Domain Restriction Zones

An Evolution of the Military Exclusion Zone

Cole M. Mooty
Robert A. Bettinger
Mark G. Reith

Since the early part of the twenty-first century, US adversaries have expanded their military capabilities within and their access to new warfighting domains. When faced with the growth of adversaries' asymmetric capabilities, the means, tactics, and strategies previously used by the US military lose their proportional effectiveness. To avoid such degradation of capability, the operational concept of the military exclusion zone (MEZ) should be revised to suit the modern battlespace while also addressing the shifts in national policy that encourage diplomacy over military force. The concept and development of domain restriction zones (DRZs) increase the relevancy of traditional MEZs in the modern battlespace, allowing them to address problems associated with cross-domain and multidomain capabilities. The growth of adversary capabilities provides a clear rationale for the implementation of DRZs through all levels of force application within the competition continuum.

Similar to its predecessor, the 2022 *National Security Strategy* prioritizes diplomatic resolutions over the potential direct application/threat of force, firmly emphasizing "using diplomacy to build the strongest possible coalitions," while ensuring military force is used as "a last resort."[1] Regardless, it remains the work of the Department of Defense to advance and safeguard vital US national interests by "backstopping diplomacy, confronting aggression, deterring conflict, projecting strength, and protecting the American people and their economic interests."[2] Warfighters must promote a Joint force that remains "lethal, resilient, sustainable, survivable, agile, and responsive," while able to support the American people in a manner beyond the greatest application of force: war.[3]

In accordance with US Air Force doctrine, this spectrum of conflict includes "a mixture of cooperation, competition below armed conflict, and armed conflict," encompassed

First Lieutenant Cole Mooty, USAF, a pilot trainee at Vance Air Force Base, holds a master of engineering in space systems from the Air Force Institute of Technology, Wright-Patterson AFB, Ohio.

Lieutenant Colonel Robert Bettinger, USAF, PhD, is assistant professor of aerospace engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio.

Dr. Mark Reith is assistant professor of computer science and adjunct assistant professor of systems engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio.

1. Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: The White House, October 2022), 16, 20, https://www.whitehouse.gov/
2. Biden, 20.
3. Biden, 21.

generally by the concept of the "competition continuum."[4] When taken in concert with national strategy, it is vital a Joint force uses a "wide variety of activities and roles that vary in purpose, scale, risk, tempo, and intensity"—specifically, tools capable of achieving national interests with efforts below the threshold of war.[5] Warfighters and policymakers alike should develop the means to pursue US security through the entirety of the competition continuum, while ensuring these means do not escalate conflict beyond their intended level of involvement.

Developing these methods requires planners and strategists recognize conflict in any form is inherently a competition—a competition in which the contenders are driven by action and counteraction in the totality of available warfighting domains. As one national security expert explains, "As competitors increasingly gain access to all domains of warfare, it becomes more likely that adversaries will seek to offset a competitor's dominance in one domain by acting more aggressively in another space."[6]

In the modern battlespace, adversaries have increased access to capabilities across all six domains of US military operations: subsurface naval, surface naval, ground, air, space, and cyberspace. Prevalent examples include the Islamic State of Iraq and the Levant's redoubled cyber operations against the West, the People's Republic of China's (PRC) expansion into the South China Sea, and Russia's Kosmos 2543 on-orbit antisatellite (ASAT) test in 2020.[7] Along the lines of these examples, as adversary technology and capabilities progress, it should be assumed that US multidomain accessibility will increasingly become contested rather than guaranteed.

Growth of adversary capabilities across the competition continuum and all domains has recently required the Joint force to prioritize multidomain operations, which "employ joint capabilities from all domains to complement and reinforce their own capabilities."[8] While the US military has devoted the majority of its "time, intensity, forces, etc." to the kinetic domination of an opponent "until the enemy is no longer able to effectively resist,"

4. US Air Force Chief of Staff, *The Air Force*, Air Force Doctrine Publication (AFDP) 1 (Maxwell AFB, AL: Curtis LeMay Center for Doctrine Development and Education, March 10, 2021), 2, https://www.doctrine.af.mil/.

5. Chairman of the Joint Chiefs of Staff (CJCS), *Joint Campaigns and Operations*, Joint Publication (JP) 3-0 (Washington, DC: CJCS, June 18, 2022), I-4.

6. James Jay Carafano, "America's Joint Force and the Domains of Warfare," Heritage Foundation (website), October 4, 2017, https://www.heritage.org/.

7. Stephen Burgess, "Confronting China's Maritime Expansion in the South China Sea," *Journal of Indo-Pacific Affairs*, August 31, 2020, https://www.airuniversity.af.edu/; Troy Smith, "The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare," *American Intelligence Journal* 34, no. 1 (2017); and Neel V. Patel, "The US Says Russia Just Tested an 'Anti-satellite Weapon' in Orbit," *MIT Technology Review*, July 23, 2020, https://technologyreview.com/.

8. Headquarters, Department of the Army (HQ DA), *Operations*, Army Field Manual (FM) 3-0, (Washington, DC: HQ DA, October 2022), 2-15, https://armypubs.army.mil/.

the modern battlespace is increasingly characterized by actors working at different points along the continuum.[9]

Therefore the modern warfighter must also ensure the tools and capabilities at their disposal remain relevant through cooperation and competition below armed conflict, as well as in the direct application of force. While some tools that remain effective in nonkinetic portions of the competition continuum prove ineffective in armed conflict, the counterpoint remains equally true: the application of tools used to prosecute war could prove detrimental to military actions and efforts that fall below the threshold of armed conflict.

