCAI).[26] The Washington-based defense policy community can be forgiven for believing the era of AI-supported intelligence analysis has nearly arrived.[27] After all, think tank reports, news articles, and marketing brochures frequently claim that the future is now.[28] Yet an AI revolution still feels impossibly far away for today's frontline U.S. intelligence analyst enduring the sheer drudgery of incompatible databases, email-based workflows, and manually built PowerPoint slides.[29] Although AI has streamlined some processes, its potential remains almost entirely unrealized as far as rank-and-file analysts are concerned. As government intelligence analyst Brian Katz

[26] National Security Commission on Artificial Intelligence (NSCAI), Final Report (March 2021), p. 23, available at https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[27] For a primer on AI technology in a defense context, see Greg Allen, *Understanding AI Technology* (Washington, DC: DoD Joint AI Center, April 2020), available at https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.

[28] John Speed Meyers and David Jackson, "The Faultline between Futurists and Traditionalists in National Security," *War on the Rocks*, January 18, 2021, available at https://warontherocks.com/2021/01/the-faultline-between-futurists-and-traditionalists-in-national-security/.

[29] Artificial intelligence (AI) is "the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems." Machine learning (ML) is a subfield of AI focused on developing applications that learn from data and become more accurate over time without being programmed to do so. Department of Defense (DoD), *Summary of the 2018 Department of Defense Artificial Intelligence Strategy* (February 2019), p. 5, available at https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

observed, "The analyst of 2020 has neither the time nor inclination to ponder this seemingly fantastical future."[30]

This chapter contends that leveraging AI to improve existing ISR processes will maximize the returns from existing ISR capabilities and enable the Deterrence by Detection operational concept. In contrast to studies contemplating an idealized AI future, the chapter emphasizes current intelligence practice to illustrate how much the intelligence community could gain—and how far it still must go—to incorporate AI. The potential gains justify continuing to strive for progress. Improving existing ISR processes through AI-enabled automation promises to yield more effective and efficient intelligence analysis in the long run.[31] According to one estimate, at-scale enterprise adoption of AI-enabled systems could save each all-source intelligence analyst as much as 364 hours (45 days) per year, freeing up that time for other tasks, such as assessing the vast amount of collected data that currently goes unanalyzed or completing additional training.[32]

The chapter focuses on applying AI to two steps in the intelligence cycle—collection and processing—because AI seems most likely to benefit those steps initially.[33] In line with this report's focus, the chapter invokes scenarios involving situational awareness in the Indo-Pacific theater. For evidence, the chapter draws on published reports, news articles, and the report authors' personal experiences serving in and around the intelligence apparatuses of the U.S. Navy and the Department of Defense.[34] The chapter embraces the perspective of the intelligence analyst working in support of military operations, as opposed to the many other roles within the intelligence enterprise, because the analyst is the primary consumer of military-focused ISR data and thus the primary victim of suboptimal ISR processes.

[30] Brian Katz, *The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis* (Washington, DC: Center for Strategic and International Studies, October 2020), p. 1, available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201008_Katz_Analytica_Edge_0.pdf.

[31] Andrew Eversden, "JAIC Director: With Flat Budgets, Turn to AI to Save Money," *C4ISRnet.com*, April 9, 2021, available at https://www.c4isrnet.com/artificial-intelligence/2021/04/09/jaic-director-with-flat-budgets-turn-to-ai-to-save-money/.

[32] Kwasi Mitchell et al., "The Future of Intelligence Analysis: A Task-Level View of the Impact of Artificial Intelligence on Intel Analysis," *Deloitte Insights*, December 11, 2019, pp. 4–5, available at https://www2.deloitte.com/content/dam/insights/us/articles/6306_future-of-intel-analysis/DI_Future-of-intel-analysis.pdf.

[33] Hampel-Arias and Meyers argue that AI most likely will aid collection, processing, and analysis. The chapter concurs with their hypothesis but restricts its scope to collection and processing because, as they note, many analysis tasks lie "beyond the purview of machine learning." Zigfried Hampel-Arias and John Speed Meyers, "What AI Can and Cannot Do for the Intelligence Community," *Defense One*, January 5, 2021, available at https://www.defenseone.com/ideas/2021/01/what-ai-can-and-cannot-do-intelligence-community/171195/. For further discussion of AI's limited applicability to strategic analysis, see Puong Fei Yeh, "The Case for Using Robots in Intelligence Analysis," *Studies in Intelligence* 59, no. 4 (Extracts, December 2015), p. 5, available at https://www.cia.gov/static/2bb716655b81bbd602d90eea9e155fd0/Case-for-Using-Robots.pdf.

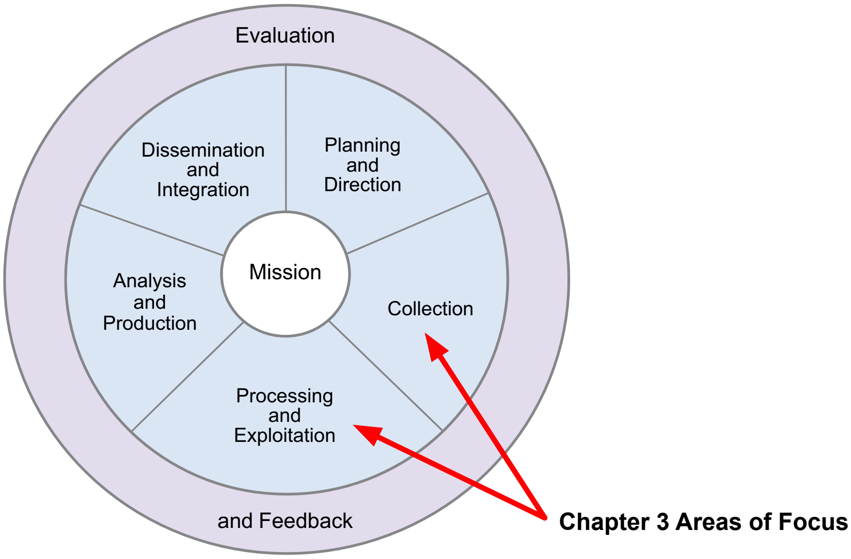
[34] Using as evidence unclassified material and personal experience may not necessarily capture all aspects of current practice within the intelligence community. This data collection challenge is both typical and inescapable for scholars producing unclassified research on intelligence matters.

Collection

Current Process Challenges

In intelligence usage, collection refers to acquiring information and then providing it to processing elements.[35] Current collection practices require humans to perform various labor-intensive and often tedious tasks, consuming precious manhours and permitting human error to befoul outcomes. The challenges begin with the staffing process. Many collection managers track intelligence collection requirements using Excel spreadsheets emailed each day to hundreds or even thousands of recipients.[36] The spreadsheets convey the breadth of activity but provide only snapshots in time, failing to capture dynamic updates. Surprisingly, this workflow prevails even in more technical intelligence disciplines (known as "INTs") such as geospatial intelligence (GEOINT) and signals intelligence (SIGINT). In these fields, making one keystroke error when manually inputting a long alphanumeric sequence could initiate collection over the wrong target, squandering a high-demand ISR capability. Collection managers do their best to call out updates and catch errors, but the spreadsheet-centric process does not lend itself to dynamic updating or surefire precision.

FIGURE 3: THE INTELLIGENCE CYCLE



Source: Joint Publication 2-0

[35] DoD, *Joint Publication 2-01: Joint and National Intelligence Support to Military Operations* (July 5, 2017), p. GL-8, available at https://fas.org/irp/doddir/dod/jp2_01.pdf.

[36] Two of the best unclassified analyses of ISR collection management are Jason M. Brown, *Strategy for Intelligence, Surveillance, and Reconnaissance*, AFRI Paper 2014-1 (Maxwell, AL: Air University Press, December 2014), available at https://media.defense.gov/2017/Jun/19/2001765010/-1/-1/0/AP_2014-1_BROWN_STRATEGY_INTELLIGENCE_SURVEILLANCE_RECCONNAISSANCE.PDF; and Daniel Elliott Sartin, "Intelligence, Surveillance, and Reconnaissance Collection Management Training: A Case for Standardization," M.A. thesis, Angelo State University, May 2019, available at https://asu-ir.tdl.org/bitstream/handle/2346.1/30929/SARTIN-THESIS-2019.pdf?sequence=1&isAllowed=y.

In another challenging staffing process, each day many collection managers manually build and brief one PowerPoint slide, known as the "ISR Sync Matrix," which summarizes how an operational unit intends to allocate collection assets and resources across targets and time.[37] The sync matrix briefing usually represents the commander's primary engagement with ISR operations each day. It therefore provides an important opportunity to receive high-level feedback on both planning and performance. Unfortunately, as with managing requirements via Excel, briefing ISR operations via PowerPoint does not readily guard against errors or convey last-minute changes, such as shifting an aircraft's time on station (or "VUL" for vulnerability window) due to weather or maintenance issues. Again, precision and dynamic updating remain elusive.

Besides staffing challenges, collection operations processes also suffer from shortcomings. One of the four principles of collection management is to task available organic collection assets first before requesting resources controlled by other organizations.[38] This principle supports how proficient militaries push problem-solving—or in this case, requirement fulfilling—down to the lowest tactical echelon possible. However, in practice, tasking available organic assets first presents problems because asset availability is not always self-evident. An asset becomes available whenever it has fulfilled its collection requirements. Unfortunately, managers and analysts often use crude rules of thumb to approximate fulfillment, such as time on target or portion of total VUL time. These rules represent imperfect benchmarks at best. They rarely clarify asset availability at any given time. Some ISR capabilities cannot offload data in near-real time, meaning analysts can only assess requirement fulfillment retroactively. Other assets provide large volumes of data that are difficult to sift and process quickly. This constraint leaves analysts perpetually unsure which assets are genuinely available, in the sense of having fulfilled requirements, at any moment.

