

# NAVAL WAR COLLEGE REVIEW

**Winter 2018**

Volume 71, Number 1



# ANTIACCESS WARFARE AS STRATEGY

---

## From Campaign Analyses to Assessment of Extrinsic Events

Sam J. Tangredi

Thinking about the concept of antiaccess warfare may be likened to thinking about the Renaissance. Leonardo da Vinci, Niccolò Machiavelli, and Dante Alighieri did not know that they were part of a renaissance; they simply experimented, strategized, and wrote in a fashion that seemed logical to them and appropriate to their times. It was the nineteenth-century European historian Jules Michelet who “discovered” that “the Renaissance” had occurred.

Likewise, Themistocles, Elizabeth I, Isoroku Yamamoto, and Adolf Hitler (after early 1943) did not know that they were conducting antiaccess warfare. They simply applied a strategy that was logical for a situation in which a strategically superior power was attempting to penetrate—militarily, politically, or both—a region they controlled. Originating circa 1991, the term *antiaccess warfare* is simply the best appellation that has been developed to describe their strategies

for comparative purposes. As used throughout this article, the term *strategy* incorporates political and economic objectives and activities, not military operations alone.

From this perspective, the concept of antiaccess warfare precedes and transcends the development of the air-sea battle concept, the *Joint Operational Access Concept (JOAC)*, the *Joint Concept for Access and Maneuver in the Global Commons (JAM-GC)*, and other recent efforts to understand the logic of opponents’ military operations that the United States would face if major war were to occur under current conditions. This logic derives from

*Dr. Sam J. Tangredi is a professor of national, naval, and maritime strategy at the Center for Naval Warfare Studies at the Naval War College, and recently was appointed director of the Institute for Future Warfare Studies at the College. A retired Navy captain, his active-duty billets included serving as head of the Strategy and Concepts Branch of the Office of the Chief of Naval Operations and director of strategic planning and business development for the Navy International Programs Office, in addition to command at sea. He is the author of numerous articles on strategy and defense policy and has published five books, most recently Anti-access Warfare: Countering A2/AD Strategies (Naval Institute Press, 2013).*

the fact that presently the United States is a strategically superior global power whose homeland lies outside the regions of potential crisis and conflict. As a global power, it has allies, commercial ties, and deep interests in areas that are thousands of miles from the continental United States, where most of its military power is based. While the United States maintains a forward military presence in many world regions, whether at sea or operating from bases in partner nations, these deployed forces are necessarily limited, either by the physical hulls or by diplomatic agreements. Forward-presence forces are intended to act as deterrents to major war and as on-scene responders to more-limited crises—to prevent the latter from becoming the former. If we are particularly alert, quick, or lucky, such forces may prove sufficient by themselves to deal even with significant crises. But they do not necessarily represent the full power required to prevail in a major regional conflict. Hence, in most cases we would need to move decisive forces from outside to inside the conflict region. Unlike most other nations, the United States actually possesses the military logistics capabilities and control of the global commons to do so.<sup>1</sup>

Antiaccess warfare is part of the strategy—used throughout history—of opposing such force movements (or the capacity, or the very decision, to move), along with an effort to empty the region of forward-presence forces and reduce the opponent's overall regional influence. It is important for U.S. national security professionals to analyze and understand antiaccess warfare as an element of peacetime as well as wartime strategy, if we are to counter it when required.

If the United States is to develop and maintain the capacity to defeat—and thereby have the ability to deter—sophisticated antiaccess strategies that threaten to reduce the U.S. presence in, influence over, or access to contested regions, a coordinated, articulated, and persistent intragovernmental approach is required, not just Department of Defense (DoD)-only planning. Logical first steps toward creating such an interagency approach involve acknowledging and analyzing the problem, examining its consequences, identifying mutually supportive actions, and outlining processes by which an approach can be coordinated.<sup>2</sup> This article identifies the elements of antiaccess warfare strategies, outlines several historical examples of success or failure, briefly suggests some of the means of countering such strategies today, and describes ways to coordinate these means and evaluate the assumptions and risks entailed.

## TOWARD STRATEGIC-LEVEL ANALYSIS

To understand how to neutralize antiaccess strategies, we must analyze the problem at the strategic level. In countering an antiaccess *strategy*, as opposed to simply preparing or tailoring a military force package to defeat an antiaccess military *campaign*, we must recognize that a viable antiaccess strategy—one

designed to reduce U.S. influence and operational capabilities in a region of potential conflict—includes political, diplomatic, economic, legal, social, and media actions, not just a military posture. This way of thinking goes beyond the military campaign analysis often used to assess antiaccess warfare scenarios.<sup>3</sup> Antiaccess strategies involve all the phases of conflict, including preconflict “peace,” referred to in planning documents as Phase 0. Some of these activities are captured by current buzzwords, such as *lawfare*, *soft power*, *cyber war*, and *gray-zone conflicts*. However, a comprehensive, multifaceted U.S. government strategy to actually counter deliberate antiaccess efforts does not exist, nor has a comprehensive plan appeared in the literature published by public research centers (think tanks) or academic institutes that influence government policies.<sup>4</sup>

In other words, we know that potential opponents rely on the concept of *antiaccess* (no matter the term they use) as their primary approach to defeating, or at least diminishing, U.S. regional influence backed by American military power. But most of our government organizations either do not recognize the activities involved or are not interested in analyzing and responding to them. Similarly, most academic analysts have not examined these mutually supportive activities as a broader unified strategy, rather than as individual issues or the elements of active military campaigns.