Reconciling the growth of adversary capabilities across all warfighting domains with the *National Security Strategy* raises a pertinent question: Are the tools the US military provides the Joint force capable of meeting threats across all domains, as well as across the entire competition continuum? This article seeks to take the existing strategy of exclusion zones traditionally used for single-domain control and adapt it into a broad means of addressing adversaries in all domains within a greater context of operations.

Existing Architectures: Historical Exclusion Zones

Although the number of domains and the tools used to access them have changed over time, the nature of conflict has always caused adversaries to seek new avenues to degrade their enemies' ability to operate within a given area. The use of military assets to perform these actions can be accomplished through a military exclusion zone (MEZ). In a notional sense, the historical use of MEZs can be grouped into three categories pertaining to three domains: a terrestrial MEZ, preventing access to a terrestrial location; a maritime MEZ, preventing access to some stretch of water; or an air exclusion zone (AEZ), colloquially referred to as a "no-fly zone." Each type of MEZ is implemented through various means, recognized within the international community with differing degrees of acceptance, and subject to specific legal and international conventions.

Terrestrial MEZs

Historical precedence. Terrestrial MEZs have the broadest grounding in historical precedence and have been implemented—to different degrees—in almost every conflict between state-level actors. Perhaps the most famous examples in modern history are the Berlin Wall and Korea's Demilitarized Zone/Joint Security Area: both zones created stark divisions between neighboring states, with the constant "possibility of death as a direct result of enemy action" and the "criminalization of entrance attempts" through direct, often lethal, enforcement of travel restrictions.[10] Historical examples of terrestrial MEZs

9. CJCS, *Joint Operations*, *Incorporating Change 1*, JP 3-0 (Washington, DC: CJCS, October 22, 2018), https://irp.fas.org/.

10. Klaus Schroeder and Jochen Staadt, "Todesfälle an der innerdeutschen Grenze und am Eisernen Vorhang bis 1989," Bundesministerium für Bildung und Forschung, December 31, 2016, https://www.bmbf

include border check zones, military-enforced security checkpoints, and closed cities, which are all zones or terrestrial regions that use military force to prevent direct access without proper approval. These exclusion zones have acted through the entire spectrum of the competition continuum, deterring adversary actions in engagements that fall below the threshold of armed conflict, and have served as launching or staging points for armed conflict.

Current implementation. Today, terrestrial MEZs are identified by the existence of standing occupational forces and the use of military forces in base and border security. Terrestrial MEZs are clearly defined regions of land that have restrictions on entrance and movement. These locations—actively patrolled, controlled, or guarded by military forces—host existing US, Allied/coalition partner, or regional/international organization forces such as NATO and are legally recognized in the international community.

Furthermore, their continued use has deterred adversary aggression and gambits for regional dominance, while also proving invaluable in regional stabilization and civil authority establishment. In various capacities, these terrestrial MEZs can be modeled by facilities that include Ramstein Air Base in Germany and Al Dhafra Air Base in the United Arab Emirates, each a functionally different but pivotal US Air Force resource that continues to operate across all warfighting domains. Defense and enforcement of these locations is traditionally reliant on conventional forces and weapons.

Legality and international considerations. Terrestrial MEZs are unique relative to other forms of the MEZ. The governing principles for these zones are defined by international humanitarian law and individual state regulations and laws. The actions of military forces stationed in and around these zones are clearly defined, forces are trained accordingly, and the right to enforce the zone is carefully considered against the principles of jus in bello and jus ad bellum, with a strong consideration for historical precedence set by existing MEZs.

Maritime MEZs

Historical precedence. As one study suggests, the history and legality of the maritime exclusion zone has evolved through three distinct phases.[11] The first phase of the maritime exclusion zone traces its roots to the Russo-Japanese War of 1904–1905. These "Phase I" maritime MEZs were "defensive in character, modest in size, and located adjacent to the State that authorized their creation."[12] These maritime MEZs have little comparative analytical value for a frequently expeditionary military such as the US Armed Forces. Such zones fill the niche of general deterrence while also supporting direct regional dominance of the enforcing nation.

.de/; and Rolf Potts, "Korea's No-Man's-Land," Salon, February 3, 1999, https://www.salon.com/.

11. Sandesh Sivakumaran, "Exclusion Zones in the Law of Armed Conflict at Sea: Evolution in Law and Practice," *International Law Studies* 92 (2016), https://digital-commons.usnwc.edu/.

12. Sivakumaran, 155.

The maritime MEZs next developed into Phase II, with areas "far larger in size than the exclusion zones of the Russo-Japanese War . . . located, in certain instances, at quite some distance from the coast of the State authorizing them."[13] Such Phase II zones were the first examples of maritime MEZs where any vessel within was deemed susceptible to attack, regardless of the vessel's belligerency or neutrality. The historical use of Phase II maritime MEZs is perhaps best exemplified in the German U-boat campaign of World War I, which acted to shape the warfighting environment through resource restriction, deter adversaries from engaging in the conflict, and seize the initiative for the German navy while actively dominating the Eastern Atlantic.

