Commons Control and Commons Denial: From JAM-GC to an Integrated Plan

Sam J. Tangredi
U.S. Naval War College

The ability to access and freely utilize the global commons is the primary enabler of the globally-deployable military power of the United States. It is also, not coincidentally, the key facilitator of international trade and the source of global prosperity. An opponent with the capability to significantly degrade or deny American use of the global commons could impede the ability to deploy U.S. military forces, challenge the future prosperity of the United States, and reduce U.S. political and economic influence throughout the world.

Defining the Commons

The global commons are the spaces and dimensions on, above, or throughout the earth which are the territory of no one nation, but can be used by all in accordance with international law and political custom. Global commons are usually defined in a legal sense. However they can be functionally defined as mediums humans use for communications, transportation and commercial and information exchange, but cannot normally inhabit.[1]
The most physically accessible global commons are the oceans, which include the air above it, as well as most (but not all) of the seabed below it. Airspace is a commons only above the oceans, which is why it is considered a part of the maritime commons rather than a separate dimension. Beyond the oceans, outer space (once termed "ocean space") is also a global commons, but is obviously less physically accessible. Cyberspace can conceptually be considered a global commons, but is obviously not physically accessible even if it utilized by more individuals than the others, albeit for information exchange rather than trade, discovery, or the transport of military forces.[2]

Access and Control Today

Fortunately, no single nation today has the capability to significantly challenge U.S. access to the global commons—in which access to the maritime commons is the most critical—except in regions close to their national periphery, utilizing anti-access/area denial (A2/AD) strategies.
Anti-satellite weapons could interfere with U.S. dominance in space, but it is still difficult to deny general access. Cyberattacks could interfere with U.S. use of the internet, but again, although damaging in the near term, U.S. vulnerabilities in this dimension are the result of choice and convenience. Not only is U.S. access to the commons difficult to deny, U.S. ability to exert "control" over these commons and deny their use to others—through its global naval, space launch, and coding and information technology management capabilities—remains largely unequalled.
This is a long-standing reality that has become a modern assumption and military tradition. In the Second World War, Imperial Japan could initially deny U.S. access to the maritime commons of East Asia, but it could not prevent the U.S. from deploying its forces into the Western Pacific and building up its power to eventually break through the Japanese wall of islands.[3] During the Cold

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of the Navy, Department of Defense, or the U.S. Government.

War, Soviet forces attempted to deny U.S. access to it maritime periphery and postured some forces (such as in Cuba) that could interfere with direct U.S. access, but it could not sustain the Soviet Navy on a globally-deployed basis. (Access to space also remained unchallenged until the development of anti-satellite weapons late in the Cold War.)

Current U.S. military dominance of the commons is demonstrated by the fact that (for example) it can contest the People's Republic of China's efforts at sea control/sea denial within the so-called first island chain—extending roughly 500-800 nautical miles from mainland China, but the People's Liberation Army-Navy. Missile and Air Force cannot contest the movement of U.S. forces from Hawaii to Guam—roughly 4000 nautical miles—or from San Diego to Guam—roughly 6000 nautical miles. U.S. naval forces also possess the power to prevent the PLAN and Chinese maritime commerce from transiting *beyond* the first island chain, effectively cutting it off from the majority of the maritime commons. This "command of the commons" is the source of, in the words of MIT professor Barry Posen, "the military foundations of U.S. hegemony."[4]

In the same way as the term "command of the sea" can be distilled to "sea control," the concept of "command of the commons" can be termed "commons control." Such a term does *not* necessarily imply that such control is absolute (although it could be). As Winston Churchill maintained concerning command of the seas: "When we speak of command of the seas, it does not mean command of every part of the sea at the same moment, or at every moment. It only means that we can make our will prevail ultimately in any part of the seas which may be selected for operations, and thus indirectly make our will prevail in every part of the sea."[5]

From that perspective, the United States possesses command of the commons or *commons control* today.

Future Challenge: From A2/AD to Commons Denial

Yet, despite conditions today, it is conceivable that a near-peer opponent could attempt to deny U.S. access and full utilization of the global commons, perhaps by 2050. Such an opponent would not necessarily be able to replicate America's commons control. Rather, it would seek a robust capacity for commons denial (in the conceptual manner of sea denial) within the 4000-6000 nautical mile extent that is currently unchallenged, as well as in space and cyberspace.

Although they has been some recognition that rising powers could contest U.S. dominance of the global commons, a future trans-global commons denial threat with substantial military effects has not yet been examined in detail. In an influential article, then-Undersecretary of Defense for Policy Michele Flournoy and co-author Shawn Brimley maintained that the relative balance of global power was shifting in ways that allow the commons to be "contested," but discussed the potential challenges in relatively modest terms, largely within the reach of current A2/AD systems closing the peripheries.[6] The authors did suggest, however, that "these developments challenge us to think creatively about how DOD can best develop the strategy, concepts of operations, and capability mix needed to meet this challenges."[7] With that in mind, now is the time to contemplate how U.S. forces in the 2050 time-frame could achieve "assured access" in the face of a severe commons denial threat.

It is not impossible, impractical or inappropriate to examine a potential 2050 threat—because strategies, tactics and systems will largely be *extensions of* and *advances in* A2/AD strategies, tactics and systems that *exist today*. Anti-access warfare is a strategy existent throughout history intended to cut off the opponent's use of the global commons, conducted at the level of technology available in the particular historical era. The principles of the strategy remains the same, and will remain the same in 2050, even as technology evolves. Moreover, much of the U.S. joint force—and certainly much of the U.S. Navy—available in 2050 will consist of platforms existing today or built in the years 2018-2030 (which means they will be based on designs and technologies emerging today). This is also true of emerging peers.