Largely this is the result of *antiaccess* being perceived as but a military term that applies solely within the province of DoD. The unfortunate, tactically oriented acronym *A2/AD*, which stands for *antiaccess/area-denial*, cements this perception.<sup>5</sup> Indeed, the most authoritative official document discussing antiaccess warfare, the Joint Staff J7–authored *JOAC*, briefly notes the comprehensiveness of antiaccess strategies, but limits itself to developing a “warfighting concept” to deal with such strategies militarily.<sup>6</sup> It does *not* reject the pertinence of other, nonmilitary activities, but simply does not regard them as falling within the purview of the joint force. However, as noted previously, the problem is that few outside DoD see these activities as falling within their purview either. The *JOAC* notes that maintaining “operational access” to regions of interest is the U.S. military’s contribution toward the “assured access” of the United States to the global commons that is the prerequisite for economic access to these regions themselves.<sup>7</sup> However, there is no evidence that the wider U.S. government perceives the need for a strategy to ensure access, and access issues are mentioned rarely, beyond cursory observations concerning the Navy’s role in maintaining “freedom of the seas.”

One might argue that preparing to defeat antiaccess campaigns militarily is exactly the narrow focus on which DoD should concentrate. However, the problem is that DoD does not control the totality of resources necessary to defeat an antiaccess strategy, and thus is at a severe disadvantage in planning or prosecuting a

counterantiaccess campaign. Such a campaign needs to include a wide range of nonmilitary activities.

Moreover, with the end of the Cold War against Soviet expansionism, there actually is less coordination of these activities within the U.S. government. During the Cold War there was often a tension between defense objectives and trade policies (wheat sales to the Soviets provide one example), requiring higher-level resolution.<sup>8</sup> Today there is less tension, since there is little perception that such activities are in any way related, except for occasional, often ineffective, economic sanctions or embargoes of selected technologies or strategic materials imposed on individual states.<sup>9</sup> Admittedly, the need to counter terrorism following the traumatic events of 9/11 did prompt mutual support among military operations, intelligence, homeland security, and law enforcement, but in a relatively narrow band of activities (e.g., physical security) against a relatively unsophisticated threat. Coordination of other transagency activities during the unending conflicts within Iraq (and Syria) cannot be rated as stellar.<sup>10</sup>

#### CHARACTERISTICS OF ANTIACCESS WARFARE

To discuss a comprehensive antiaccess strategy, it is important to examine the fundamental elements of antiaccess warfare itself. They are as follows:

1. The perception of the strategic superiority of an opponent
2. The primacy of geography, as the element that most influences time and facilitates the combat attrition of the opponent's forces
3. The general predominance of the maritime domain as conflict space
4. The criticality of information and intelligence, and concomitantly the effects of strategic and operational deception
5. The determinative impact of extrinsic, sometimes apparently unrelated, events in other regions or globally

The first element motivates a nation (or an armed group) to adopt antiaccess as a primary defense strategy. The specification of *defense* strategy does not mean that the nation or group has no offensive objectives, such as the seizure of another's territory or the intimidation of neighbors; rather, it indicates that the primary aspect of the potential conflict is the involvement of an opponent of greater military, political, diplomatic, or economic power, considered on a global scale.

This characterized the grand strategy of imperial Japan in the Second World War. Competent Japanese leaders, such as Admiral Yamamoto, knew that the United States was a strategically superior power by almost any measure. (Having spent time in the United States, Yamamoto knew that firsthand.) However, Japan's leaders were committed to making conquests in the Asia-Pacific. This required

driving U.S. military forces out of the region and ending U.S. political, diplomatic, economic, and social influence in the western Pacific. To protect their gains, they needed to create an antiaccess barrier (fortified island chains and a powerful navy) to ensure that the strategically superior but now regionally ousted United States could not reenter the contested region. The United States thus needed to penetrate that barrier.

All military planners recognize geography to be a critical operational factor and seek to “manipulate the physical environment, exploit its strengths, evade its weaknesses . . . and contrive always to make nature work for them.”<sup>11</sup> If an antiaccess defender has greater accessibility to nearby regional geographic features, it can facilitate attrition of its opponent through delay and constraint. Exploiting geography is the primary physical factor underlying an antiaccess strategy. For example, without a barrier of islands (to complement the advantage of the vast distances the United States faced) in the central and western Pacific, imperial Japan would have found it difficult to adopt an antiaccess posture (i.e., the positioning of its forces) against a U.S. response to its conquests. Similarly, the islands and straits that isolate the South China Sea and East China Sea from the vast expanse (and maneuver space) of the Pacific allow China today to adopt an antiaccess strategy against potential military responses and to counter U.S. political influence in the region. A Chinese antiaccess posture would be much less effective without the vast distances of the Pacific, the relatively shorter distances from China to its neighbors (the probable targets of any military action and the definite targets of its expansion of influence), and the maritime geography that would channel the U.S. fleet if it sought to enter the so-called first island chain. The very use of the term *first island chain* by military planners implicitly acknowledges the geographic underpinning of China’s antiaccess strategy.

Given that wide oceans separate the United States from the areas of potential regional conflict, it is an incontrovertible fact that the maritime domain (which includes the air and space above it) would be the predominant conflict space in any contingency involving the United States opposing a major enemy employing an antiaccess strategy. Quibbles concerning that verity are largely parochial.

The criticality of information and intelligence in the cyber age is acknowledged by everyone. However, when discussing them in terms of antiaccess warfare, the focus is primarily on *operational and tactical* deception; yet what has succeeded best in antiaccess campaigns has been *strategic* deception. Whereas operational and tactical deception is directed at an opponent’s military operations, strategic deception is directed at decision making on the national command authority level, and is linked to the manipulation of extrinsic events, defined as events that occur outside the contested region or do not involve military force, yet have a significant impact on the strategically superior power’s decision making. According

to an influential source, strategic deceptions “involve large numbers of individuals and organizations as perpetrators and victims of deception, including the national command authorities on both sides of the deception interaction; second, . . . they are relatively long-term deceptions . . . and third, . . . their stakes are very high, in that they can affect the outcomes of wars.”<sup>12</sup>

In contrast to all the above, the determinative impact of extrinsic, sometimes unrelated events on the efforts and attention of the strategically superior power is generally the element *least acknowledged* by those who conduct campaign- or tactical-level analyses of antiaccess warfare, yet it is the *most important*. The current “win-hold” construct—building an American joint force that can defeat an opponent in one region while holding off another in a different region until forces can be “swung”—does appear to acknowledge that simultaneous conflicts can occur. However, what is grasped only rarely is that events that are not conflicts, or have not yet become conflicts—events that may occur in other regions, are merely prevalent on a global basis, or are confined to nonmilitary dimensions—nonetheless can have a profound impact on any “win.”