Current implementation. Phase III maritime MEZs are typically rooted in the changes to maritime law introduced by the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, adopted in 1994.[14] The *San Remo Manual* established regulations for maritime MEZs and offers a definitive demarcation between their establishment and enforcement should they be created. The manual, though not internationally binding, has influenced doctrine in navies around the world. Specifically, the stipulation that "a belligerent cannot be absolved of its duties under international humanitarian law by establishing zones which might adversely affect the legitimate use of defined areas of the sea" has had a significant influence on the use of a Phase II-style maritime MEZ.[15]

The *San Remo Manual*, however, does not weigh in "on the inherent legality or illegality of exclusion zones, but regulates the zones in the event that the belligerents decide to create them."[16] As a result, Phase III maritime MEZs are typically subjected to, and judged with, individual consideration, specifically as their own terms relate to the rules of the law of the sea. In their current implementation, these Phase III maritime MEZs have been involved with elements of the competition continuum that fall at or above the threshold of armed conflict. These maritime MEZs are most readily applied by enforcing nations to seize the initiative from adversaries or dominate the targeted region directly.

Legality and international considerations. To determine the legality of maritime MEZs, the UN Convention on the Law of the Sea (UNCLOS) has two clauses of particular interest. The first is Article 88, which mandates that "the high seas be reserved for peaceful purposes" and seeks to guarantee "freedom of navigation, freedom of overflight, and freedom of fishing."[17] But this is restricted by Article 301, which allows the "exercise of conditions laid down by this Convention and by other rules of international law,"

13. Sivakumaran, 155.

14. Various authors, *San Remo Manual of International Law Applicable to Armed Conflicts at Sea, 12 June 1994* (International Institute of Humanitarian Law, Livorno, Italy, 1994), https://ihl-databases.icrc.org/.

15. *San Remo Manual*, 17, note 105.

16. Sivakumaran, "Exclusion Zones," 194–95.

17. UN General Assembly, United Nations Convention on the Law of the Sea (UNCLOS), December 10, 1982, https://www.un.org/.

effectively leaving the door open to consider exclusion zones, blockades, and associated measures as legitimate under the "rules in the law of armed conflict at sea."[18]

In general, the legal frameworks tied to maritime MEZs have continued to be unclear when the enforcing nation is required to defend their maritime MEZ's legitimacy within the realm of international law. One fact which rules supreme in international convention, however, is that a vessel's protection under international law, regardless of belligerency or neutrality, does not change simply because the vessel crosses an "imaginary line" constituting the boundary of a zone.

US implementation of maritime MEZs. The US military has incorporated the *San Remo Manual* approach to maritime MEZs, as noted in the 1997 and 2007 *Annotated Supplements to the Commander's Handbook on the Law of Naval Operations* published by the US Navy. The supplement notes that "such zones serve to warn neutral vessels and aircraft away from belligerent activities," and stipulates that "to the extent that they do not unreasonably interfere with legitimate neutral commerce, they are undoubtedly lawful."[19]

Air Exclusion Zone or No-Fly Zone

Historical precedence. The history of the air exclusion zone (AEZ) is significantly shorter than either the terrestrial or maritime MEZ. The first practical implementation of a no-fly zone is also arguably its most famous example: the post-1991 Gulf War no-fly zones over Iraq. Follow-on implementations of AEZs include coalition no-fly zones enforced over Bosnia and Herzegovina between 1993 and 1995 that included a UN Charter right for member states to "take all necessary measure to ensure compliance with the no-fly zone restrictions."[20] Recent examples of no-fly zones include AEZs enforced over Libya between 2011 and 2019.

Unilaterally, AEZs are characterized by a significantly more stringent implementation than maritime MEZs, defined by direct and often lethal use of force against any agent that violates the terms of the no-fly zone, regardless of belligerency or neutrality. This causes the legality of AEZs to be dubious at times and has brought into question the ethics of their implementation related to the potential loss of innocent life. It has furthermore severely limited the utility of an AEZ for cooperation and competition below armed conflict, as such rigid enforcement practically guarantees involvement beyond the threshold of armed conflict.

Current implementation. Contemporary no-fly zones are both a political tool and an implementation of direct military force. Though frequently enforced by the US military or some form of coalition forces, they are established by démarche. Current AEZs are

18. UN General Assembly, UNCLOS; and Sivakumaran, "Exclusion Zones," 196.

19. A. R. Thomas and James C. Duncan, eds., *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (Newport, RI: US Naval War College, 1999), 7.9, *International Law Studies* 73 (1997), https://archive.org/.

20. UN Security Council, Resolution 816, Bosnia and Herzegovina, March 31, 1993, S/RES/816 (March 31, 1993), https://www.refworld.org/.

implemented as either "declaratory policy, not subject to enforcement," or "operational policy, subject to enforcement and military action."[21] In general, no-fly zones are a clear departure "from traditional airpower missions by their imposition in another nation's airspace, absent of war, surrender, or occupation."[22] This distinct tie to the use of military force for the pursuit of national objectives below the threshold of war makes the AEZ a tool that can be expanded across the entire competition continuum.

Legality and international considerations. The implementation of no-fly zones traditionally occurs when the enforcing state invokes Article 42 of the UN Charter, a stipulation that the UN Security Council "may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[23] The situation is complicated by the fact that "there are no existing legal definitions or criteria for a no-fly zone," and their establishment and enforcement lie ambiguously in the realm of permissibility—they are neither explicitly allowed nor explicitly denied by international convention, leaving their legality up to case-by-case interpretation.[24]

The legality of an AEZ is determined by the UN Security Council, frequently well after such a zone's establishment: the Gulf War no-fly zone is a clear example of such rulings. Though invoked as part of UN Charter Article 42, the 2003 UN secretary general deemed the no-fly zone was illegal as well as not directly authorized 12 years after the zone's establishment. This places no-fly zones in a similar position as maritime MEZs, lacking explicit approval or denial, but with noticeably less international and historical precedence to guide an enforcer's actions.