Another collection management principle is to embrace a multi-INT approach to avoid becoming too reliant on a favored intelligence discipline.[39] One discipline's strengths can compensate for another discipline's weaknesses, helping to increase overall confidence in the information gathered. Although straightforward in theory, multi-INT collection presents difficulty in practice. Multi-INT collection is more art than science. Collection managers must consider tradeoffs among competing priorities and intelligence gain versus loss while simultaneously allowing flexible, real-time changes to the plan. Collection managers and analysts often must manually intervene to deconflict multiple ISR capabilities working the same target, a situation often caused by underdeveloped collection strategies and the absence of an ISR common operating picture. Without human intervention, one capability's collection could disrupt another capability's collection, effectively wasting assets. An ISR capability's tasking does not update automatically to reflect information gathered recently

[37] In ISR planning, a collection asset is organic to a particular commander whereas a collection resource is not organic and must be requested from a higher echelon. DoD, *Joint Publication 2-01*, p. GL-8.

[38] Ibid., III-16.

[39] Ibid., pp. III-15–III-16.

by another ISR capability. Instead, the tasking remains as specified by the spreadsheet submitted the day prior. This lack of dynamic updating can stop multi-INT collection from reaching its full potential and obstruct the targeting cycle.

Potential Process Improvements

AI tools could improve current ISR collection processes by addressing the challenges of workflow precision, dynamic updating, requirement fulfillment, and multi-INT synchronization. AI could help automate how ISR collection requirements get tracked and tasked, increasing precision by reducing human error while saving collection managers' and analysts' time.[40] Rather than calling up a specific UAS, satellite, or another collection platform by "tail number," human operators working with partnered machines could allocate collection resources according to factors such as availability, location, threats, vulnerability, sensor phenomenology, or prioritization, enabling easier multi-INT synchronization. For example, General Atomics has used the Metis application to demonstrate the feasibility of using AI to manage ISR tasking.[41]

Advances in machine learning (ML) could aid in "tipping and cueing" ISR collection, a breakthrough that would simultaneously advance dynamic updating, requirement fulfillment, and multi-INT synchronization.[42] In the future, a ML tool might detect an unforeseen collection opportunity, generate notifications, and even task an ISR capability to capitalize on the opportunity.[43] Anomaly detection opportunities in the Western Pacific might include identifying a mismatch between a vessel's automatic identification system (AIS) report and its radar return, detecting unusual behavioral patterns such as two vessels maneuvering close to one another and remaining in close proximity (indicating a possible ship-to-ship transfer), and spotting vessels that violated identified restriction zones.

Imagine a scenario in which a new ML model reviewing imagery data identified a vessel located close to an island feature. If learning from previous data had taught the model that vessels usually did not appear so close to island features in the area, then the model could flag an anomaly, notify human analysts, and perhaps automatically request the next available collection opportunity. Of course, a vessel cruising near an island feature could prove totally benign. Maybe it was a fishing boat searching for its next catch. Then again,

[40] Brian Katz, *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection* (Washington, DC: Center for Strategic and International Studies, July 2020), p. 2, available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20713_Katz_CollectionEdge_v4_WEB%20FINAL.pdf.

[41] Frank Wolfe, "General Atomics Developing Automated Tasking of ISR Platforms with Metis Application," *Aviation Today*, June 23, 2020, available at https://www.aviationtoday.com/2020/06/23/general-atomics-developing-automated-tasking-of-isr-platforms-with-metis-application/.

[42] Tipping and cueing refer to using one intelligence discipline, asset, or sensor type to cross-cue or initiate collection by a more precise sensor. DoD, *Joint Publication 2-01*, p. III-29.

[43] CSIS Technology and Intelligence Task Force, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation* (Washington, DC: Center for Strategic and International Studies, January 2021), p. 10, available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

China has installed surveillance infrastructure at previously untouched island features.[44] Maybe it was a Chinese vessel conducting reconnaissance. Either way, human analysts would want to study the anomaly. ML can help them recognize the collection opportunity more efficiently.

AI-supported tipping and cueing could harness the power of open-source intelligence (OSINT), a rich data source that the intelligence community underutilizes for various reasons, including a lingering cultural bias in favor of classified collection techniques. During the 10-month period following Daesh's successful June 2014 seizure of Mosul in northern Iraq, approximately 23 million tweets appeared regarding the group's marshaling of support and influence operations.[45] Some of that information carried intelligence value, but the sheer quantity rendered manual review by human analysts impossible. ML could help in a similar future scenario by alerting analysts to specific phrases, locations, or individuals trending in the data, providing a basis for targeting follow-on collection. Since governments can publicly disclose intelligence based on publicly accessible information more easily than intelligence based on classified sources and methods, they could potentially release ML-supported OSINT products to the public, helping turn popular opinion against an adversary's illicit behavior.

Another OSINT tipping and cueing task for AI involves perusing foreign-language news. The massive quantity of foreign news content produced each day easily overwhelms human readers and translators. Recognizing the challenge, the intelligence community's Open Source Enterprise has begun using AI to comb through the data to identify trends, geopolitical developments, and potential crises.[46] These OSINT-derived findings provide a basis for targeting collection, whether by human or technical means. In the future, ML could accelerate these searches for the proverbial needle in the haystack.

[44] H.I. Sutton, "China Builds Surveillance Network in South China Sea," *Forbes*, August 5, 2020, available at https://www.forbes.com/sites/hisutton/2020/08/05/china-builds-surveillance-network-in-international-waters-of-south-china-sea/.

[45] Elizabeth Bodine-Baron et al., *Examining ISIS Support and Opposition Networks on Twitter* (Santa Monica, CA: RAND Corporation, 2016), p. xii, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf.

[46] Patrick Tucker, "Spies Like AI: The Future of Artificial Intelligence for the US Intelligence Community," *Defense One*, January 27, 2020, available at https://www.defenseone.com/technology/2020/01/spies-ai-future-artificial-intelligence-us-intelligence-community/162673/.

Tipping and Cueing Collection: The Capabilities of Commercial Firms

In June 2020, India and China clashed along the line of actual control (LAC), a demarcation of remote Himalayan territory that the two nations have disputed since the 1950s.[47] As news of a violent encounter in the Galwan Valley between two nuclear powers spread across the world, each belligerent tried shaping the narrative to their advantage. The fog of war descended upon Twitter as search results for #IndiaChinaStandoff, #Galwan, and #Ladakh were overrun by malicious bots, government propagandists, and online trolls stoking the flames of racism, nationalism, and conflict. The crisis exhibited all the geopolitical and technological hallmarks of a gray-zone conflict.

Two commercial geospatial intelligence firms, Planet Labs and HawkEye 360, worked together to confirm details of the fast-developing crisis along the LAC. Amid the confusion, the firms provided timely, unvarnished information. Imagery collected by Planet Labs indicated that China had been damming a river in the valley prior to the clash.[48] Meanwhile, HawkEye 360's satellites detected radio frequency emissions in the Galwan Valley typically associated with the Chinese People's Liberation Army (PLA). In a textbook example of tipping and cueing, HawkEye 360 used its collections to vector one of Planet Labs' high-resolution SkySat satellites to image the valley.[49] SkySat's imagery exposed newly arriving Chinese military units, including armored personnel carriers and self-propelled artillery, a clear violation of a June 6, 2020 de-escalation agreement.

The combined efforts of Planet Labs and HawkEye 360 demonstrated a multi-INT synchronization capability that previously existed only with highly classified, government-operated space systems. This capability offered a glimpse into the potential advantages of integrating commercial collections into existing ISR processes. By disseminating accurate unclassified intelligence to both the public and policymakers, Planet Labs and HawkEye 360 sliced through online misinformation to deliver timely insights.[50] The Deterrence by Detection operational concept will harness commercial capabilities to overcome some of the inherent constraints of government-led ISR collection and dissemination.

[47] Marc Santora, "For China and India, a Border Dispute That Never Ended," *New York Times*, updated March 1, 2021, available at https://www.nytimes.com/2020/06/16/world/asia/india-china-border.html.

[48] Simon Scarr and Sanjeev Miglani, "Satellite Images Suggest Chinese Activity at India's Himalayan Border Before Clash," *Reuters*, June 19, 2020, available at https://graphics.reuters.com/INDIA-CHINA/BATTLE/yxmvjkzxwpr/index.html.

[49] HawkEye 360, "Increased RF Activity Points to Chinese Military Buildup in the Galwan River Valley," June 17, 2020, available at https://www.he360.com/increased-rf-activity-points-to-chinese-military-buildup-in-the-galwan-river-valley/.

[50] Ankit Kumar, "Exclusive: First Images from Galwan Show Chinese Build-up Intact after Ladakh Carnage, India Holding Ground," *India Today*, June 17, 2020, available at https://www.indiatoday.in/india/story/exclusive-satellite-images-of-galwan-valley-clash-india-chinese-troops-in-ladakh-1689900-2020-06-17.

Processing and Exploitation

Current Process Challenges

The intelligence community uses the term processing and exploitation to mean converting collected information into forms suitable to producing intelligence.[51] In practice, processing involves pinpointing and preparing a subset of collected information that will prove most informative to intelligence analysis. To draw an analogy to academic research, processing is akin to conducting a literature review. It follows acquiring sources (collection) and precedes developing one's own argument (analysis). Every student understands the importance of having a good literature review. Without it, one cannot position one's own work against the backdrop of what researchers have said previously. Yet every student also understands that literature reviews are time-consuming and often dreary. No wonder senior scholars (or junior scholars with healthy research budgets) often outsource literature reviews to research assistants, asking them to flag only the most important sources for the scholar's attention.