Research indicates that most nations (or armed groups) adopting an antiaccess approach never actually defeat their strategically superior opponents in combat.<sup>13</sup> What has occurred historically is that the strategically superior power just quits fighting, because the costs appear too high when an event or other concerns of even greater interest occur elsewhere.

For example, the ancient Greeks, led by Themistocles, were able to cut the sea lines of communication that had allowed Xerxes to feed his vast Persian force in Greece during the conflict of 480–479 BCE. However, what actually caused Xerxes to cease his efforts at conquest was his perception that revolts were brewing in his empire, so his repressive hand was needed elsewhere. Of course, the Greeks played a role in fanning those revolts.<sup>14</sup>

Similar actions have been a hallmark of antiaccess strategies throughout history. In preventing and defeating the Spanish armadas (note the plural), England’s Queen Elizabeth I used multiple methods to incite extrinsic events. She financed the prolonged war of independence that the Dutch United Provinces fought against Spain. She let loose the English pirates of the Caribbean (in her eyes, unofficial privateers or high-risk “adventurers”) against Spanish colonies. She employed spies and agents, and even feigned contemplation of marriage to forestall a Franco-Spanish alliance against England. All this was done in a time of ostensible peace.<sup>15</sup> Over a period of more than two decades, such activities effectively bankrupted Spain, ensuring that Philip II never could concentrate enough force to plow through the Royal Navy and land on English shores, an event that would have pitted battle-hardened Spanish troops against local English levies. By

the time the first Spanish armada reached the English Channel, Spain's strategic power already had been reduced.

In the example of imperial Japan, its improbable 1940 alliance with Nazi Germany (and tacit nonaggression agreement with the Soviet Union) can be understood only as an effort to help ensure that a war in Europe would draw in the United States. Generating this extrinsic event was intended to divert U.S. attention and forces away from the western Pacific.

With this in mind, a strategist might be prompted to ask: In the event of a pending conflict, what would China do today, or in the future? Is a potential war in the South China Sea over reefs claimed by Vietnam or the Philippines of more-profound interest to U.S. decision makers than Russian pressure on the Baltic nations, all of which are members of NATO? These questions—often stated but only lightly examined—must be analyzed in detail, because they, not a weapons count, will determine the outcome of an antiaccess conflict. Again, historical analysis indicates that antiaccess forces rarely have defeated the strategically superior power on the battlefield (witness the Korean and Vietnam Wars). In many cases, the dominant actor seemed on course for a military victory; it was other considerations that caused that superior power to change course. In the case of the Greek-Persian conflict, it should be recalled that Athens—one of Xerxes's major targets—already had been abandoned and burned to the ground before the Athenian Themistocles was able to orchestrate the battle of Salamis.<sup>16</sup>

The sorts of questions posed above, generated by the fact that extrinsic events historically have played the greatest role in successful antiaccess strategies, should prompt analysts both in government and in think tanks to make a more detailed examination of the phenomenon on the strategic level. Mostly, however, we just continue to argue about A2/AD.

#### THE UNFORTUNATE ACRONYM

The discourse on antiaccess warfare has been dominated by the acronym *A2/AD*, standing for *antiaccess/area-denial*. Credit for the term largely belongs to the highly influential defense issues think tank the Center for Strategic and Budgetary Assessments (CSBA). However, since its origination the term *A2/AD* has been used more often as an adjective to describe the types of weapons systems and networks expected to be used in an antiaccess campaign, rather than to refer to the underlying strategy.<sup>17</sup> The tortuous origin of the *A2/AD* acronym—which has been in use for over fifteen years—has been covered elsewhere, and that discussion will not be repeated here.<sup>18</sup> What should be noted is that use of the acronym, and the full term *antiaccess/area-denial*, has driven much of the discussion of antiaccess away from strategy and almost exclusively toward tactics and

force structures. The construct seems perfectly tailored to campaign analysis. This is not to say that discussion of tactics and force structures is not important, only that discussion of how to deter or defeat the underlying strategy is equally important, if not more so.

There has been some pushback, albeit rare, on the use of the *A2/AD* acronym. In October 2016, Chief of Naval Operations (CNO) Admiral John Richardson, USN, authored an article on the *National Interest's* website that sought to “deconstruct,” and thereby discourage, use of the *A2/AD* term. In the CNO’s view, “A2AD is a term bandied about freely, with no precise definition, that sends a variety of vague or conflicting signals, depending on the context in which it is either transmitted or received.” More importantly, from his perspective, the “area denial” half of *A2/AD* symbolizes a “mindset” in which the U.S. Navy automatically would be forced to operate outside the “red arcs” that mark the theoretical range of the kinetic weapons of the potential opponent, thereby discounting the Navy’s ability to operate within that range—particularly using its superior undersea warfare forces—from the outset of any conflict. As he puts it, “Often, I get into A2AD discussions accompanied by maps with red arcs extending off the coastlines of countries like China or Iran. The images imply that any military force that enters the red area faces certain defeat—it’s a ‘no-go’ zone! But the reality is much more complex. . . . Those arcs represent danger, to be sure . . . but the threats are not insurmountable.” He concludes, “If we fixate on A2AD, we are not looking far enough forward.”<sup>19</sup>

In his article, the CNO does not go on to capture the complexity of antiaccess strategies from the broader perspective, as that was not his intent. But his point about not “looking far enough forward” also can be applied to critiquing the lack of a broad approach to the broader perspective. The combination term *A2/AD* prompts a focus on weapons system performance in operational situations (e.g., Chinese DF-21 missiles vs. USN aircraft carriers), making it easier for analysts to neglect nonmilitary aspects and the role of deterrence. Indeed, the *area-denial* portion of the *A2/AD* construct refers to what could be considered standard tactics in force-on-force combat, and therefore contributes little to the broader perspective.