US implementation of AEZs. The US military recognizes that a "no-fly zone is a *de facto* aerial occupation of sovereign airspace in which . . . only aircraft of the enforcement forces may fly."[25] In terms of strategy, however, no-fly zones have had questionable effects. The AEZ as a tool is not constrained by its military utility, but rather by its management, institution, and prosecution by policymakers and warfighters that seek to achieve that which an AEZ is not made to do.[26]

Understanding the regional impacts of an AEZ prevents such a tool from overriding or harming national interests once direct armed conflict ceases and regional stabilization and transition to civil authority return. These requirements are compounded by the fact that "a no-fly zone relies on . . . conventional deterrence backed by the resolve to swiftly

21. Jan-Marc Jouas, "No-Fly Zones: An Effective Use of Airpower, or Just a Lot of Noise" (research report, US Air Force Academy, January 6, 1998), 2, https://apps.dtic.mil/.

22. Jouas, 2.

23. UN General Assembly, UN Charter, signed June 26, 1945, https://www.un.org/.

24. Jouas, "No-Fly Zones."

25. Michael M. Schmitt, "Clipped Wings: Effective and Legal No-Fly Zone Rules of Engagement," *International Law Studies* 72 (1998): 240, https://digital-commons.usnwc.edu/.

26. Alexander Benard, "Lessons from Iraq and Bosnia on the Theory and Practice of No-Fly Zones," *Journal of Strategic Studies* 27, no. 3 (September 2004), https://papers.ssrn.com/.

and ferociously enforce it if challenged."[27] In the face of antiaircraft artillery, man-portable air defense, or advanced surface-to-air missile systems, enforcing no-fly zones in this manner becomes "neither operationally feasible nor politically appetizing."[28] The utility of an AEZ is much more questionable than that of a terrestrial MEZ or maritime MEZ, especially in an environment where direct application of force is unappetizing.

A Military Exclusion Zone Overview

The key attributes of an effective military exclusion zone are defined as follows:

Observable targets. In 1978, the first protocol addendum to the Geneva Conventions of 1949 rightfully led to "the prohibition of indiscriminate attacks" in "international and non-international armed conflicts."[29] As MEZs inherently result in the targeting of any force entering a specific region, reducing collateral damage mandates that targeted assets be clearly defined and observable. This is even more important in modern combat, where assets act in, and threaten across, multiple domains in conditions of compressed time and increased lethality.[30]

Looking forward, effective MEZ implementation will require planners and strategists to "solve the physics of this expanded battlespace and understand the capabilities each domain can provide," rather than simply define generic target assets. Whereas the previous definition of a military exclusion zone could be as generic as a no-fly zone, the modern MEZ requires details such as the target aircraft type and capability.[31] A properly defined target might be a fighter aircraft capable of supersonic flight and carrying munitions, which could be identified through available sensors and detection technology.

Boundaries. A successful MEZ clearly defines its boundaries.[32] Furthermore, an effective MEZ should "represen[t] these elements in a physically based framework" to clarify "an already very complex multi-domain operating environment."[33] Fundamentally, for a modern MEZ to prove successful, it should definitively lay out the physical space within which it functions. These boundaries should be distinct and internationally recognizable, such as a certain radius from a given latitude and longitude point, or a geographically defined space an aircraft could overfly.

---

27. Mike Benitez and Mike Pietrucha, "The Dangerous Allure of the No-Fly Zone," War on the Rocks, March 4, 2022, https://warontherocks.com/.
28. Benitez and Pietrucha.
29. International Committee of the Red Cross, "Protocol II to the Convention on Certain Conventional Weapons, Article 3(3)," Committee on International Humanitarian Law, October 1986.
30. US Army Training and Doctrine Command (TRADOC), *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025–2040*, Version 1.0 (Fort Eustis, VA: TRADOC, December 2017), i, https://www.tradoc.army.mil/.
31. TRADOC, ii.
32. TRADOC, 8.
33. TRADOC, 8.

Communication. Across the board, military exclusion zones require clear communication of intent to all involved parties. Today's adversaries "challenge the traditional metrics of deterrence by conducting operations that make unclear the distinctions between peace and war."[34] The enforcing party and parties involved—willingly or not—with or contained within the zone must communicate directly and clearly. The battlespace of the late twentieth century to today contains a dynamic mixture of state and nonstate actors, both potential targets within an MEZ; as such, enforcement is crucial. Perhaps the cleanest example of effective communication is the announcement and subsequent enforcement of AEZs over Bosnia in the 1990s and Libya in the 2010s, where clear target and location definitions were communicated and prosecuted.

Flexibility. The modern Joint force is focused on "deterring escalation through the application of flexible deterrent options"; a successful MEZ, as part of this Joint effort, must be sufficiently flexible, adapting to changing actors within the zone.[35] Aircraft, depending on the platform, could also serve other purposes, including transportation of personnel and goods, so defining a method for such an asset to selectively operate within the MEZ is important. A waiver mechanism capable of allowing actions for recognized parties, specifically actions prohibited by the type of MEZ in consideration, would be invaluable in the successful prosecution of the desired end-state of the zone.