Sadly, current intelligence processing practices offer no such salvation as a dutiful research assistant. Instead, analysts must spend inordinate amounts of time preparing data for analysis. The massive volume of data collected presents a formidable barrier. According to one estimate, the U.S. intelligence community collects more raw data in one day than the entire intelligence workforce could analyze in their combined lifetimes.[52] Moreover, the demands of processing raw data detract from higher-order analytic tasks. As one RAND report recently noted, "[B]asic analysis of incoming collections currently requires enormous human effort, often at the expense of doing higher-level synthesis of information from many sources to answer larger intelligence questions."[53]

Many of today's analysts still manually browse through raw GEOINT and SIGINT collections, seeking suitable start points for analysis.[54] Analysts can use indicators such as the National Imagery Interpretability Rating Scale (NIIRS) to quickly cull the highest quality data.[55] Yet, selecting data based on such indicators offers an imperfect solution. An image might have a lower NIIRS value, but the target of interest could still exhibit discernible and noteworthy activity. An analyst who ignored the image based solely on its NIIRS would thus miss potentially relevant collection.

[51] DoD, *Joint Publication 2-01*, p. GL-12.

[52] Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2017), p. 25, available at https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

[53] Lance Menthe et al., *Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 1, Findings and Recommendations* (Santa Monica, CA: RAND Corporation, 2021), p.3i, available at https://www.rand.org/pubs/research_reports/RRA341-1.html.

[54] Katz, *The Collection Edge*, p. 3.

[55] For background see Imagery Resolution Assessments and Reporting Standards (IRARS) Committee, "Civil NIIRS Reference Guide," *Federation of American Scientists*, March 1996, available at https://fas.org/irp/imint/niirs_c/guide.htm.

SIGINT research poses a similar challenge. In a 2015 report, the National Research Council reported that analysts "may set up 'standing queries' (which need special approval) that run each day to report new events associated with their active targets."[56] Although useful, a standing query will not find all the relevant collection on a target if the activity of interest occurs on search terms (known as "selectors" or "identifiers") other than those specified by the query.[57]

Full motion video (FMV) data processing presents additional obstacles. The current exploitation process forces analysts to monitor a video feed continuously in search of objects or areas of interest.[58] Exploitation analysts often monitor multiple video feeds from different ISR assets simultaneously. As highly trained professionals, exploiters excel at such multitasking. But even the most proficient exploiter will struggle at times to recall what mission-specific things they are looking for (known as essential elements of information or "EEIs") in each feed, particularly when the feeds pertain to different missions in different locations.[59]

Human intelligence (HUMINT) data processing has unique hindrances. More than any other intelligence discipline, HUMINT lives and dies by text. The written word is the coin of the realm. Clear, concise, and accurate writing—supplemented by reporting references and analyst comments—makes for powerful HUMINT. Anything else does not. In such a demanding discipline, inconsistencies in data preparation inevitably occur, whether because of human error, variation in collector reporting skills, or the inherent difficulty of standardizing qualitative content. These inconsistencies can wreak havoc on analysts who retrieve HUMINT via keyword searches, which is still common practice.

A classic HUMINT processing conundrum is consistently rendering Arabic names into English, a task that still befuddles U.S. intelligence analysts even after decades of non-stop military operations in the Middle East.[60] An analyst will often spend hours searching different spellings of the same name in a desperate quest for information. Every spelling variation tried that differs from the original spelling could be a different person entirely,

[56] National Research Council, *Bulk Collection of Signals Intelligence: Technical Options* (Washington, DC: The National Academies Press, 2015), p. 32, available at https://doi.org/10.17226/19414.

[57] Ibid., pp. 36–37.

[58] Amado Cordova et al., *Motion Imagery Processing and Exploitation (MIPE)* (Santa Monica, CA: RAND Corporation, 2013), p. vii, available at https://www.rand.org/pubs/research_reports/RR154.html.

[59] According to *Joint Publication 2-01*, "Information requirements that are also critical or that would answer [priority intelligence requirements / PIRs] are known as EEIs. EEIs may require answering numerous specific questions regarding the collected area/target, such as threat [order of battle], operational status and readiness of troops and equipment, or identification of unique signature information as well as human factor analysis and [information operations intelligence integration]." DoD, *Joint Publication 2-01*, p. III-8.

[60] A thorough discussion of the challenge appears in Ryan Burchnell, "Dynamic Personal Identity and the Dynamic Identity Grid: How Theory and Concept Can Transform Information into Knowledge and Secure the American Homeland," M.A. thesis, Naval Postgraduate School, September 2008, pp. 22-32, available at https://calhoun.nps.edu/handle/10945/3874.

raising the dreadful possibility of mistakenly attributing derogatory information to an innocent person. Few alternatives currently exist to these labor-intensive and potentially error-prone processes.

Potential Process Improvements

AI tools could improve current ISR processing and exploitation efforts by letting machines help with the workloads of GEOINT and SIGINT data processing, FMV exploitation, and HUMINT data preparation. In effect, AI could function as a research assistant providing the intelligence equivalent of a literature review. AI assistance would set up human analysts to do what they do best: connect dots, draw inferences, and make predictions.

In tactical environments, "smart" sensors capable of pre-processing raw intelligence could prioritize which data to transmit and which data to store, saving bandwidth while providing analysts with only the most relevant GEOINT and SIGINT collection.[61] In 2020, for example, General Atomics successfully flight-tested Agile Condor, an AI-powered targeting pod developed by SRC, Inc. The companies integrated the pod "at the edge" onboard the MQ-9 Reaper UAS.[62] Agile Condor performs preliminary data processing to identify and classify objects of interest. It then transmits that information, and only that information, directly to analysts.[63] Information deemed irrelevant by the processing algorithm does not get distributed to analysts, decluttering their workflow and keeping them focused on the most valuable collection. Another MQ-9 development effort led by the Air National Guard, "Ghost Reaper," has added new pods to the aircraft to improve its integration with air and ground assets.[64]

[61] NSCAI, Final Report, p. 81.

[62] Joseph Trevithick, "MQ-9 Reaper Flies with AI Pod That Sifts Through Huge Sums of Data to Pick Out Targets," *The Drive*, September 4, 2020, available at https://www.thedrive.com/the-war-zone/36205/reaper-drone-flies-with-podded-ai-that-sifts-through-huge-sums-of-data-to-pick-out-targets.

[63] SRC, "Teraflops of Processing Power at 26,000 Feet," 2018, available at https://www.srcinc.com/pdf/Whitepaper-Agile-Condor.pdf.

[64] Courteny Albon, "ANG Demonstrating 'Ghost Reaper' Capabilities at Northern Edge," *Inside Defense*, May 10, 2021, available at https://insidedefense.com/insider/ang-demonstrating-ghost-reaper-capabilities-northern-edge.

FIGURE 4: FORWARD COMMAND ELEMENT

Source: U.S. Army Southern European Task Force, Africa, May 2011. Photo by Rich Bartell, U.S. Army Africa Public Affairs Office.

AI could greatly aid GEOINT and SIGINT data processing beyond tactical applications, too. The ongoing Space-based Machine Automated Recognition Technique (SMART) initiative overseen by the Intelligence Advanced Research Projects Activity aims to automate analysis of space-based imagery to recognize events such as heavy construction and human migration.[65] SpaceNet, the open innovation project launched in 2016, has compiled several open-source geospatial imagery datasets that have accelerated ML research. The datasets have helped researchers develop new models such as change detection algorithms that can track building construction over time, an application with obvious appeal for intelligence analysts tasked with scouring the globe for military-related facilities.[66] SpaceNet contains imagery with resolution as high as 50 centimeters, making it an appropriate training environment for intelligence-focused ML models.[67] The surge in geospatial ML research has even led scholars to reevaluate the relevance of NIIRS values to GEOINT research.[68]

[65] Intelligence Advanced Research Projects Activity, "Space-based Machine Automated Recognition Technique (SMART)," accessed April 16, 2021, available at https://www.iarpa.gov/index.php/research-programs/smart.

[66] Debra Warner, "SpaceNet Launches New Challenge with Planet Dataset," *Space News*, August 19, 2020, available at https://spacenews.com/spacenet-7-planet/.

[67] Tom Simonite, "Amazon and the CIA Want to Teach AI to Watch from Space," *MIT Technology Review*, August 25, 2016, available at https://www.technologyreview.com/2016/08/25/157892/amazon-and-the-cia-want-to-teach-ai-to-watch-from-space/.

[68] John M. Irvine and Steven A. Israel, "An Exploration of NIIRS, Image Quality, and Machine Learning," Proc. SPIE 11398, *Geospatial Informatics X*, 113980J (April 21, 2020), available at https://doi.org/10.1117/12.2560587.

In SIGINT applications, natural language processing (NLP) could streamline several labor-intensive tasks.[69] NLP models could perform speech-to-text transcription, voice identification, text summarization, and language translation of intercepted communications.[70] With NLP models performing this grunt work, skilled linguists would have more time to concentrate on higher-order questions of cultural context and meaning.