### AN EXAMPLE OF THE BROADER VIEW

To apply a broader strategic perspective to an apparent antiaccess disposition, let us consider the South China Sea scenario that many defense analysts wargame to assess the outlines of a potential conflict between the United States, particularly the U.S. Navy and Air Force, and China, particularly the People’s Liberation Army (PLA) Navy (PLAN), the PLA Air Force, and the PLA Rocket Force (the

latter controls both conventional warhead- and nuclear-armed ballistic missiles). The chosen battleground is the vicinity of the Spratly islets that China has solidified and fortified.<sup>20</sup>

The South China Sea situation has been analyzed in extensive detail in classified and unclassified reports and war games, and academic studies abound, so only a sketch will be included here. It would be most logical for the scenario to incorporate Chinese adoption of an antiaccess strategy. By all open-source measures, the U.S. Navy appears superior to the PLAN. Combined with U.S. Air Force assets, the U.S. Navy potentially could establish sea control in the South China Sea if it faced the PLAN alone. (It is China's potential use of land-based Rocket Force missiles that makes an antiaccess approach viable.) The current capabilities of USN attack submarines would make it difficult for major PLAN vessels to sortie without considerable risk. China is working steadily to improve PLAN capabilities, particularly in naval aviation (aircraft carrier based) and antisubmarine warfare; but, as a point of comparison, the U.S. Navy can deploy in force and threaten Guangzhou, whereas the PLAN cannot deploy out of area and threaten Pearl Harbor. Clearly, the United States is strategically superior in terms of conventional force on a global basis. (Since this is a maritime scenario, a contest between U.S. land forces and the PLA is presumed not to occur.)

As would any antiaccess force facing an out-of-area, strategically superior power, China would attempt to take advantage of the geographic conditions to employ asymmetric means to prevent the American fleet from entering the South China Sea. Most planners agree that the primary asymmetric means would be the antiship ballistic missiles (ASBMs) (e.g., DF-21Ds) or land-attack intermediate-range ballistic missiles (IRBMs) (e.g., DF-26s) controlled by the PLA Rocket Force. These are definitely asymmetric capabilities, since the U.S. joint force does not possess such weapons (primarily because of the U.S.-Soviet Intermediate-Range Nuclear Forces [INF] Treaty of 1988, which eliminated all land-based U.S. IRBMs).<sup>21</sup> In the event of conflict, U.S. analysts expect China to use ASBMs and IRBMs in addition to ship- and land-based cruise missiles against American ships and allied naval ports, along with cyber- and other electronic-warfare attacks.

But in the broader perspective, would China really have to rely on military means to achieve the goal of neutralizing a U.S. response? Antiaccess strategies include nonmilitary means, along with every other possible leverage that the antiaccess nation (or armed group) possesses, to make entering the region very costly to the out-of-area, strategically superior power. An important factor not usually discussed is that the DF-21 (and probably the DF-26) was designed to carry a nuclear warhead, and it is difficult to determine which missile is conventionally armed and which is nuclear armed. An early means of achieving an

asymmetric effect could consist of political-military-diplomatic signaling and be informational: China might declare that it will not rule out using tactical nuclear weapons to defend its sovereignty claims over the Spratlys and the South China Sea. Since the U.S. homeland would not be threatened, such use logically would not trigger an intercontinental nuclear response. Perhaps such a statement would constitute strategic deception—the Chinese Politburo might be very reluctant to spark (or reenergize) what otherwise inevitably would become a nuclear arms race in East Asia.<sup>22</sup> However, the threat is credible because the PLA has built the means (antiaccess systems) to carry it out. The PLAN fleet would not even have to sortie. In response, U.S. decision makers would face the difficult choice among threatening a nuclear response—which could escalate into an intercontinental nuclear war; avoiding any confrontation of the Chinese claims; issuing an ambiguous “all military options are on the table” statement; or simply ignoring the threat.

The United States has many global interests besides those in the South China Sea. Some would argue that it has no vital interests riding on who controls that area. Because of the INF Treaty, the United States has no IRBMs with which to threaten an analogous response and thereby deter the PLA. Would the U.S. president hazard a tactical nuclear attack on U.S. and allied forces over the Spratlys? Would DoD feel confident that it could determine which DF-21 is nuclear armed and which is not, such that it could determine the validity of the threat? Would it feel confident that it could blind the PLA strike-reconnaissance network sufficiently to make the threat ineffective? How would U.S. allies and partners react to the potential for tactical nuclear use in East Asia?

Going a step further, consider the integration of the Chinese economy into the West and Western manufacturing supply chains. What if China declares that it will end the export of rare earth elements (minerals) if its sovereignty claims are challenged in the South China Sea?<sup>23</sup> This would increase manufacturing costs in the near term, and eventually would affect high-tech industries worldwide. For that matter, what if China threatened to withdraw its global investments? A “coalition of the willing”—those countries that would be willing to challenge Chinese sovereignty claims in the Spratlys—might prove to be pretty thin.

In effect, such actions would generate extrinsic events in the global economy that would increase the cost of a U.S. movement or a “return to the region.” Similar Chinese threats against Japanese or Korean sovereignty likely would have no effects whatsoever on the current strong U.S. commitments to defend Japan and Korea—except possibly strengthening them. But our nontreaty partnerships with other countries involve no formal U.S. commitments.

Using nonkinetic means, the antiaccess force potentially can check the strategically superior power. That is what antiaccess strategies are all about.