Mediation. The successful mediation of an MEZ requires two specific developments. First, to abide by international convention, the laws of armed conflict, and the accepted morality of war, there must be a means to de-escalate violent enforcement. For an MEZ to fulfill its role of controlling "the escalation and de-escalation of crisis," across the continuum of competition including reducing collateral damage, there must be a defined, routine, nonviolent method of resolving infractions in addition to the kinetic enforcement.[36] Second, an MEZ must have a defined, nonviolent resolution or exit strategy. De-escalation of an MEZ ensures that final de-escalation "maintains or improves conditions favorable to US interest."[37]

Current Military Exclusion Zone Limitations

The understanding and execution of military exclusion zones are limited to four of the six warfighting domains available. Applying MEZ tools in today's battlespace, however, necessitates changes to nomenclature and enforcement to permit flexibility across all domains. The US position of power is jeopardized when an adversary's asymmetric capabilities allow it to distract or detract from US control in another domain; changing the way the United States implements MEZs to address this lack of context on the warfighting scale is the next step.

34. TRADOC, 2.
35. TRADOC, 21.
36. TRADOC, 5.
37. TRADOC, 46.

Additionally, current MEZs are inherently limited by the geographic domains they encompass. Multidomain weapons used by US adversaries are not countered by the geographic boundary requirements of a military exclusion zone. Current MEZ architectures may address some cross-domain capabilities such as maritime MEZs, which frequently also restrict the airspace above their maritime locality. MEZ enforcement, however, is ineffective at restricting asymmetric influence from domains that chafe against traditional physical definitions—that is, space and cyber architectures. The specificity of a military exclusion zone to the domain within which it is employed severely limits the ability of the MEZ to degrade an adversary's cross-domain capabilities. This is true even if the zone is employed across all four historically involved domains—for example, the total exclusion zone as implemented by the United Kingdom during the Falkland War. Among other effects, communications, transportation of resources, and intelligence-gathering sources increasingly span numerous domains, further requiring a redefinition of the traditional MEZ.

In addition to geography, these zones are limited by the nature of the domain they target. As noted, a successful MEZ requires definable, observable targets. The zone actors, assets, and potential targets within the four historical domains are physical in nature and therefore subject to observation and classification. The modern battlespace, however, is not entirely classifiable in a physical sense. Although certain targets in the space domain are physical in nature and can be observed, the same cannot be directly extended to cyberspace. In particular, the cyber domain is still in the fledgling stages of both development and understanding: The inherent agility, flexibility, and pure adaptability of cyber domain maneuvering require that targets be treated differently than other domains.

Domain Restriction Zones

This article contends the concept of an MEZ may be applied more broadly, and that a novel domain restriction zone (DRZ) should be designed to flexibly exert tools of national power through any domain or combinations of domains against a desired adversary (fig. 1).

Defining these restriction zones comes as a function of five key domains: a land DRZ that would be the modern application of a terrestrial MEZ; a sea DRZ that would be the modern application of a maritime MEZ (for both the naval surface and naval subsurface domains); an air DRZ that would be the modern application of an air exclusion zone; and the new additions of space and cyberspace DRZs that extend the concept of an MEZ into domains to which it has yet to be applied. The first three of these principally involve a rebranding and do not require further definition or explanation. Space and cyberspace DRZs, however, are a new concept.

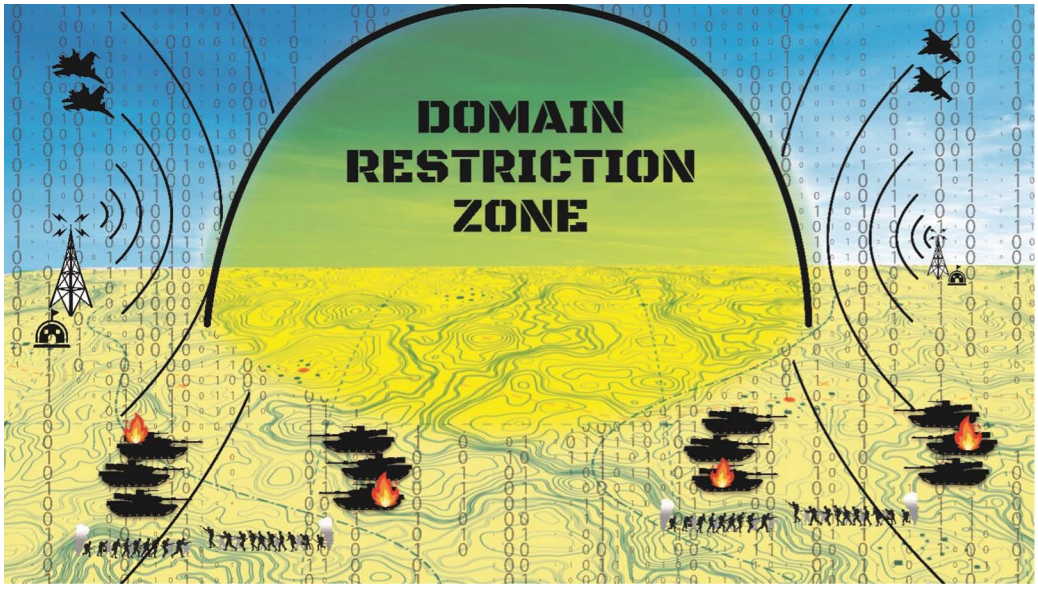

Figure 1. A notional domain restriction zone

Space Domain Restriction Zone

The space domain has two key differences relative to the other domains. These differences relate directly to the nature of historically successful MEZs and lead to some different attributes necessary for success.