DoD already has made progress in applying AI to FMV exploitation, but future advances could yield additional gains. Project Maven, also known as the Algorithmic Warfare Cross-Functional Team, manually labeled more than 150,000 images to create the initial training data needed for deep learning AI technologies to aid targeting against Daesh.[71] Future developments could harness ML to tag imagery and identify objects and people, performing many of the most important tasks in phase one analysis.[72]

This type of AI-enabled FMV exploitation would prove highly useful to achieving persistent situational awareness in the Indo-Pacific theater. For example, imagine that a maritime UAS flying a routine reconnaissance patrol spotted a merchant vessel transiting through a certain geographic area. AI-enabled FMV processing tools could classify the target as a specific class of ship. Next, the tools could run an automated query surveying historical activity by that class of ship in that geographic area at that time of year. Discovering that such activity was anomalous, signifying a potential intelligence lead, the tools then could automatically task the UAS to use its FMV sensor, or another sensor, to try and identify the specific ship, not just the class of ship. That task complete, the tools could run yet another automated query surveying the specific ship's recent activity, including port visits, transit routes, and any relevant serialized reporting. Finally, having prepared a literature review, as it were, regarding the vessel of interest, the tools could notify human analysts and deliver the preliminary research, initiating follow-on collection and analysis led by humans. This vignette illustrates how AI-enabled FMV exploitation could accelerate activity-based intelligence (ABI), an increasingly important intelligence method in a world dense with information.[73] Although humans can perform ABI quite well, DoD and the intelligence community have recognized that machines excel at the repetitive data-sifting inherent in ABI.[74]

[69] Natural language processing is "A field of study that aims to analyze and understand human language communications both spoken and textual [and] [c]an include analysis and generation of language." Office of the Director of National Intelligence, *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (2019), p. 15, available at https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

[70] CSIS Technology and Intelligence Task Force, *Maintaining the Intelligence Edge*, p. 10.

[71] Gregory C. Allen, "Project Maven Brings AI to the Fight against ISIS," *Bulletin of the Atomic Scientists*, December 21, 2017, available at https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/.

[72] Menthe et al., *Technology Innovation and the Future of Air Force Intelligence Analysis*, p. 21.

[73] Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Force Quarterly* 77 (2nd Quarter 2015), pp. 24-33, available at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_24-33_Atwood.pdf.

[74] SBIR.gov, "Big Data Analytics for Activity Based Intelligence," accessed April 19, 2021, available at https://www.sbir.gov/node/1208115.

For HUMINTers, AI could help ensure precision and concision in their text-heavy workflows. Automated text summarization would help analysts avoid having to scan an entire document to identify critical details. Automated cross-referencing, which some newer intelligence research tools have started incorporating, would automatically create a hyperlink for any name, location, grid reference, identifier, or other data point contained in a HUMINT report, allowing the analyst to access related information instantly rather than having to copy-paste each search term into a separate query in a separate database. In the future, more sophisticated narrative-generation AI tools could potentially produce written products with relatively little analyst input, including products featuring illustrations and graphs.[75] With less time spent writing reports, a HUMINTer could spend more time cultivating human sources, a task only a skilled human can do.

Conclusion

The current generation of ISR capabilities still has much to offer the United States and its allies. Yet unlocking its full potential will require improving ISR processes. This chapter has argued that incorporating AI could significantly streamline intelligence collection and processing, two essential steps in the intelligence cycle. Implementing "fusion of fusion" in ISR processes will remain a challenge for the foreseeable future, but planners can start tackling that difficulty today. AI will never replace the central role of the human analyst in drawing complex inferences and making ethical decisions. However, AI can assume greater responsibility for certain laborious tasks, helping analysts increase their effectiveness and efficiency. The intelligence community still has a long way to go before it realizes many of these gains. But the technology available today provides a sufficient foundation for starting to build the intelligence enterprise of tomorrow.

[75] Ibid., p. 14.

CHAPTER 4

Organizational Adaptation in the Indo-Pacific: A Neighborhood Watch-Based Approach

The preceding chapters outlined how the United States and its allies and partners could fully leverage existing ISR platforms with improved processes to maximize the intelligence returns from a Deterrence by Detection operational concept. This chapter illustrates this integration by proposing a "neighborhood watch" approach to maintaining situational awareness in the Indo-Pacific region.

Focusing on organizational coordination, an oft-neglected aspect of coalition military effectiveness, the chapter begins by drawing an analogy to domestic neighborhood watch programs in the United States.[76] It then applies the analogy to using regional multi-domain fusion centers (RMFCs) to maintain situational awareness in the Indo-Pacific. The centers would leverage and build upon existing regional initiatives, such as information fusion centers, anti-piracy programs, and counterterrorism centers, to support operations across the competition continuum. After sketching the proposed benefits of this approach, which include the efficiency benefits of leveraging existing organizational structures, the chapter introduces a vignette to illustrate the concept.

Neighborhood Watch Concept

The United States and other like-minded nations seek to maintain a free and open Indo-Pacific for maritime trade, access to resources, and shared security. The region's political and economic importance demand a priority effort. As Admiral Philip Davidson, former

[76] Nora Bensahel, "International Alliances and Military Effectiveness: Fighting Alongside Allies and Partners," in Risa A. Brooks and Elizabeth A. Stanley, eds., *Creating Military Power: The Sources of Military Effectiveness* (Stanford: Stanford University Press, 2007), pp. 186–206.

head of U.S. Indo-Pacific Command (INDOPACOM), noted recently, "In 10 years, the region will host two-thirds of the world's population and two-thirds of the global economy."[77] One way to achieve this objective is to conceptualize it as a neighborhood watch.[78] Founded in 1972 to assist citizens and law enforcement, the U.S. National Neighborhood Watch program has evolved to assist with disaster preparedness, emergency response, and terrorism awareness. Additionally, it has helped identify resources and best practices for specific security challenges.[79] Today, these resources include digital technology such as low-cost security cameras and information-sharing applications such as "Ring" and "Nextdoor." Without meeting in person to coordinate, neighbors can rapidly share information based on local developments and national news.

The rapid growth of social media information and digital technology means that collective security requires agreeing upon processes to inform, validate, and respond. For neighborhood watches, these tasks fall to traditional first responders including police, fire, and medical services. However, situations sometimes require specialized capabilities such as police Special Weapons and Tactics (S.W.A.T.) units, fire department hazardous materials (HAZMAT) units, or medical airlift units. Additionally, many traditional first-line response services establish liaison officers or response plans with commercial sectors such as power and energy; airport, rail, and port operators; and federal agencies such as the Federal Bureau of Investigation or Federal Emergency Management Agency. Social media monitoring applications such as Dataminr's First Alert provide another way to monitor neighborhood activity.[80] No two neighborhoods are alike, so although the tools and processes may differ in each location, this complex response network works most effectively when first responders receive rapid notification about a situation, including as many validated operational details as possible.

Regional Multi-Domain Fusion Centers

As with the neighborhoods described above, areas of the Indo-Pacific have differing approaches to maritime security. However, today many countries use information fusion centers for maritime awareness and security. For example, India, Malaysia, and Singapore have recently stood up or expanded information fusion centers focused on maritime security. Some centers have specific priorities, such as counterpiracy or counterterrorism,

[77] Jim Garamone, "Erosion of U.S. Strength in Indo-Pacific Is Dangerous to All, Commander Says," *DoD News*, March 9, 2021, available at https://www.defense.gov/Explore/News/Article/Article/2530733/erosion-of-us-strength-in-indo-pacific-is-dangerous-to-all-commander-says/.

[78] For an empirical assessment of the effects of neighborhood watch organizations, see Katy Holloway, Trevor Bennett, and David P. Farrington, *Does Neighborhood Watch Reduce Crime?* Crime Prevention Research Review No. 3, U.S. Department of Justice, Office of Community Oriented Policing Services (2013).

[79] National Neighborhood Watch, "Our History," accessed April 23, 2021, available at https://www.nnw.org/our-history.

[80] Paul Rothman, "Using Real-Time Data for Proactive Risk Mitigation," *Security Info Watch*, April 5, 2017, https://www.securityinfowatch.com/alarms-monitoring/integrated-security-management-systems-psim/article/12321484/leveraging-social-media-feeds-has-become-a-perquisite-for-almost-any-public-safety-and-law-enforcement-agency.

but all are built on the foundation of regional information sharing. Similarly, the proliferation of cellular and satellite communications, social media, and unmanned systems means there are more ways to obtain information for situational awareness beyond traditional radar and AIS data. Taken together, these trends have enabled the proliferation of RMFCs.[81]

Capitalizing on this development, a Deterrence by Detection neighborhood watch would coalesce these efforts through agreed-upon processes and information sharing. As a distributed network of information fusion hubs, these centers would support the foundational provisions of UNCLOS for open and transparent maritime security.[82] As a baseline, all participants would agree to report and share information on surface and subsurface activity in three broad areas: 1) normal "white shipping" and economic activity; 2) safety of life and environmental activity; and 3) criminal activity.

One approach to organizing such an effort would involve standing up a Joint Interagency Task Force Indo-Pacific (JIATF-IP).[83] Acting as the lead facilitator, it would assist the regional fusion centers with best practices and tools for them to integrate the vast amounts of data being generated in the maritime environment. The supporting architecture would include satellites across multiple orbital regimes, high- and medium-altitude unmanned systems, and surface and subsurface sensors. Investments in data processing and information fusion at the centers would provide tailored capabilities for the neighborhood watch participants, both ensuring participation and elucidating preferred rules for collaboration. Using common applications with participants would allow fusion centers to ingest significant amounts of local, commercial, law enforcement, and military data to assist response management. Planners could create applications to report and monitor AIS data and electromagnetic spectrum activity, as well as a general reporting application with prescriptive reporting criteria for fishing and economic activity. Planners could contract to receive information from global digital commercial sources of radio frequency, social media, and weather data, then fuse it with local information to improve situational awareness.[84]

Networking together U.S., allied, and partner manned and unmanned platforms through improved communication capabilities, onboard and offboard computing, and AI combined

[81] For background on regional maritime fusion centers, see Deon Canyon, Wade Turvold, and Jim McMullin, *A Network of Maritime Fusion Centers Throughout the Indo-Pacific* (Honolulu, HI: Daniel K. Inouye Asia-Pacific Center for Security Studies, February 2021), available at https://apcss.org/wp-content/uploads/2021/02/2545_Canyon_Network-of-Maritime-Fusion-Centers.pdf.