## GENERATING CONSIDERATION OF EXTRINSIC EVENTS

The point of examining the South China Sea scenario from a broader perspective is not to give Chinese military planners new ideas; undoubtedly they are not new to them. The point is to identify considerations that the U.S. government must examine as a whole. For example, a Chinese tactical nuclear threat might be neutralized by negotiating an Asian INF arms control treaty. Conversely, an analogous deterrent effect might be achieved if the United States reinterpreted the existing INF Treaty as allowing the deployment of IRBMs in the Pacific region. That is not to suggest that doing either of these things is possible, or even wise policy. Rather, it is to suggest that these are actions that the U.S. Department of State (DOS) should be examining if the U.S. government—not just DoD—were to recognize antiaccess warfare as necessitating a whole-of-government strategy (to employ a clichéd phrase), not as just a military operational problem. There are ideas with which DOS needs to grapple if it is to be part of the effort to counter or deter the Chinese Communist Party (CCP) antiaccess calculus. (The PLA is pledged to the Party, not the Chinese state; the matter of the CCP's survival also can have an impact on extrinsic events.)

The rest of the U.S. government needs to recognize the importance of extrinsic events (or the threat thereof). In the scenario of a temporary Chinese stranglehold on rare earth elements—which would be extrinsic to the issue of South China Sea sovereignty—it would fall to the Department of Commerce to determine whether there is indeed a dependency, and therefore whether the U.S. government should maintain a stockpile of such strategic materials to protect U.S. industries in the event of a cutoff executed as an element of a Chinese antiaccess strategy. Maintaining a stockpile is a deterrent to the threat or execution of such an embargo to further Chinese objectives in East Asia. However, one profitably might ask whether any planner in the Department of Commerce ever has heard the term *antiaccess*.

One hopes that the Department of the Treasury is scrutinizing closely the likely effects of a Chinese disinvestment from global markets (particularly the securities market in the United States). But the South China Sea scenario is probably not a concern within the Treasury Department, so Treasury likely is not considering such disinvestment as part of an antiaccess strategy that the United States must prepare to counter. Have the department's planners determined whether, from a global perspective, the U.S. government could declare treasury bills held by the CCP or Chinese citizens to be null and void—without completely unraveling the rest of the bond market? The threat of these actions might provide more deterrence against the PLAN than a military theater posture.<sup>24</sup> Would other investors lose faith in the security of U.S. treasury bonds, even if these extraordinary actions were necessitated within a context of armed conflict? What would

happen to global markets if the U.S. Navy were to interdict the transshipment of oil from the Persian Gulf to China? The operational aspects of such a presidential decision fall to the Navy, but the economic effects transcend DoD and need to be examined by other departments and agencies.

### A COORDINATED U.S. RESPONSE

Countering an antiaccess challenge—whether it emanates from the CCP, Iran, ISIS, or other entities—requires a whole-of-government approach. If extrinsic events ensure the success of antiaccess strategies, a mechanism must be created to bring together the resources of non-DoD agencies to identify, analyze, plan for, and take actions to deter or respond to the antiaccess strategies of particular competitors.<sup>25</sup> The problem is broader than a strictly military challenge, so the solutions must emanate from something broader than military campaign analysis. These solutions, when combined, would enhance the deterrence from armed conflict and the credibility of military options. DoD traditionally has had strong, practical, working relationships with DOS and the Central Intelligence Agency, but—as the examples above make clear—this is not enough.

It is never fair to argue for solutions without suggesting a process to generate them. There are at least three distinct methods or processes that the U.S. government has used in the past to coordinate across departments and agencies, or at least to determine how to coordinate. They are as follows: (1) creating an executive committee; (2) drafting presidential-level strategic plans; and (3) appointing a bureaucratic “czar” or setting up a “coordinating center.” Each method has its pros and cons, its assumptions and risks, and all should be considered.<sup>26</sup> Of course, the last thing most government executives want to do is to staff yet another committee or maintain an independent center.

A primary model of the executive committee approach is the National Security Council (NSC). The public often perceives the assistant to the president for national security affairs (i.e., the national security advisor) and his or her staff as constituting the NSC, but that is primarily bureaucratic and journalistic shorthand.<sup>27</sup> The council actually is chaired by the president and falls under the Executive Office of the President. Its statutory members are the vice president, Secretary of State, Secretary of Defense, and Secretary of Energy. Other cabinet members (often the Attorney General) attend when requested (or when they insist on being invited). As strategic analysts are well aware, the national security advisor controls the process (the scheduling and content of meetings), thereby wielding an influence over policy that sometimes exceeds that of cabinet members, depending on his or her relationship with the president. The national security advisor has a staff of at least twenty-five deputies and special assistants (most

of whom focus on regional affairs), who attempt to tailor policy responses to the council's (or the national security advisor's) interests.<sup>28</sup>

Creating a position of special assistant for countering antiaccess strategies within the NSC staff would be one method of raising the awareness of top national security decision makers, including the president, regarding how comprehensive the antiaccess challenge is. This special assistant could coordinate a government-wide strategic response. Of course, the assumption is that such a special assistant would be able to raise the issue to the council via the national security advisor. The risk of that assumption is that the number of issues and topics facing the national security advisor is prodigious, and the need for a comprehensive strategy in this area might not be considered a priority. The personal relationship between the special assistant and the national security advisor might determine whether the issue rose to the council level.

An additional assumption is that, having been given direction by either the council or the national security advisor, the special assistant would have the credibility and interpersonal skills necessary to coordinate responses from agencies that might be disinterested or recalcitrant.<sup>29</sup> The NSC staff itself has no authority over the policies of the agencies except that which the relationship between the national security advisor and the president implies. The cabinet-level council members likely would inform their own staffs of decisions relating to a comprehensive strategy; but, again, the risk is that the strategy's importance would get lost amid the noise of other issues, leaving the special assistant with little influence over member priorities. Moreover, many departments and agencies are not represented on the council, and incorporating them via invited attendance or through the efforts of the special assistant likely would be difficult. However, if the special assistant were successful in these tasks, he or she might become effectively an antiaccess issues czar—converting this first option into the third method of coordination.

