Agreed Competition in Cyberspace[1]

Michael P. Fischerkeller and Richard J. Harknett

Two strategic games are possible with cyber operations and campaigns, each with different rules and dynamics. The United States has focused almost exclusively on the strategic game of armed conflict in the cyber domain, while many states are playing the strategic game of competition. Recognizing the differences between armed conflict and competition is essential to maintaining strategic stability in cyberspace.

Agreed competition is a unique, structurally derived and defined phenomenon of cyberspace that allows for a better understanding of the cyber strategic competitive space short of armed conflict.

Introduction

Pursuing U.S. objectives in the operational domain of cyberspace requires strategies that can succeed in armed conflict and the competitive space short of armed conflict. Arriving at acceptable behavioral norms requires explicit bargaining in the strategic space of armed conflict. But a tacit bargaining approach is the better starting point for producing mutual understandings of acceptable and unacceptable behavior in the competitive space short of armed conflict. Empirical evidence suggests that a form of *tacit agreed competition* is ongoing in this competitive

[1] Based on M. P. Fischerkeller and R. J. Harknett, “What Is Agreed Competition in Cyberspace?” *Lawfare*, February 19, 2019, https://www.lawfareblog.com/what-agreed-competition-cyberspace.

space. In this essay, we explain the logic of agreed competition in the cyber operational domain.

Defining Agreed Competition

We have argued that a strategy of deterrence for cyberspace is appropriate in the strategic space of armed conflict but that a strategy of persistent engagement is more appropriate in the cyber strategic competitive space short of armed conflict (see Fischerkeller and Harknett 2017). Strategic escalation, through threat or action, can provide an advantage in limited conflicts, according to Herman Kahn (1965). In limited conflict, deterrence is only as effective as the threat of escalation is credible. Deterrence is combined with the threat of escalation to achieve escalation dominance—the condition in which an adversary's response must be either to accept the status quo or to back down. Coercive escalation strategies like those developed by Kahn are viable in the strategic space of armed conflict, including cyber, due to the nature and threat of war.

Kahn described another way adversaries could seek to gain strategic advantage in conflict—by making use of factors associated with a particular level of escalation he called *agreed battle*. Agreed battle manifests when adversaries have strategic rationales to not escalate. Agreed battle does not imply a shared understanding, an intention of indefinite containment, or even a conscious quid pro quo arrangement. The concept combines the range of conflict agreed upon and the acceptable and unacceptable behaviors within that conflict space. Interactions between adversaries are necessary to reach agreement on these conditions. The way to gain strategic advantage is by adopting an approach within the battle's structural boundaries. The resulting dynamic is competitive interaction within those boundaries, rather than spiraling escalation into new levels of conflict.

With the concept of *agreed competition*, we have refined Kahn's concept of agreed battle to better align with the cyber strategic competitive space short of armed conflict. Behaviorally, cyber actors appear to have tacitly agreed on the bounds of this space as being between operational inactivity and operations just short of what would generate the cyber equivalent of armed attack. The strategic dynamic that follows from continuous cyber operations, then, is competitive interaction within agreed competition's boundaries, not escalation out of them.

The tacit agreement over the substantive character of acceptable and unacceptable behaviors within agreed competition's boundaries is still being formed. The United States has not agreed, for example, that China's theft of intellectual property and personally identifiable information is acceptable behavior. The United States is in the early stages of an agreed competition with China in which the structural boundaries are tacitly understood, but mutual understanding of acceptable and unacceptable behaviors are still being developed through competitive interaction. We expect that a more active U.S. strategy of persistent engagement will help define the character of acceptable cyber competition and differentiate it from cyber armed conflict.

Advantages of Adopting the Agreed Competition Concept

Kahn's mechanisms of escalation (i.e., widening the area, compounding, and intensifying) can be repurposed so that an operational objective of persistent engagement is to inhibit an adversary's attempts at the same. Persistent engagement can inhibit adversary campaigns that seek to increase the number of systems affected (widening cyber); the number of actors affected or implicated as causing an effect (compounding cyber); and increase the frequency, duration, level, and visibility of effects (intensifying cyber).

This framework highlights three concerns regarding the stability of agreed competition:

1. Some states may seek to legitimize significantly disruptive cyber actions or operations short of armed conflict while the substantive character of agreed competition is still maturing.
2. Differing perspectives about types of acceptable campaigns or operations introduce avenues for unintended escalation out of agreed competition. Such uncertainty will affect both actors with harmful intent and states exploring this competitive space with defensive objectives.
3. Imbalances in outcomes of long-term competitive interactions will produce shifts in relative power that may lead to instability; when a state experiences a decline in power and senses rising competitors, the incentive for deliberate escalation into armed conflict increases.