[82] For background see United Nations, "The United Nations Convention on the Law of the Sea: A Historical Perspective," 1998, available at https://www.un.org/depts/los/convention_agreements/convention_historical_perspective.htm.

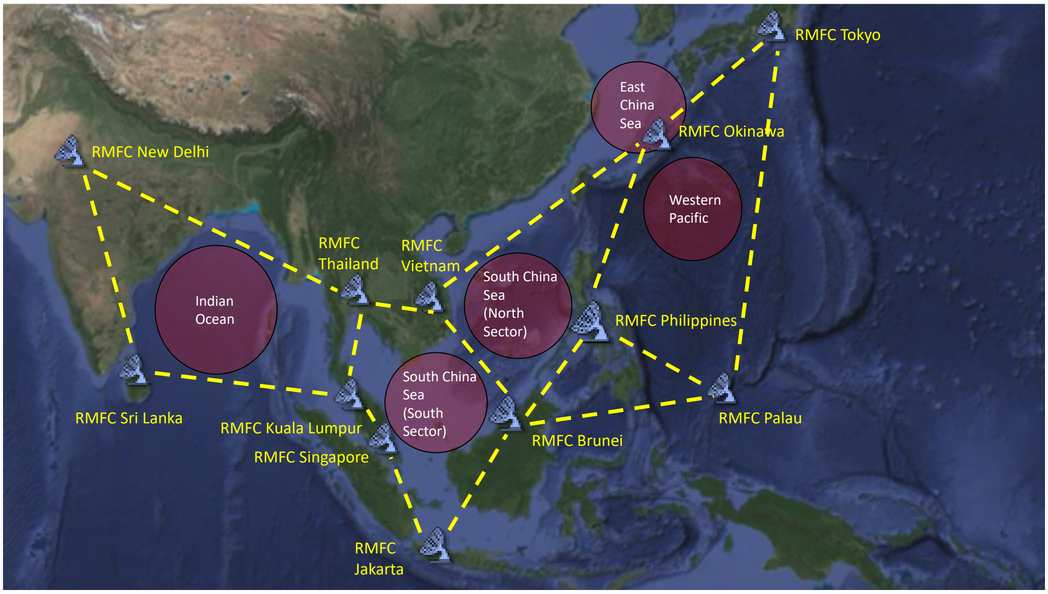
[83] This arrangement would leverage the existing organizational model of the Joint Interagency Task Force-South (JIATF-S) in Key West, as a long-standing interagency and multi-national fusion capability and command organization. A physical headquarters location for JIATF-IP remains to be determined but would integrate inputs from across the regional fusion centers and coordinate response activities.

[84] Further information on these applications is available at https://www.he360.com, https://www.dataminr.com/firstalert, and http://www.buoyweather.com.

with programmable sensors offers the ability to gather and share real-time situational awareness to meet the differing informational needs of each RMFC. Scalable and tailorable with informational dashboards, the RMFCs could ingest and fuse scientific, law enforcement, and military information. Together, the countries would monitor safety and criminal activity prior to initiating agreed-upon response options. Upholding sovereignty in accordance with UNCLOS would provide the foundational premise and legal framework for potential responses involving specialists such as coast guard rescue, police S.W.A.T., or simply additional sensor coverage. Through active information integration, the RMFCs would connect the neighborhood digitally as opposed to using onsite liaison officers and post-incident report sharing. The COVID-19 pandemic has demonstrated that virtual coordination and collaboration often achieve better inclusivity and timeliness than traditional onsite meetings coupled with after-action reports.

JIATF-IP and the RMFCs would also build a coalition of the willing for shared patrols and response options. Using collaborative tools and applications, the forces could share and report information to spur appropriate responses to maritime security and governance challenges. Moving beyond simple historical reporting of incidents, the centers would actively build and maintain real-time multi-domain awareness through the increased connectivity of operators in these environments. Each partner would retain responsibility for resourcing responses or requesting collective support.

FIGURE 5: NOTIONAL LAYDOWN FOR MULTI-DOMAIN FUSION CENTERS



Source: CSBA

This collaborative information ecosystem would provide response management and automated decision-support tools through access to multi-domain sensor networks. Through the adoption of technology enablers such as cloud, artificial intelligence, and distributed computing, this approach would underpin a network of manned and unmanned platforms ideally suited to respond to crises and provide indications and warning (I&W).

By building trust and interoperability, regional partners would learn how to stand up secure ad-hoc mesh networks for information sharing and communications during a crisis. With tactics, techniques, and procedures (TTPs) developed through INDOPACOM's extensive exercise campaigns, the region would improve its ability to both monitor and respond to maritime security incidents while upholding UNCLOS standards and protecting sovereign national rights.

Benefits of the Proposed Approach

Implementing Deterrence by Detection would strengthen the bonds between like-minded nations in support of maritime security and governance. It would provide effective neighborhood watch for day-to-day competition and uphold established rules and norms for maritime transit, trade, and access to resources. By using wide-area multi-domain surveillance platforms combined with emerging technologies, the concept would empower local operators and partner nations to share information, thus building and maintaining situational awareness.[85] Using digital technologies would require coordination and collaboration among partner nations in cyberspace to ensure trust and validate information. This burgeoning trust would further attract additional countries to participate in international and regional governance forums, creating a virtuous cycle.

In the event of a crisis, Deterrence by Detection would prepare participants to respond effectively. Fusing a multi-domain network of sensors and communication pathways would enable rapid coordinated responses to typhoons, disabled vessels, environmental disasters, or resource disputes. As an example, the competition for resources in the Spratly Islands has triggered escalating sovereignty disputes that countries must monitor closely. It would be a priority area for multi-domain awareness.

Through this active neighborhood watch, participants would stand ready to respond to a conflict should escalation occur. Because response capabilities would interlink through a multi-domain network, transitioning from observation to response would occur more seamlessly, with participants rapidly fielding capacity and sustainment capabilities to stifle potential crises. Whether a short-duration event or precursor to a long campaign, the initial moves in a crisis set the tone for effectiveness. Returning to the neighborhood watch analogy, if a fire department is to respond successfully, it must know a fire's location, size, and composition of combustibles. Deterrence by Detection provides exactly that type of information for Indo-Pacific situational awareness.

[85] The concept could also provide climate change and environmental data for long-term research on the risks to fishing stocks, coral reefs, and trade routes.

Vignette: A Crisis Response Scenario

RMFC New Delhi is coordinating a response with RMFC Australia and RMFC Sri Lanka to an oil tanker fire in the Bay of Bengal. An Australian MQ-4 has been diverted to image and communicate with the tanker until an Indian P-8 arrives on the scene. RMFC Sri Lanka is routing a Coast Guard firefighting vessel to the scene. RMFC Singapore receives the initial notification of a large container ship that is dead in the water and sinking in sector seven of the traffic separation scheme in the Strait of Malacca. It is coordinating with RMFC Kuala Lumpur and RMFC Jakarta to either stop or reroute maritime traffic. A category five typhoon has passed through Mindanao, Palawan, and the Spratly Islands. RMFC Manila is leading relief efforts, and RMFC Vietnam is tracking a large Chinese Amphibious Group potentially transiting to the Spratly Islands or the Strait of Malacca. RMFC Okinawa is reporting a large Chinese fishing fleet with Chinese Coast Guard and maritime militia vessels approaching the Senkaku Islands. A Japanese Coast Guard MQ-9 Sky Guardian is on station providing SIGINT cueing to P-8 and P-1 aircraft.

While the RMFCs coordinate first responder efforts and designate supported and supporting local agencies, JIATF-IP monitors and adjusts available forces as necessary with partner nations. Aware of the coordinated regional efforts, Australian MQ-4 and MQ-9 aircraft prepare to assist with ISR in the Strait of Malacca while U.S. Coast Guard ships assist with security patrols in the area. Singapore secures and investigates the damaged vessel in the Strait. Meanwhile, Brunei, Vietnam, the Philippines, Australia, and Japan organize a task force to provide needed capabilities to support the typhoon recovery effort. The United States and Japan provide additional MQ-4 and MQ-9 patrols in the Senkakus to ensure an effective and enduring I&W posture.

As this vignette illustrates, close collaboration and shared information across multiple domains with today's platforms will prove indispensable when responding to emergencies, criminal or gray zone nation state activity, or longer-term economic and environmental threats. By establishing an active neighborhood watch, more local resources could flow into any coordinated response, helping to clarify the need for more specialized or enduring capabilities. This active and continuous posture will both deterrence and the ability for more focused and sustained responses throughout the spectrum of competition, crisis, and conflict.

CHAPTER 5

Conclusion

The United States and its allies face an increasingly challenging strategic environment. For the foreseeable future, we will be engaged in a long-term competition with China in the Western Pacific region and increasingly in the areas beyond. Information, in the form of situational awareness, represents the bedrock of strategic advantage in this competition. Persistent overt observation offers the ability to gain a more holistic understanding of China as a competitor through enhanced knowledge of deployment patterns, routine behaviors, and responses to various contingencies.

First and foremost, the United States and its allies need to gain a better understanding of our competitors. In the case of China, this includes the need for a more detailed and accurate assessment of the technical capabilities of Chinese forces; deeper insight into the deployment patterns of the People's Liberation Army (PLA), China Coast Guard, and Maritime Militia; as well as a better understanding of the PLA's tactics and operational concepts. The Deterrence by Detection architecture described in this report both offers the means to provide persistent monitoring of Chinese activities and the ability to support coalition responses should competition turn to crisis or conflict.