At first glance, the second process—drafting and promulgating an executive, presidential-level, public document for implementing a counterantiaccess strategy (which might be termed an *access strategy*)—would seem the most desirable method by which to achieve government-wide coordination. The assumption is that once the president states, “This is my policy,” members of the executive branch would endeavor to incorporate it into their department or agency plans and carry it out. The problem (and risk) is that it would get lost amid the myriad of such policy pronouncements—most published in “slick and glossy” format—on a variety of issues, many of which contain language designed for public consumption that is too vague for actual policy implementation. Making government policy clear to the voting public is commendable; however, the reality is

that, because such “strategies” primarily are a means of public communication, they generally are limited in actionable direction and are read only rarely by decision makers in other agencies, each of which has its own strategic plan, or at least its own policies and priorities.

Issuing a classified plan might allow the inclusion of actionable direction, approaching the specificity of a war plan, and perhaps that would be the appropriate way to initiate interagency coordination and collaboration. However, two risks or disadvantages need to be considered. First, classification inevitably results in limiting the audience. Second, allowing access to classified material across agency boundaries is difficult owing to conflicting or inconsistent classification standards, particularly among agencies that do not have a history of close cooperation. Both risks can be mitigated, but they cannot be ignored.

The third method is the creation of a czar who has independent authority over specific actions and can direct activities through a coordination center staffed by individuals seconded from and empowered by their parent agencies. As it relates to the federal government, *czar* is an informal term used, primarily by the media, to refer to a senior official charged with developing and implementing a specific policy rather than leading an agency. Examples include the head of the Office of War Information during the Second World War and the director of the National Cybersecurity Center, director of National Drug Control Policy, and director of the Office of National AIDS Policy today. However, the effectiveness of the individuals appointed to these positions is always dependent on their personal relationships with the president and their ability to assuage the concerns of cabinet members and agency directors as well as Congress.<sup>30</sup> The risk of tasking a policy czar with coordinating an overall approach to countering antiaccess strategies is that he or she becomes bureaucratically ineffective if he or she does not remain in the president’s direct view.

So, which of the three methods would be appropriate for coordinating an intragovernmental response to competitors’ antiaccess strategies? The most honest answer—“It depends”—is hardly satisfying. However, application of the principle that, when dealing with uncertainty, the simplest solution is the place to start means that appointment of an NSC staff special assistant for countering antiaccess strategies would be the logical initial—inevitably experimental—step. It appears the least costly option, in that it builds on an existing process, with a specific individual responsible for success or failure. That individual would be responsible for managing the drafting of an actionable U.S. counterantiaccess plan—here’s where *access strategy* might be a better term—by subject-matter experts from all agencies involved.<sup>31</sup> Once such an access strategy was approved

via the NSC process, the same special assistant would be tasked with achieving interagency implementation. The risks can be mitigated only by appointing a particularly skilled and determined individual, and those risks might reemerge when that particular individual departed.

#### PURVIEW OF AN ACCESS STRATEGY

It is important to note that a government-wide access strategy should *not* duplicate the campaign analysis that DoD conducts. Responsibility for planning to conduct combat operations against an opponent's antiaccess posture or campaign belongs to DoD, and the department has expended great effort to examine the problem from a war-fighting perspective. In Admiral Richardson's article, the CNO comments that "the A2AD problem is currently well understood—challenging, but understood." On the operational level, he is right. There is plenty of room for debate concerning the means and force structure required to "break the great walls," but that debate is ongoing.

The government-wide access strategy should focus on assessing extrinsic events—that is what is lacking. We need a plan—one that goes beyond the purely military—to routinely identify, analyze, deter, and, if necessary, respond to elements of an antiaccess strategy. National security agencies certainly examine many of the nonmilitary aspects of antiaccess, such as governments deploying fishermen as maritime militia, exerting economic pressures on neighboring states, and fomenting ethnic disturbances in "near abroads." However, these nonmilitary aspects currently are considered as isolated phenomena or merely regional events. China experts examine the use of the maritime militia. Russia experts examine naval basing in Syria. Such steps are examined in terms of their effects on sovereignty claims in the South China Sea or the military balance in the Mediterranean; they are not examined as tactics in support of strategies to reduce the influence and presence of the United States and other Western nations as a prelude to denying U.S. access to the region through military means. They are not seen as coordinated components. Moreover, the questions of how to deter such actions and how to respond with nonmilitary means currently are examined in isolation or not at all.

Use of the term *grand strategy* often provokes definitional debates. If it is defined as a strategy based on all vital interests of a nation-state (or some other, nongovernmental global actor), then antiaccess strategies are only a part of grand strategy. Yet the perspective required to understand antiaccess must be grand, the instruments of deterrence and response must be grand, and countering antiaccess strategies must be a grand effort.

What are the assumptions and risks involved in creating a government-wide access strategy?

Obviously, the entering assumption is that the very concept of antiaccess is real or practical and not simply an academic construct. Thus far, experts have not challenged its validity, but perhaps that is only because it is perceived as a DoD-only issue. A vigorous debate would be useful. Some analysts may doubt that potential opponents can implement and coordinate antiaccess strategies, because of their complexity. However, antiaccess strategies leading to war primarily have been the tools of authoritarian regimes (such as imperial Japan and junta-controlled Argentina), which have the means to coordinate nongovernmental as well as governmental resources.<sup>32</sup>

The risks might include the NSC fixating on the antiaccess concept, so that it sees conspiracies at every hand. However, the likely military and geopolitical opponents of the United States and its allies and partners are pretty easy to identify. If assessing their actions in terms of the antiaccess concept and examining nonmilitary means of responding lead to enhanced deterrence, a coordinated access strategy has done its job. From the perspective of DoD, any nonmilitary means of response serve to fortify its military planning. A strategic plan need not be implemented to be useful; it is useful if it identifies options that the president had not examined previously. The primary risk, therefore, is that the time and effort of the planners involved will be wasted if decision makers ultimately reject the concept and plan. Of course, that occurs every single day in the world of strategic planning.