Boundaries. First, space DRZ boundaries cannot be determined in a geographical manner. Space is an inherently mobile domain, with existing satellite architectures moving along their orbits. Defining a domain restriction zone in purely geographic terms would require the direct threat of destruction to any and all satellites whose orbits overfly the geographic zone, regardless of the capabilities they possess. A space DRZ is, therefore, more readily defined as a cross-reference between capabilities and locations. Whereas an air DRZ would prevent overflight within a certain defined region, a space DRZ would reduce or remove an adversary's space-based capabilities—such as communications, imagery, or positioning information—within that region, rather than space-based assets.

Observable targets. Second, the scale of the assets and systems in play in space is significantly greater than those in other domains. Space architectures are expensive relative to assets in other domains due to space-lift costs and the inability of asset servicing, necessitating complex, high-value systems for continued on-orbit missions' operations for years or even decades. Furthermore, space assets are often strategic in nature. Threats against strategic assets, in any capacity, are universally seen as a touchpoint for war, further raising the stakes of emplacing a space DRZ relative to other domains. Red lines that, if crossed, could lead to international conflict must be closely observed so that using a space DRZ does not cause direct escalation to war.

Tools to employ. Although the tools and assets that would be used to enforce land, sea, and air DRZs are already well defined—that is, surface-to-air missile systems, mines, guarded fortifications, and others—the tools used to enforce a space DRZ are less so. Understanding the enforcement tools will also further clarify how the zone itself should be defined. These tools include "extant capabilities to deny, disrupt, or physically destroy space systems."[38] They are traditionally identified as offensive counterspace capabilities, which include denial and deception measures, electronic warfare capabilities, ground station attacks, space mines, and both co-orbital and direct-ascent ASAT weapons.[39]

- **Denial and deception.** Actors can enforce space DRZs by directly defeating satellite "orbital and sensor characteristics."[40] Knowledge of an asset's capabilities, specific sensors and equipment, and critical sensor usage times allow the DRZ enforcer to pinpoint not just the physical asset, but specific effects. Examples of service denial include satellite dazzling or blinding of satellite sensors/payloads; spoofing, or the insertion of "fake instructions" to a satellite; and effects specific to the targeted system, or "selective availability," which is the targeted accuracy reduction of GPS signals.[41] In general, any means of denying the adversary's use of sensors or the quality and accuracy of the data collected may be effective ways to enforce a space DRZ.
- **Electronic warfare.** The majority of commercial and civil satellites do not have built-in protection capabilities and are vulnerable to electronic jamming capabilities that can disrupt their bus and/or payload functions.[42] A prime example of this form of offensive counterspace is GPS jamming. As identified by one study, "the weakness of GPS signals . . . provides a range of opportunities for criminals, terrorists and state actors using GPS jamming devices."[43] Analogous to terrestrial jamming, electronic warfare provides less kinetic means of restricting space architectures.
- **Ground station attack.** Offensive counterspace capabilities are not limited to targeting the satellite and on-orbit architecture. An alternate method for disrupting and/or degrading space architectures, thus avoiding the need for accurate targeting or more advanced weapons systems, is to attack the ground station(s). Though simplistic and limited by the increasing scope and accessibility of space architectures in general, strikes ranging from physical attacks to the intrusion of computer

38. Commission to Assess United States National Security Space Management and Organization [Space Commission], *Report to the Commission to Assess United States National Security Space Management and Organization*, January 11, 2001, viii, https://spp.fas.org/.

39. Space Commission.

40. Space Commission, 19.

41. Bruce M. DeBlois et al., "Space Weapons: Crossing the U.S. Rubicon," *International Security* 29, no. 2 (2004): 57, http://www.jstor.org/.

42. Space Commission, *Report,* 19.

43. Tegg Westbrook, "The Global Positioning System and Military Jamming: Geographies of Electronic Warfare," *Journal of Strategic Security* 12, no. 2 (2019): 1, https://www.jstor.org/.

networks provide an easily accessible manner of disruption.[44] Such attacks prove effective against adversaries with limited space accessibility—such as insurgencies and terrorist organizations—or low resiliency in space command-and-control architectures.

- **Space mines and co-orbital ASATs.** Satellite proximity operations are another way to enforce a space DRZ. Employing small explosive devices or kinetic/directed energy weapons on-orbit enables the DRZ enforcer to physically threaten an adversary's space systems. While the concept of space mines represents a broad spatial threat against the orbital regime targeted by the DRZ, the use of co-orbital ASATs could provide a means for guided close-in intercept to yield a potentially "fatal collateral blow to the satellites intended" or to force an adversary to maneuver to avoid collision.[45] The threat of these techniques, and the likelihood they would cause conflict escalation, is likely greater than that of the denial, deception, or electronic warfare methods, which yield more transient effects on targeted assets.
- **Direct-ascent ASAT capabilities.** A no-fly zone is characterized by direct, often lethal, engagement of force against adversary forces violating the region. This translates directly into the space DRZ as the direct-ascent ASAT mission, which uses a ground-, sea-, or potentially air-based system to destroy an adversary's space-based asset. And similar to space mines and co-orbital assets, these technologies have the potential to trigger broader conflict.[46]

Cyberspace Domain Restriction Zone

Cyberspace is an even less defined or constrained domain than space, affecting global society and critical infrastructure.[47] A general restriction of an adversary's access to cyberspace, as the traditional interpretation of an MEZ requires, is impractical for three reasons innately tied to the differences between the cyber domain and other domains.