The United States, its allies, and partners also need to be able to dissuade or respond to acts of intimidation. Deterrence by Detection aims to provide real-time awareness of these activities, whether violations of sovereign waters, intrusions into airspace, or harassment of ships at sea. A multi-domain architecture that yields real-time detection would provide national leaders with increased clarity to devise and implement a calibrated set of options to respond to provocations. Moreover, the unmanned systems that comprise the architecture themselves provide an economical and flexible means of persistence and response to such acts.

Persistent real-time situational awareness also has a vital role to play in deterring conflict. Deterrence by Detection's central premise is that potential transgressors are less likely to act if they know they are being watched constantly and that their actions can be publicized widely. Moreover, attempts to interfere with, or even attack, a multi-domain ISR architecture would provide evidence of aggressive intent. Finally, if deterrence fails, the reliable information collected during attacks on the architecture can serve as the predicate for a political response and military action.

In the current strategic and budgetary environment, the United States ought to get the maximum value out of existing or near-term capabilities even as it develops and fields new ones. To maximize the effectiveness and resilience of the Deterrence by Detection architecture, these sensors must be knitted together into a multi-domain system of systems. Using existing platforms to host the types of sensor, processing, and communication payloads that collectively yield persistent surveillance offers a way to reduce the risk of developing new systems. In addition, the experience of implementing the Deterrence by Detection concept can inform efforts to develop new systems and integrate them into new architectures.

A multi-domain ISR network designed to implement Deterrence by Detection should be visible, ubiquitous, affordable, and interoperable. First, *visibility* is a key attribute of platforms in an ISR network designed to deter opportunistic aggression. Whereas there are many cases where it makes sense for ISR assets to operate covertly, in the case of Deterrence by Detection there is value in being overt. Being detectable is an attribute to inform an adversary we are always present and always watching, denying them the ability to operate covertly.

Second, maintaining *ubiquitous presence* is another key attribute of such an architecture. Whereas there are many cases where it makes sense for ISR assets to operate unpredictably to catch an adversary unaware, deterring through the threat of detection requires that a competitor have high confidence they are being observed.

Third, for an ISR network to provide the sort of persistent, visible coverage needed to implement the concept of Deterrence by Detection, individual system elements need to be *affordable*.[86]

Finally, the argument in favor of including U.S. allies and partners as *interoperable contributors* to such a network is strong. Given the changing military balances in the Western Pacific, the United States should seek new ways of informing and reassuring its allies and friends and galvanizing collective responses to crisis and aggression. An interoperable multi-domain ISR network represents a promising approach to do just this.

The key to unlocking the full effectiveness of a multi-domain Deterrence by Detection architecture is maximizing the use of existing systems while strengthening the overall architecture by investing in several key enabling capabilities. These enabling capabilities include:

[86] For example, as of 2017 AFTOC data, MQ-9s flew 83 percent of the U.S. Air Force ISR enterprise's total flying hours but at only 28 percent of the total cost of the U.S. Air Force's ISR flying hours.

- Line-of-sight communication, such as laser communications, both among and across layers (e.g., space-to-space or air-to-space) to allow large amounts of data to move quickly;

- Distributed computing at the tactical edge to support a distributed and multi-level tasking, collection, processing, exploitation, and dissemination (TCPED) architecture featuring both multi-static, distributed sensing within a domain and across domains and ad-hoc mesh networks; and

- Artificial intelligence and machine learning (AI/ML) approaches to enable one crew to operate and control many orbits of systems, inverting much of the current operational paradigm of large ground crews and operators for each individual system.

- Timely dissemination of information to relevant organizations and partners for action and public consumption.

Implementing Deterrence by Detection also will require adapting processes to unlock the full potential of modern collection platforms. For ISR platforms, this means modernizing the current TCPED process and architecture. Too often, relatively inexpensive unmanned systems have borne the burden of costs associated with labor-intensive processes to extract, use, and exploit the copious amounts of information that they can collect.

Finally, implementing Deterrence by Detection will require organizations to adapt to ensure that full-time situational awareness is delivered broadly across joint, interagency, and coalition partners to maximize its strategic effect.

Given the eroding military balance in the Western Pacific, Deterrence by Detection is a strategic imperative. We face these challenges today, not in the distant future. To meet them, we need to implement Deterrence by Detection in the very near term using existing platforms augmented with communication, computing, and AI/ML enhancements to field a multi-domain architecture capable of yielding persistent situational awareness. This near-term effort can, in turn, help shape and inform future investments.

APPENDIX

Maximizing the Use of Existing Systems

This Appendix describes existing platforms that can support the Deterrence by Detection operational concept.

Unmanned Aerial Systems

Large UAS

Photo Credit: U.S. Air Force

RQ-4 Global Hawk

The Global Hawk is the U.S. Air Force's high-altitude long-endurance (HALE) UAS. It can stay airborne for more than 24 hours and survey up to 100,000 sq km every day, equivalent to the entire territory of South Korea. The Global Hawk first entered service in 1998 and has functioned since then as an image and intelligence collection platform. It has a 40m wingspan and is 14m long, making it one of the larger unmanned aircraft operated by the U.S. military.

To date, the RQ-4 has undergone four block upgrades to improve the platform's capabilities. Block 20 included the ability to convert Global Hawks into airborne communications relays, and Block 30 created the capability to carry Airborne Signals Intelligence (ASIP) payloads. RQ-4s also can carry synthetic aperture radar for intelligence collection.

Photo Credit: U.S. Air Force

MQ-4C Triton

The Triton is the U.S. Navy's version of the RQ-4 Global Hawk and is designed to provide persistent maritime ISR capabilities. The Triton complements P-8 Poseidon maritime patrol operations and works in tandem with manned aircraft. Indeed, both the United States and Australia are developing manned-unmanned teaming or "dyad" concepts that bring together unmanned systems such as the Triton and manned systems such as the P-8 for maritime patrol and reconnaissance missions.[87] The MQ-4C can remain airborne for up to 24 hours at an altitude of 17,000m and maintain speeds up to 330 knots. Early operational capability (EOC) was declared in 2020, and the Triton is expected to reach initial operational capability (IOC) by 2021.

Differing from Global Hawk, Triton can descend to lower altitudes when it identifies an object of interest, with a reinforced wing structure specifically designed for this purpose.[88] Descending to a lower altitude allows onboard cameras and sensors to obtain a clearer picture of what is happening on the ocean's surface without being obstructed by weather. Some of the Triton's current and planned payloads include electro-optical and infrared (EO/IR) sensors, signals intelligence collection payloads, and communications nodes allowing the aircraft to act as a mobile communications relay for low probability of intercept, detection, and jamming (LPI/LPD/LPJ) signals.

Photo Credit: U.S. Air Force

MQ-9 Reaper

The MQ-9 Reaper is operated by the U.S. Air Force and Marine Corps.[89] With the extended range kit, it can remain airborne for up to 35 hours at a maximum altitude of over 15,000m with a range of nearly 10,000km. The Reaper has historically functioned as a hunter-killer UAS with sensor apertures onboard to identify targets and weaponry to attack those targets. Under the Deterrence by Detection concept, it would normally operate in a defensive configuration and use its diverse sensors, including maritime and multi-mode radars as well as electronic warfare payloads and communications relays, for satellite communications (SATCOM) denied environments. For the maritime domain awareness mission, it would use its onboard Lynx radar in maritime wide area surveillance mode; its SeaVue maritime wide area surveillance radar on the center line stores location; and an electronic support measure payload that can surveil to the radar horizon for signals of interest. When planners wanted a weapons loadout, the MQ-9 could carry four AGM-114 Hellfire missiles plus two 500lbs laser-guided or GPS-guided bombs or four Small Diameter Bombs II.

[87] "The Coming of the Maritime Domain Enterprise to Australia: The P-8/Triton Dyad," *SLD Info*, July 11, 2018, available at https://sldinfo.com/2018/07/the-coming-of-the-maritime-domain-enterprise-to-australia-the-p-8-triton-dyad/; and Greg Waldron, "Australia to Obtain Two Additional P-8A Poseidons," *Flight Global*, December 29, 2020, available at https://www.flightglobal.com/defence/australia-to-obtain-two-additional-p-8a-poseidons/141782.article.

[88] Northrop Grumman, "MQ-4C Triton," accessed April 23, 2021, available at https://www.northropgrumman.com/what-we-do/air/triton/.

[89] Joseph Trevithick, "Marines Lay Out Plan for Their Own MQ-9 Reaper Drone Force in Budget Request," *The Drive*, March 12, 2019, available at https://thedrive.com/the-war-zone/26924/marines-lay-out-plan-for-their-own-mq-9-reaper-force-in-new-budget-request.

The MQ-9A was delivered to the U.S. Air Force in 2007, and the MQ-9B is set for delivery to the United Kingdom in 2021. One difference between the MQ-9A and MQ-9B is that the MQ-9A is not certified to fly in civilian airspace, which limits its ability to operate, whereas the MQ-9B has been designed to be certified in certain countries.[90] Unlike the MQ-9A, the MQ-9B can operate in adverse weather with its de-icing system and lightning protection; integrate in national and international airspace systems using its detect and avoid system; and perform expeditionary operations from short runways with a minimal operating footprint. The MQ-9B can remain aloft for up to 40 hours and can carry up to 4,800 lbs. of external payloads.[91] In April 2021, the State Department approved a $1.6 billion foreign military sale of MQ-9Bs to Australia.[92]

Photo Credit: General Atomics

MQ-1C Gray Eagle

The MQ-1C Gray Eagle was introduced into service in 2009 as an Army-operated MALE UAS. Gray Eagles upgraded to Block II can carry either a 250kg payload or a 360-degree ISR sensor package. The platform can operate for up to 36 hours at a maximum altitude above 7,500m. The MQ-1C Block I has a payload capacity of up to 360kg, and the Block II can carry weapons if desired, including the AGM-114 Hellfire missile and other air-launched effects (ALE).