#### **OPERATIONALLY READY, BUT STRATEGICALLY UNPREPARED**

Regarding the CNO's remarks, DoD indeed has examined the antiaccess concept from a war-fighting perspective. The studies and reports are numerous, and presumably the key insights have been integrated into the operational planning of the combatant commanders. The naval services, like the other services, have attempted to grapple with the A2/AD environment in developing their force structures. DoD officials of the Obama administration certainly were attuned to the military aspects of the antiaccess challenge. Indeed, prior to his return to government service, Deputy Secretary of Defense Robert O. Work authored significant reports related to A2/AD.<sup>33</sup> The air-sea battle approach to syncing Navy and Air Force efforts in a potential counterantiaccess campaign eventually was sunk, but that was because it hit the rocks of joint ideology, diplomatic concerns, and academic alarmism, not because the existence of the threat was rejected.<sup>34</sup>

It is easy to argue that the U.S. Navy, along with other services, has not made the correct investments to deal with antiaccess campaigns, but making force-structure changes to a current fleet whose life span exceeds thirty years is not

easy.<sup>35</sup> There are many gaps in our capabilities to break the great walls.<sup>36</sup> Yet it would seem that the CNO's perception that—within DoD—the A2/AD problem is “currently well understood” is true.

But while that may be true on the operational level, the strategic antiaccess challenge will not be understood well unless we examine it as a whole. We need to move beyond DoD campaign analysis to assessing the extrinsic events that can constitute the nonmilitary elements that comprise such campaigns. We do not need the genius of a Leonardo, Machiavelli, or Dante to do that. What we need is a process that brings together the minds of all the practitioners, develops an intragovernmental strategic plan, and assigns responsibility to an individual to ensure coordination and execution. Would integrating the planning of DoD and the other relevant agencies perhaps produce a “strategic renaissance”?

---

#### NOTES

The author thanks the anonymous referee who went far beyond commentary and assisted substantially with editing.

1. For a discussion of U.S. control of the commons and facilitation of the overseas movement of decisive U.S. forces, see Barry R. Posen, “Command of the Commons: The Military Foundation of U.S. Hegemony,” *International Security* 28, no. 1 (Summer 2003), pp. 5–26.
2. Joint doctrine approaches “planning and coordination with other agencies” with the perspective that the nonmilitary agencies are functioning in support of DoD, rather than as bureaucratic-political equals. See, for example, U.S. Defense Dept., *Joint Operation Planning*, JP 5-0 (Washington, DC: Joint Staff, August 11, 2011), pp. II-36–II-37.
3. Such operational-level analysis has gone by a number of names over the years, such as *mission analysis*, *military modeling*, *campaign modeling*, *campaign simulations*, and *analysis of objectives*. *Campaign analysis* is currently the preferred term used by the Military Operation Research Society and the staff of the Chief of Naval Operations.
4. A study that does examine a comprehensive nonmilitary approach to the South China Sea antiaccess scenario is Ross Babbage, *Countering China's Adventurism in the South China Sea: Strategy Options for the Trump Administration* (Washington, DC: Center for Strategic and Budgetary Assessments [hereafter CSBA], 2016).
5. For a discussion of the unfortunate effects, see Sam J. Tangredi, “CNO vs A2AD: Why Admiral Richardson Is Right about Deconstructing the A2/AD Term,” *The Navalist*, January 10, 2017, [thenavalist.com/](http://thenavalist.com/).
6. U.S. Defense Dept., *Joint Operational Access Concept (JOAC)*, ver. 1.0 (Washington, DC: Joint Staff [J7], January 17, 2012), p. 3.
7. *Ibid.*, p. 1.
8. The extensive efforts within the U.S. government (and with NATO allies) to coordinate trade policies with the Soviet Union is discussed throughout Philip J. Funigiello, *American-Soviet Trade in the Cold War* (Chapel Hill: Univ. of North Carolina Press, 1988).
9. The question whether economic sanctions (the term *embargo* usually is not countenanced) levied or led by the U.S. government have achieved their stated goals is debated hotly. It must be observed, however, that some of the sanctioned states required subsequent military (or cyber) actions to force them to curtail their objectionable activities, and others with tight authoritarian regimes simply have lived with the sanctions. Sanctions may have degraded, but did not dispossess, Saddam Hussein, the target of