One can therefore discern an outline of the nature of this potential threat: undersea forces that can linger but a dozen miles from the ports of San Diego or Long Beach; conventionally-armed anti-ship ballistic missiles that can reach 2000-3000 nautical miles; anti-satellite satellites that can be positioned within the launch trajectories of Kennedy Space Station or Vandenberg Air Force Base; an alternative global internet network to which American access could be cut; and global norms that close off regional seas to non-regional military vessels, as a few examples.

In a commons denial strategy, the targets of the enemy may be extensively re-prioritized: combat logistics force and sealift first, aircraft carriers second. Potential opponents, if they intend to win, will not wait like Saddam Hussein in 1991 for the U.S. to build an "iron mountain" of power in their region. Today they construct A2/AD systems to deny U.S. access to *their* region. Tomorrow they will attempt to attack U.S. power before it moves outside *our* region.

Efforts Thus Far

As noted, these are threats that have hardly been intellectually examined, even by those tasked with assessing the future security environment. Postulating the extension of A2/AD systems into a commons denial construct is simply not part of the planning focus on "the fight tonight." At the same time, those examining the future appear fixated on the search for that fabulous beast, the "game changer"—the technology that makes "everything all different." Game changers are rare, possibly non-existent; the tools of commons denial can just as easily creep up as dramatically emerge.

The Naval Services do have a glimmer of the commons denial threat as reflected from the anti-access strategies it currently recognizes. The March 2015 revision of *A Cooperative Strategy for 21st Century Seapower* adds the "essential function" of "all domain access" to four previously enunciated functions (the previously fifth function of humanitarian assistance being subsumed into the category of missions). *All domain access* is defined simply as "the ability to project military force in contested areas with sufficient freedom of action to operate effectively."[8] The primary context is of operations within the range of existing A2/AD systems, and the document imports the concept of "cross-domain synergy"—the centerpiece of the 2012 Joint Staff *Joint Operational Access Concept* (*JOAC*)—as the required capability.

This context should be expanded beyond the focus of the *JOAC* to examine the practical requirements of all domain access in a future commons denial environment. Unfortunately, the follow-on joint document, *Joint Access and Maneuver in the Global Commons* (*JAM-GC*), released 19 October 2016, is but an anemic shadow. Organizationally, *JAM-GC* evolved out of the Air/Sea Battle Office, an unfortunate victim of political-academic alarmism and the cult aspect of jointness ideology. Instead of focusing, however, on assessing the operationally capabilities needed, the *JAM-GC* concludes that U.S. forces must be "distributable," "resilient," "tailorable," on a "sufficient scale," and of "ample duration" to ensure operational access to the global commons. Of course they should—but hopefully for *any and all types of operations*, whether dealing with the global commons or not. A recent description of the *JAM-GC* notes that "JAM-GC puts forth an evolutionary approach to joint force operations that centers on enhanced all-domain integration across Services and component lines…"[9] That may be a great description of the goal of all jointness; but it does not come to grips with the full challenge that denial of the commons would present to the joint force.

What is Needed

Now is indeed the time for military and civilian strategists to begin a more detailed examination of the potential of global commons anti-access and options for countering it. Some of the issues that should be examined include: (1) vulnerability of CONUS deployment ports and nodes, (2) effects of creeping "lawfare" efforts to de-legitimize freedom of the seas, (3) over-reliance on space and cyberspace for C2, (4) potential development of access denial/sea denial systems (such as modern strategic naval mining) than can confine our enemies, (5) ensuring stockpiles of strategic materials, (6) surge capacities in defense industries, and others. The eventual goal should be an integrated plan to ensure commons access. Since these issues have yet to be examined in the detail they deserve (due to our focus on "the fight tonight," the hope of a game changer, etc.), we are not yet ready to build such a plan. It is time to step beyond the platitudes of joint concepts. We cannot wait for 2050 to find that access to the global commons is too difficult to be the foundation of our global military power. In fact, without access to the global commons, we have no military power.

[1] For a more detailed explanation of the logic behind this definition, and how it relates to navies, see Sam J. Tangredi, "Beyond the Sea and Jointness," in Thomas J. Cutler, ed., *The U.S. Naval Institute on Naval Strategy* (Annapolis, MD: Naval Institute Press, 2015), pp. 141-150.

[2] It is logical to argue that the internet is a source of trade, or rather a trading platform, since so much of global financial exchange is conducted via the internet. However, financial investment and exchange exists for the purpose of facilitating trade in goods and services which cannot in themselves travel by internet. The cost of manufacturing by 3D printing is prohibitive except for plastics.

[3] For a discussion of Imperial Japan's strategy as anti-access warfare, see Sam J. Tangredi, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis, MD: Naval Institute Press, 2013), pp. 141-149.

[4] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28:1 (Summer 2003), pp. 5-26.

[5] From a speech in the House of Commons 11 October 1940.

[6] Michele Flounoy and Shawn Brimley, "The Contested Commons," U.S. Naval Institute *Proceedings* 135/7/1277 (July 2009), pp. 16-21.

[7] Ibid, 20.

[8] U.S. Department of the Navy, *Forward, Engaged, Ready: A Cooperative Strategy for 21st Century Seapower*, March 2015, p. 19.

[9] Michael E. Hutchens, William D. Dries, Jason C. Perdew, Vincent D. Bryant, and Kerry E. Moores, "Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept," *Joint Forces Quarterly* 84, 1st Quarter 2017, pp. 134-139.