Medium UAS

Photo Credit: Northrop Grumman Corporation

MQ-8 Fire Scout

The MQ-8 Fire Scout is an unmanned vertical takeoff and landing (VTOL) aircraft designed to serve as a forward scouting and target-identification platform operated by the U.S. Navy. The Fire Scout entered service in 2000 and can carry payloads up to 315kg while staying aloft for five to eight hours. Fire Scout can carry various payloads, including synthetic aperture radars, moving target indicators, a tactical datalink, and a minefield detection system. The MQ-8C will enter service in 2021, replacing the MQ-8B throughout the Littoral Combat Ship class. Because the MQ-8 is a rotary-wing aircraft, it can operate from aircraft carriers, amphibious ships, and large surface combatants, in addition to shore-based locations.

[90] Ewan Levick, "MQ-9B Sky Guardian Chosen Over Reaper," *Australian Defence Magazine*, November 28, 2019, available at https://australiandefence.com/au/news/mq-9b-sky-guardian-chosen-over-reaper.

[91] General Atomics, "MQ-9B SkyGuardian / SeaGuardian," accessed May 18, 2021, available at https://www.ga-asi.com/remotely-piloted-aircraft/mq-9b.

[92] Valerie Insinna, "US State Department Clears Australia to Buy MQ-9B Drones," *Defense News*, April 26, 2021, available at https://www.defensenews.com/global/asia-pacific/2021/04/26/state-department-clears-australia-to-buy-mq-9b-drones/.

Photo Credit: Embention

VTOL UAS

VTOL UAS such as the DroneTech Pelican are commercially available UASs that can be converted into a hybrid takeoff-and-landing aircraft if necessary. The Pelican has a wingspan of 4m, a length of 3m, a range of 1350nm, a cruising speed of 48kts, and a sprint speed up to 65kts. The total payload capacity for the Pelican VTOL is approximately 10kg and includes an ISR sensing package including full-motion video.[93]

Photo Credit: DPI UAV Systems

Tethered UAS

Tethered UAS systems can increase the height-of-eye for valuable sensors. An example is the Dragonfly Unmanned Multirotor Aerial Relay (UMAR) that can deploy from one 20-foot shipping container and can reach up to 150m in the air. Its payload options include EO-IR sensors or communications relays that can be held aloft indefinitely under tethered power.[94] Filling the role of a modern-day crow's nest, a tethered system can extend line-of-sight ISR and communications coverage. In a Deterrence by Detection scenario, a tethered system could occupy and monitor a portion of the search area, providing collection capability and acting as a node to relay data through the broader surveillance network.

Small and Very Small UAS

Long-endurance UAS with external payload capacities can also act as motherships, carrying additional smaller vehicles aloft. Wing-mounted dispenser pods can release small unmanned aerial systems or ALE.[95] These ALE can carry autonomous flight systems, sensors, and communications packages and remain on station for periods of 60-90 minutes or longer, while extending surveillance of a given target without consuming capacity from other aerial systems in the Deterrence by Detection architecture. In its April 2021 Unmanned Systems Integrated Battle Problem, the U.S. Navy used a long-endurance small

[93] DroneTech UAV, "AV-2 Pelican," accessed April 23, 2021, available at https://dronetechuav.com/av2-pelican/.

[94] DPI UAV Systems, "Medium Tethered Unmanned Aerial System for Vehicles," last updated January 5, 2021, available at https://dragonflypictures.com/products/tuav/.

[95] Further information on these capabilities is available at https://www.ga-asi.com/multi-mission-payloads, https://www.ga.com/ga-asi-conducts-sparrowhawk-suas-flight-tests, and https://www.ga-asi.com/ga-asi-participates-in-usaf-abms-on-ramp-demonstration.

UAS produced by Vanilla Unmanned to provide up to three days' worth of beyond-line-of-sight communications and relays.[96]

ALEs can augment long-endurance UAS by deploying from those UAS to interrogate contacts, gaining higher sensor resolution without forcing the UAS to descend from its high-altitude vantage point. If equipped with ALEs, a long-endurance large UAS can remain at its optimized cruising altitude without burning additional fuel, time, and coverage descending and ascending repeatedly. Meanwhile, ALEs can descend below weather to collect on targets and disaggregate to increase the number of surveillance sensors available on any given mission. ALEs also have demonstrated swarming capability whereby they collect information collaboratively from multiple vantage and phenomenological perspectives, presenting complex counter-air targets to an adversary.[97]

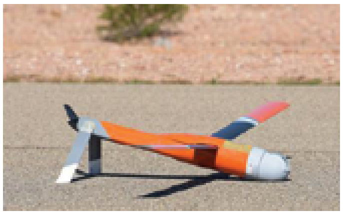


Photo Credit: Area I Industries

Altius 600 and 900

The Altius 600 and 900 are tube-launched systems capable of loitering over a target for up to four hours (Altius 600) or 15 hours (Altius 900). They can carry full-motion video and signals intelligence (SIGINT) sensors, and the UAS itself can function as a kinetic kill option.[98] These UAS operate either as quick-reaction surveillance mounted on aircraft and ship decks to respond to threats or as attritable surveillance collection mechanisms in contested environments.

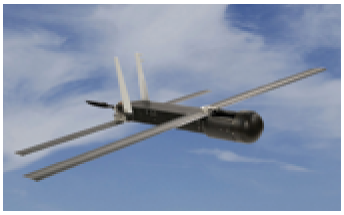


Photo Credit: Raytheon

Coyote Containerized System

Similar to the Altius systems, the Coyote containerized UAS system launches individual UAS (similar in size to the Altius 600) or multiple UASs as a swarm to conduct electronic warfare or ISR. Deploying multiple UASs from a single common launch tube, they can form a larger swarm to act as ad hoc mesh communications or ISR-gathering networks. Coyote containers can deploy on the decks of ships or on land-based vehicles.

[96] Richard R. Burgess, "Navy's Unmanned Systems Battle Problem Features All-Domain Sensing," *Seapower Magazine*, April 26, 2021, available at https://seapowermagazine.org/navys-unmanned-systems-battle-problem-features-all-domain-sensing/.

[97] Raytheon, "Mind of the Swarm," last updated March 20, 2020, available at https://www.raytheonmissilesanddefense.com/news/feature/mind-swarm; and "ONR: Swarming UAVs Could Overwhelm Defenses Cost-Effectively," *Aviation Week*, April 23, 2015, available at https://aviationweek.com/aerospace/onr-swarming-uavs-could-overwhelm-defenses-cost-effectively.

[98] Area I Industries, "Altius 600" and "Altius 900," accessed April 23, 2021, available at https://areai.com/altius-600-2/; and https://areai.com/altius-900/.

Photo Credit: AeroVironment, Inc.

Blackwing

The Blackwing is a tube-launched, loitering sensor and aerial attack platform that can function as a kamikaze UAS. Each Blackwing has a 0.34m wingspan and is 0.45m long, containing an EO/IR ISR collection suite. Blackwing UASs can launch from maritime platforms and use tactical data links for communications.[99]

Airborne Sensors

Balloons and other aloft surveillance systems can provide temporal windows to cover areas of interest, freeing up other systems like long-endurance UAS for other tasks or providing more dense coverage during desired periods. Low-cost stratospheric balloons can serve as high-altitude pseudosatellites (HAP) that can surveil large areas without incurring the expenses of launching and operating orbital satellites. Operating above the jet streams at altitudes of 15-20km or higher, these steerable, solar-powered balloons can navigate using wind currents and moderating air ballast. With a typical payload capacity of 45-70kg, these balloons can typically stay aloft for 100 days, but an ongoing record-setting flight has lasted over 300 days.[100] HAPs could provide an intermediate maritime domain awareness solution at less complexity and cost than traditional satellites.

Unmanned Maritime Systems

To augment the capabilities of unmanned aerial systems, unmanned maritime platforms can provide persistent detection for surface and undersea activity, even if more limited in area coverage.

Photo Credit: Metal Shark

Long-Range USV (LRUSV)

The LRUSV is the 11-meter rigid-hulled, inflatable USV under development for the Marine Corps. It will act as a logistics and support vessel for Marine Littoral Regiments conducting Expeditionary Advanced Base Operations (EABO). The LRUSV could carry small, tube-launched UAS. The LRUSV will likely have a range of 500nm and a payload capacity up to six tons when first deployed.

[99] AeroVironment Incorporated, “Blackwing Loitering Reconnaissance System,” accessed April 23, 2021, available at https://www.avinc.com/tms/blackwing.

[100] Loon, “The Loon Flight System,” accessed April 23, 2021, available at https://loon.com/technology/flight-systems/.

Photo Credit: Textron Systems

Common Unmanned Surface Vessel (C-USV)

Sometimes known as the fleet-class unmanned surface vessel, the C-USV is an 11-meter platform currently deployed by the Navy to conduct mine countermeasure missions. The C-USV also can carry the Coyote containerized UAS system.

Afloat Sensors

Photo Credit: SailDrone

SailDrone

SailDrones are unmanned meteorological monitoring devices. Each drone is solar-powered from its 5-meter wingsail, giving SailDrones unlimited range traveling at speeds up to 7 knots. Current SailDrone payloads include sensor arrays to monitor wind speed, water temperature, salinity, and atmospheric pressure, in addition to full-motion video and communications payloads.

Photo Credit: Office of Naval Research

AXIB Buoys

The airborne expendable ice buoy (AXIB) was originally designed for deployment in the Arctic to monitor sea levels and meteorological and oceanographic conditions. These air-deployable buoys could be modified to carry small camera payloads or act as nodes within a communication relay network, functioning as an alternative to satellite communications. Each buoy is 2m tall and 0.5m in diameter across at its widest point. AXIBs can deploy from C-130 aircraft or other air transport platforms. With overflight of U.S. and allied airspace, the buoys could cover large segments of the First Island Chain nearly simultaneously.