- the most substantial Western sanctions. A recent discussion of why most U.S. economic sanctions have failed is Bryan R. Early, *Busted Sanctions: Explaining Why Economic Sanctions Fail* (Stanford, CA: Stanford Univ. Press, 2015). A frequently used text that views sanctions in a positive light reports that “we found sanctions to be at least partially successful in 34 percent of the cases that we documented.” But the authors caveat this statistic by admitting that most of the successful episodes involved “modest and limited goals.” This can be translated to mean that in nearly 70 percent of the cases sanctions had no effect, and in 30 percent they had modest effects. Gary Clyde Hufbauer et al., *Economic Sanctions Reconsidered*, 3rd ed. (Washington, DC: Peterson Institute for International Economics, 2007), pp. 158–59.
10. The term *transagency* is used instead of *interagency* because, whereas *interagency* usually implies cooperation, in these areas many of the issues crossed agency lines but were not coordinated; in some cases, they were never even recognized as requiring participation by other agencies.
  11. John M. Collins, *Grand Strategy: Principles and Practices* (Annapolis, MD: Naval Institute Press, 1974), p. 167.
  12. Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (New York: Pergamon, 1981), p. xi.
  13. Sam J. Tangredi, *Anti-access Warfare: Countering A2/AD Strategies* (Annapolis, MD: Naval Institute Press, 2013), pp. 107–33, 234–35.
  14. Xerxes was able to suppress most of these revolts on his return; however, they broke out in earnest on his death. The Athenian role in these revolts, particularly in Egypt, is detailed in John R. Hale, *Lords of the Sea: The Epic Story of the Athenian Navy and the Birth of Democracy* (New York: Penguin, 2009), pp. 99–109.
  15. Two excellent sources that describe the activities surrounding the first Spanish armada are Colin Martin and Geoffrey Parker, *The Spanish Armada* (New York: W. W. Norton, 1989); and Garrett Mattingly, *The Armada* (Boston: Houghton Mifflin, 1959).
  16. A good depiction of the capture and destruction of Athens is provided in Barry Strauss, *The Battle of Salamis: The Naval Encounter That Saved Greece—and Western Civilization* (New York: Simon & Schuster, 2004), pp. 59–72.
  17. In fairness to CSBA’s work, its usage of the term A2/AD was intended to develop an “operational concept” for dealing with the military challenges at the operational level of war that a Chinese or Iranian antiaccess approach poses. The problem is that developing an operational concept without an examination of nonmilitary factors results in operations divorced from strategic objectives.
  18. Tangredi, *Anti-access Warfare*, pp. 40–52.
  19. John Richardson [Adm., USN], “Deconstructing A2AD,” *National Interest*, October 3, 2016, [nationalinterest.org/](http://nationalinterest.org/).
  20. This leaves aside the fact that the South China Sea scenario both is less probable and would be less operationally taxing than a conflict over Taiwan.
  21. The treaty does not ban sea-based IRBMs. A recent congressionally mandated study on USN future fleet architecture completed by the MITRE Corporation recommends the development of a sea-based Pershing III missile as a deterrent and response to Chinese ASBMs. MITRE, *Navy Future Fleet Architecture Platform Study* (McLean, VA: July 1, 2016). The publication is available on the website of Senator John McCain, [www.mccain.senate.gov/](http://www.mccain.senate.gov/).
  22. Paul Bracken long has argued that a nuclear arms race in Asia is inevitable. Currently dormant, it is waiting for a spark. See Paul Bracken, *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (New York: HarperCollins, 1999).
  23. Estimates of Chinese dominance over the rare earth elements vary, but U.S. Director of National Intelligence James Clapper estimated in 2013 that it had a 95 percent market share. See Jeff Nesbit, “China’s Continuing Monopoly over Rare Earth Minerals,” *U.S. News & World Report*, April 2, 2013, [www.usnews.com/](http://www.usnews.com/).
  24. A discussion of economic responses to the South China Sea scenario is in Babbage, *Countering China’s Adventurism in the South China Sea*, pp. 29–30, 52, 58–61. Of course, business opposition to such a move would be extreme. As Michael Mandelbaum notes, “By

- 1994 the American business community had mobilized in opposition to using trade with China as leverage for the pursuit of political goals. . . . China's remarkable economic growth since the beginning of reforms in 1979 had created an American political constituency for preserving economic ties between the two countries." Michael Mandelbaum, *Mission Failure: America and the World in the Post-Cold War Era* (New York: Oxford Univ. Press, 2016), pp. 28–29.
25. The argument that extrinsic events ensure the success of antiaccess strategies is developed in Tangredi, *Anti-access Warfare*, pp. 20–22, 104–105, 114–15, 122, 128.
  26. These “methods” are my own terminology, adopted for the sake of simplicity. There are many more-specific and more-erudite terms that could be used to describe the models, and the terms used in this article are certainly not official. Detailed definition and description are beyond the scope of the article.
  27. This description is admittedly a simple outline of the NSC and its staff. A recent detailed discussion is R. D. Hooker Jr., *The NSC Staff: New Choices for a New Administration*, INSS Strategic Monograph (Washington, DC: National Defense Univ. Press, 2016).
  28. These deputies and special assistants have their own ministaffs of two to ten personnel seconded from government agencies. Hooker reports that during the Obama administration there were over four hundred people on the NSC staff, although this included those who supported the White House Situation Room and performed other ancillary functions. *Ibid.*, p. 10.
  29. Hooker maintains that NSC staff offices “with cross-cutting responsibilities” have invited internal “conflict and competition.” “Without a very limited and clearly defined charter, such offices will tend to stray across the policy landscape, often leading to in-fighting and intramural clashes.” *Ibid.* Avoiding this would require an assignee with a strong sense of cooperation and tact—qualities that Hooker suggests are necessary for all NSC staff members.
  30. In a bitter statement posted on the White House website, President Obama's director of communications Anita Dunn attacks the use of the term *czar*, portraying it as partisan. However, she does admit that there were “jobs that involved coordinating the work of agencies on President Obama's key policy priorities.” Anita Dunn, “The Truth about ‘Czars,’” *The White House* (blog), September 16, 2009, [obamawhitehouse.archives.gov/](http://obamawhitehouse.archives.gov/).
  31. Use of the term *access* is meant to parallel the concepts of *operational access*, *assured access*, and *access to the commons* used in DoD, particularly in the *JOAC* and *JAM-GC*.
  32. On the Argentine case, see Tangredi, *Anti-access Warfare*, pp. 149–56.
  33. For example, Robert O. Work [Col., USMC (Ret.)], *The Challenge of Maritime Transformation: Is Bigger Better?* (Washington, DC: CSBA, 2002), pp. 22–30.
  34. A fine example of academic alarmism concerning air/sea battle is Amitai Etzioni, “Who Authorized Preparations for War with China?,” *Yale Journal of International Affairs* 8, no. 2 (Summer 2013), pp. 37–51, [www2.gwu.edu/](http://www2.gwu.edu/).
  35. Tying the concept of antiaccess to force-structure decisions seems to provoke accusations that the whole concept (and the former Air-Sea Battle Office) is merely a method for the U.S. Navy and Air Force to grab a greater share of the defense budget away from other services and agencies. However, one hopes that all strategies are designed to be implemented, requiring force-structure choices.
  36. An example of the discussion of a particular gap in the context of A2/AD is Sam J. Tangredi [Capt., USN (Ret.)], “Breaking the Antiaccess Wall,” U.S. Naval Institute *Proceedings* 141/5/1,347 (May 2015), pp. 40–45, available at [www.usni.org/](http://www.usni.org/).