Boundaries. First, a total cyberspace phase restriction is infeasible to enforce, as its scope and breadth is tied so deeply into every aspect of modern life. Cyberspace as a domain cannot be delineated by geography or cleanly cut into sections that interact with each other. Rather, it is integral to the information environment. Cyberspace "continuously

44. Space Commission, *Report*, 19.

45. DeBlois et al., "Space Weapons."

46. Kurt Gottfried and Richard Ned Lebow, "Anti-Satellite Weapons: Weighing the Risks," *Daedalus* 114, no. 2 (1985): 168, https://www.jstor.org.

47. Nick Ebner, "IFAR Fact Sheet: Cyber Space, Cyber Attack, and Cyber Weapons: A Contribution to the Terminology" (paper, Institute for Peace Research and the Security Policy at the University of Hamburg, October 2015), 1, https://ifsh.de/.

interacts with individuals, organizations, and systems" across dimensions that meld between "the physical, informational, and cognitive."[48]

Observable targets. Second, potential targets in cyberspace differ from those of the other domains. Though this domain contains observable targets such as the infrastructure and systems through which cyberspace maneuvering is accomplished, the cognitive and informational aspects are less conventionally observable. Cyberspace requires users to understand the movement of "content and code between humans and machines with the goal of getting them to act"—chiefly to act in a manner beneficial to the enforcer.[49] Finally, the cyber domain is characterized by agility; efforts to restrict movement lead to adversary adaptation—likely at a rate much greater than the enforcer's ability to restrict. The "continuous intertwining of cyberspace and human activity," as well as the agility of content and code as it pertains to shaping action, makes clear target definition in the cyber domain vastly different than target refinement in other domains.[50]

Flexibility. Third, the range of the cyberspace domain ensures that domain restrictions could include persistent comprehensive attacks on national and international security.[51] With this in mind, one should recognize cyberspace operations have traditionally sought to "disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[52] This highlights a key consideration that should be carefully evaluated for a cyberspace DRZ: collateral damage. Enforcement of restrictions on an adversary's cyberspace capabilities has the potential to adversely affect those who are not targets of the restriction; such actions must avoid being "excessive in light of the overall military advantage anticipated."[53] To mitigate collateral damage associated with cyber activities, the flexibility of actions in the cyber domain requires more consideration than other domains.

Tools to employ. Joint Publication 3-12, *Cyberspace Operations*, identifies three primary core cyberspace activities: military operations in and through cyberspace, national intelligence operations in and through cyberspace, and DoD "ordinary business operations in and through cyberspace."[54] The first of these core activities provides a ready reference for DRZ enforcement mechanisms available to the US military.

- **Civil operations.** The Department of Homeland Security is responsible for "strengthening cybersecurity resilience across the nation and sectors, investigating

48. Richard Crowell, "Some Principles of Cyber Warfare—Using Corbett to Understand War in the Early Twenty-First Century" (Corbett Paper No. 19, King's College London, Corbett Centre for Maritime Policy Studies, January 2017), 3–4, https://www.academia.edu/.

49. Crowell, 4.

50. Crowell, 4.

51. Ebner, "IFAR Fact Sheet."

52. James Cartwright, "Joint Terminology for Cyberspace Operations," memorandum, Vice Chairman of the Joint Chiefs of Staff, August 18, 2009, https://info.publicintelligence.net/.

53. Cartwright.

54. CJCS, *Cyberspace Operations*, JP 3–12 (Washington, DC: CJCS, June 8, 2018), II-9, https://info.publicintelligence.net.

malicious cyber activity, and advancing cybersecurity alongside our democratic values and principles."[55] One subordinate agency, the Cybersecurity and Infrastructure Security Agency, is the nexus for coordination and information across public and private entities. This agency is positioned to work with sovereign counterparts and international telecoms to observe activity in a defined cyber domain restriction zone.[56]

Consider a commercial datacenter in a neutral country or a geographical area where wireless emanations are highly regulated. Parties to a cyberspace DRZ agreement might send civil representatives to observe operations, signals, and data flow to provide transparency and assistance in securing the agreed-upon DRZ. This cooperative effort could ensure adversary military resources and activities are absent and increase the likelihood that third-party operatives are also excluded. This approach would primarily occur before conflict and likely require similar laws across all parties and the neutral host in order to leverage the civil legal and policing capabilities. As the situation escalates, a sovereign country might transition to military operations.

- **Military operations.** The tools available to enforce a cyberspace DRZ fall under the umbrella of two different operations: cyberspace exploitation and cyberspace attack. Cyberspace exploitation includes "military intelligence activities, maneuver, information collection, and other enabling actions."[57] Exploitation typically relates to discovering vulnerabilities, enabling target development, and supporting the planning, execution, and assessment of military operations. This probing and determination step is invaluable to planning relevant cyberspace attack follow-ons that enforce the desired capability restrictions of the cyberspace DRZ.

  Cyberspace attack is focused on the two primary efforts of service denial and service manipulation. To deny, the US military attempts to "prevent access to, operation of, or availability of a target[ed] function by a specific level for a specific time," through the means of degradation, disruption, or destruction.[58] Note that disruption is the case where degradation is set to a level of 100 percent for the desired span of time, while destruction is a relative term as the majority of cyberspace targets are subject to reconstitution with sufficient time and resources.