Miniature Buoys

Miniature buoys approximately the size of a basketball can deploy from surface platforms. Miniature buoys feature an approximate endurance of one year and can carry electromagnetic/radio frequency communications equipment, sonar, cameras, and meteorological sensors. Because of their small size and low cost, they can cover a specific geographic area in relatively large numbers.

Photo Credits: AXYS Inc.

Undersea Research Networks

Undersea research networks can provide acoustic, seismic, or other phenomenological measurements of undersea activities. Examples include rapidly deployable sensor grids, such as the Maritime In Situ Sensing Inter-Operable Network (MISSION) involving Singapore and the United States, and other fixed and towed array sensor systems, such as digital thin line arrays which can be towed behind unmanned undersea and unmanned surface vessels or deployed from fixed seabed locations.[101]

Space Systems

Since the launch of the Project CORONA satellites in the 1960s, the United States has used space as a key domain to monitor the activities of its adversaries. However, space-based surveillance systems have until recently been limited by their dwell time, coverage, and the level of classification of the information they produce. For example, U.S. EO, IR, and radar satellites possess very high spatial resolution but lack the quantities to search continuously. The biggest impediment to integrating these systems into a multinational persistent maritime domain awareness architecture remains the inability to disseminate space-based intelligence quickly and widely.

Space-Based Commercial Systems

Today, a growing number of commercial space-based remote sensing companies are expanding access to an emerging market for collection and analysis of intelligence from proliferated constellations of small satellites. This paradigm of commercial space-based systems can provide one alternative to the current constraints of classified U.S. space systems. Commercial space products and services leverage advances in low-cost launch, power and cooling systems, on-board processor and computing miniaturization, and artificial intelligence and machine learning (AI/ML) to make these capabilities more affordable and accessible for nontraditional (i.e. non-governmental) users as well as governments.[102] Commercial space companies are replicating and, in certain respects, rapidly advancing technologies and techniques traditionally restricted to a small number of technologically advanced national governments.

[101] Joseph Rice, *Maritime In Situ Sensing Inter-Operable Networks (MISSION)* (Monterey, CA: Naval Postgraduate School, 2013), available at https://www.onr.navy.mil/reports/FY13/oarice.pdf; and Venugopalan Pallayil, "Light Weight Array Technologies for Underwater Applications," Acoustic Research Laboratory, Tropical Marine Science Institute, National University of Singapore, April 10, 2021, available at https://arl.nus.edu.sg/research-posts/light-weight-array-technologies-for-underwater-applications/.

[102] Early government investment in these technologies, particularly by DoD, helped bring them to commercial markets.

For example, Planet Labs is building a “megaconstellation” of cheap small satellites for overhead imaging. Each of Planet Labs’ “Dove” satellites is about the size of a shoebox. Although a Dove satellite lacks the spatial resolution of classified U.S. systems, it can take 10,000 pictures a day over an area equivalent to the size of Mexico. Planet Labs’ entire constellation of hundreds of Dove satellites will be able to photograph the entire planet at least once every 24 hours.[103] Planet Labs is also working to field a few high-resolution satellites capable of following up on tipping from Dove collection with additional fidelity and resolution.

Companies such as Capella and ICEYE are building constellations of commercial synthetic aperture radar (SAR) satellites. Critically, these systems can collect at night and through cloud cover. Again, these satellites do not meet the highly classified resolution standards of historical and current U.S. satellites, but their value lies in rapid revisit rates over large coverage areas. Capella, which is providing data to the U.S. Air Force, can provide SAR collection within 20 minutes of being tasked. [104] Given the speeds at which maritime targets travel, achieving a temporal resolution of 20 minutes from space is operationally relevant when tasking long-endurance UAS to respond. Using rapid temporal resolution constellations, an imagery analyst can use commercial space-based remote sensing imagery for initial identification of changes that may necessitate a more detailed look from long-endurance UASs.

Hawkeye360 is a relatively unique entrant in the commercial space-based remote sensing field. Its satellites perform geolocation of radiofrequency (RF) emissions. Although this type of capability has historically been the exclusive realm of well-resourced governments, developers such as Hawkeye360 have demonstrated the capability to track AIS transponder emissions from ships. An AIS transponder broadcasts a vessel’s identity, position, course, and speed. These systems can also share information related to destination and cargo type. An AIS transponder shares its information with AIS transponders aboard other ships and land-based AIS receivers, aiding collision avoidance, search and rescue, and maritime law enforcement and security. Although AIS was originally intended for terrestrial use over distances of roughly 50 miles, in 2005, a satellite successfully detected AIS broadcasts from space.[105] Today, commercial space-based RF can collect transmissions to derive insights about global commerce and security, as well as identify platforms that may not have AIS active (so called “dark targets”) and potentially merit interrogation using other assets.

Commercial space companies are also increasing their sophistication, including using distributed sensing algorithms to fuse information across large constellations, formation

[103] Contrary to what some observers expect, coverage of maritime areas remains relatively sparse due to limited business-case applications of interest.

[104] Capella Space, “Our Story,” accessed April 23, 2021, available at https://www.capellaspace.com/about-us/our-story/.

[105] “Satellite AIS – Addressing Some Misconceptions,” *Big Ocean Data*, April 22, 2016, available at https://www.bigoceandata.com/white-paper/satellite-ais-addressing-some-misconceptions/.

flying, and rapid production of heterogeneously customized satellites at current scales of one to two dozen per month.[106]

Photo Credit: ISI Space Netherlands

Containerized Space Launch Systems

Containerized microsatellites offer another way to add components rapidly to the space layer of a Deterrence by Detection architecture. Existing examples include a 40-ft. containerized system that can launch up to four satellites into low-earth orbit (LEO), each of which can provide communication for up to three weeks. The same launch system can provide tactical satellite coverage focusing on ISR collection rather than communications. Containerized launch systems provide for ease of transportation, difficulty to clearly discern launch capability, and the ability to leverage vessels of opportunity to accommodate these payloads.

Photo Credit: National Aeronautics and Space Administration

Space Planes

Although space planes may seem outlandish to some readers at first glance, they have become increasingly viable in recent years. A space plane flies like an aircraft in Earth's atmosphere and maneuvers like a spacecraft in outer space, a revolutionary advance beyond space shuttle technology.[107] Sierra Nevada Corporation's "Dream Chaser" is a reusable, unmanned space plane that has passed numerous development milestones and will fly to the International Space Station in 2022 under current plans.[108]

[106] "HawkEye 360 to Be First Commercial Company To Use Formation-Flying Satellites," *CBS Boston*, accessed April 23, 2021, available at https://boston.cbslocal.com/video/5226773-hawkeye-360-to-be-first-commercial-company-to-use-formation-flying-satellites/.

[107] Kenneth Chang, "25 Years Ago, NASA Envisioned Its Own 'Orient Express,'" *New York Times*, October 20, 2014, available at https://www.nytimes.com/2014/10/21/science/25-years-ago-nasa-envisioned-its-own-orient-express.html.

[108] Richard Tribou, "Former Shuttle Landing Site to Welcome Spacecraft Again When Dream Chaser Missions Begin in 2022," *Orlando Sentinel*, May 4, 2021, available at https://www.orlandosentinel.com/space/os-bz-snc-dream-chaser-clearance-to-land-at-kennedy-space-center-20210504-pqbqqm4evjhx5mli4ruzkn4s2e-story.html.

LIST OF ACRONYMS

ABI	activity-based intelligence
AFRL	Air Force research lab
AI	artificial intelligence
AIS	automatic identification system
ALE	air-launched effects
AXIB	airborne expendable ice buoy
CSBA	Center for Strategic and Budgetary Assessments
C-USV	common unmanned surface vehicle
DoD	U.S. Department of Defense
EABO	expeditionary advanced base operations
EO	electro-optical
EOC	early operational capability
FMV	full-motion video
GEOINT	geospatial intelligence
GPS	Global Positioning System
HALE	high-altitude long-endurance
HAZMAT	hazardous materials
HPC	high-performance computing
HUMINT	human intelligence
INDOPACOM	Indo-Pacific Command
IOC	initial operational capability
JIATF-IP	Joint Interagency Task Force Indo-Pacific
LAC	line of actual control
LEO	low Earth orbit
LPD	low probability of detection
LPI	low probability of interception
LPJ	low probability of jamming
LRUSV	long-range unmanned surface vehicle
MALE	medium-altitude long-endurance
MISSION	Maritime In Situ Sensing Inter-Operable Network
ML	machine learning
NDS	National Defense Strategy
NIIRS	National Imagery Interpretability Rating Scale
NLP	natural language processing
NSCAI	National Security Commission on Artificial Intelligence

OSINT	open-source intelligence
PED	processing, exploitation, and dissemination
PLA	People’s Liberation Army
RF	radiofrequency
RMFC	regional multi-domain fusion center
SAR	synthetic aperture radar
SATCOM	satellite communications
SIGINT	signal intelligence
SMART	Space-based Machine Automated Recognition Technique
SWAT	special weapons and tactics
TCPED	tasking, collection, processing, exploitation, and dissemination
UAS	unmanned air system
UMAR	Unmanned Multirotor Aerial Relay
UNCLOS	United Nation Convention on the Law of the Sea
USV	unmanned surface vehicle
VTOL	vertical takeoff and landing
VUL	vulnerability window

CSBA

Center for Strategic and Budgetary Assessments

1667 K Street, NW, Suite 900
Washington, DC 20006
Tel. 202.331.7990 • Fax 202.331.8019
www.csbaonline.org