  The techniques here range widely in potential and include network throttling, such as the intentional degradation of internet speed and web performance; denial of service attacks; man-in-the-middle attacks; malware attacks; ransomware; URL interpretation; DNS spoofing; transmission interruption; jamming of signals; and a whole host

55. US Department of Homeland Security (DHS), "Cyber Mission Overview," DHS (website), October 3, 2022, https://www.dhs.gov/.
56. DHS.
57. CJCS, *Cyberspace Operations*, II-6.
58. CJCS, II-7.

of other offensive capabilities.[59] The nature of cyberspace attack makes the enforcement of these restrictions a very flexible, dynamic process.[60]

Employing domain restriction zones to create restrictions across multiple domains will increasingly become a requirement in order to successfully counter adversary multidomain weapons systems and capabilities. For example, a DRZ could restrict a targeted nation's communications capabilities. Such an operation would require presence in no less than four domains—land, air, space, and cyberspace—restricting the targeted nation's potential communication capabilities across these nonmaritime domain distinctions (fig. 2). This means of selecting both a capability to restrict and a region or space within which to restrict it is paramount to not only space and cyberspace DRZs in particular, but also the concept of a DRZ in its totality.

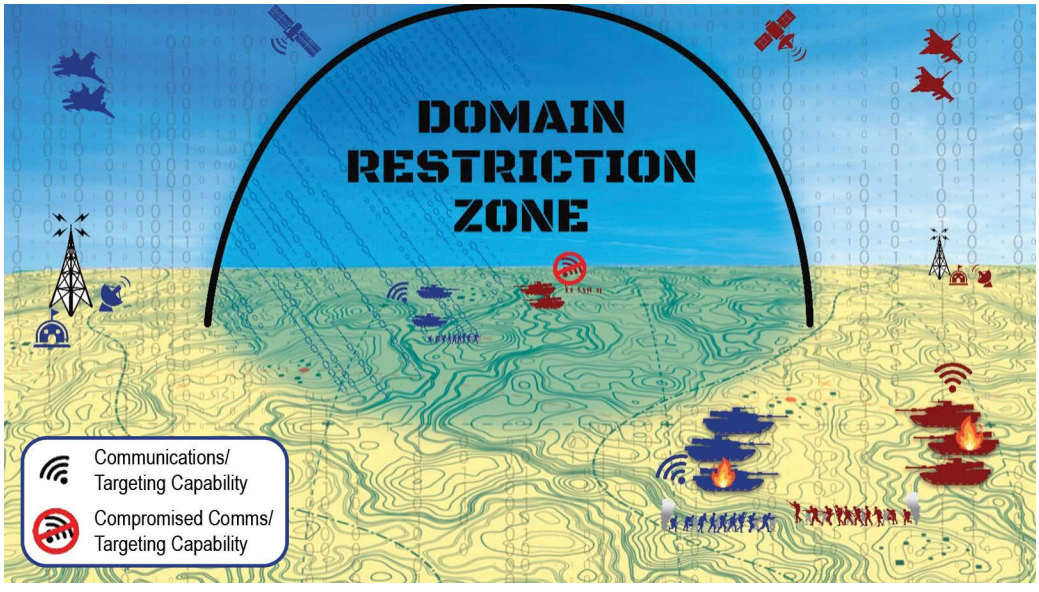

Figure 2. A notional domain restriction zone restricting adversary communication capabilities across land, air, space, and cyberspace, within a nonmaritime geographic location

Cross-referencing figures 1 and 2 against the current operational planning phase framework demonstrates the flexibility and utility this framework provides for a tool such as a domain restriction zone. First, a DRZ can produce the same effects as a military exclusion zone across domains: By enforcing limitations on space operations enforcement

59. FortiGuard Labs, *Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs*, Fortinet (website), February 2022, https://www.fortinet.com/.

60. Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," Cato Institute, January 15, 2019, https://www.cato.org/

mechanisms and shaping opponent action through cyberspace attack and exploitation, the DRZ could deter and/or incapacitate enemy forces in a given region. By targeting all enemy capabilities, a DRZ focused on total cyberspace restriction could produce an optimal environment within which to operate or stabilize a region while ensuring the development of a reliable civil authority.

When one of the involved parties seeks to seize the initiative in conflict or dominate a given region, the ability to target a given capability in that region, such as communication or targeting capabilities, is critical. Figure 2 highlights the benefits of changing an MEZ model toward a DRZ focus. By cross-referencing a desired capability restriction with the physical region targeted, a DRZ would prove a decisive factor in engagements within the targeted region.

Instead of focusing on force exclusion—the prevention of enemy presence and action in a region—a DRZ focuses on the capabilities, seeking to shape adversary action by limiting an adversary's warfighting ability, guiding the manner in which such an engagement would be prosecuted, and applying general pressure to belligerents in and around the targeted location. The domain restriction zone answers the shortcomings of the military exclusion zone problem by providing flexibility, adapting to domains where exclusion is infeasible, and targeting capabilities rather than assets. This combination makes an increasingly irrelevant tool practical for the modern warfighter.

Conclusion

Military exclusion zones have historical and military precedent as wartime and peacetime tools. Yet MEZs increasingly have reduced utility due to interdomain ties and the movement of assets and capabilities into domains not covered by MEZ architectures. Eliminating this tool is impractical and detrimental to planning for the contemporary battlespace; instead it must be adapted, particularly as existing MEZ considerations can simply be pivoted to a more relevant model: the domain restriction zone. Applying the idea of domain restrictions zones to certain targeted adversary capabilities provides the path forward for the traditional MEZ and offers a revitalized tool to policymakers and war planners. The flexibility gained by the multidomain approach, the dynamics available when targeting desired capabilities, and the focus on managing the escalation of force fits the DRZ into a greater context of the competition continuum while keeping it grounded in international precedence and reasonability. ✈