All significant actors face challenges in agreed competition, and clarifying these challenges would help ensure stability. Seeing the strategic competitive space as agreed competition highlights the strategic pitfalls of advancing interests too assertively and highlights areas that require further study. Adversaries in this competitive space have mutual interests in avoiding escalation to violent conflict, and these interests could be the basis for explicit or tacit bargaining in support of stability.

Agreed Competition does not Apply to Other Military Operating Domains

The land, maritime, and air military operational domains share the same core structural feature—segmentation (see Fischerkeller and Harknett 2017). Segmentation derives from states exercising their sovereign rights within recognized boundaries. When states move out of the space short of armed conflict into open war, sovereignty is violated, and those domains become connected temporarily. However, in non-conflict situations, segmentation is the enduring structural feature of the land, maritime, and air domains. The military operating domain of space is different because space is accepted as commons by international agreement, meaning that space is not subject to national appropriation by claim of sovereignty. However, the absence of sovereignty-derived segmentation in space does not imply structural interconnectedness. National systems operate within the commons without connection to each other.

Segmentation does not produce a structural disincentive to escalate in these domains. It results in a condition of episodic contact, during which the incentivize is to use escalation as the strategic approach. Land, maritime, air, and space capabilities reflect this; they are designed and developed to coerce and deter, and, should that fail, to prevail in conflicts through threats of or actual escalation in uses of force. National interests in these domains can be advanced by holding capabilities in reserve or holding at risk (on the basis of prospective threat). These actions would not apply in a cyber strategic competitive space short of armed conflict, which demands persistence.

Agreed Competition is not the Same as Gray Zone Challenges

Kapusta (2015, 20) defines gray zone challenges as "competitive interactions among and within state and non-state actors that fall between" traditional, declared war and peace, and that "are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks." The definition seems to include cyber operations, but because it describes challenges, not a strategic space, a straightforward comparison with agreed competition is inappropriate. The definition could, however, suggest a description of a *multidomain gray zone strategic space*. To explore a structurally based apples-to-apples comparison, we examine how that space would be characterized.

One difference is that a gray zone strategic space would be bounded by peace at one end and traditional, declared war at the other. The tacit structural upper bound characterizing the agreed competition in cyberspace is exclusive of and below operations that generate effects equivalent to those of an armed attack. A typical gray zone operation cited by the literature is the invasion and occupation of the Dominican Republic in 1965–1966. The operation involved more than 40,000 U.S. troops, significant armed attacks, and tragic loss of life. These actions fall within the defined range of actions in the gray zone strategic space, but not the agreed competition framework for cyber strategic competitive space short of armed conflict.

Another difference is that segmentation, not constant contact, is the core structural feature of a multidomain gray zone strategic space. The gray zone literature notes that nation-states made deliberate choices during the Cold War to engage in gray zone activities. At that time, U.S. responses were governed by the rules of state-to-state relations—the same principles of sovereignty that structure the land, maritime, air, and space domains today. This suggests a condition of episodic contact, a strategic approach of escalation, and a strategic dynamic of an escalation ladder.

The literature also notes that nations today are interconnected in unprecedented ways and the velocity of technological change portends an expansion of gray zone challenges. We believe that cyber operations could represent that expansion. The important consequence is that the interconnectedness that is central to technological change has brought forth an entirely novel cyber strategic competitive space short of armed conflict—agreed competition—the features of which lead to equally novel operational prescriptions and strategic concerns.

Agreed Competition and the Return of Great Power Competition

The main focus of current U.S. national security strategy is countering the strategic struggle between great powers in the political, economic, and military arenas (White House 2017, 27; Department of Defense 2018, 1–2). The agreed competition framework has important implications for this anticipated return of great power competition.

If the comprehensive great power competition were viewed structurally as a comprehensive *strategic competitive space* (as we did with the gray zone), it would share the following characteristics of cyberspace's agreed competition: tacit agreement on structural bounds and a rationale to seek strategic advantage short of armed conflict. However, it would not share the structural disincentive to escalate because it would not share the core structural feature of interconnectedness from which the disincentive ultimately derives. Moreover, a comprehensive great power competitive space would comprise all military domains, multiple sectors, and every instrument of national power, making it far more expansive than the competitive space characterized as agreed competition. Agreed competition should be understood as a component of the great power competitive space with its own distinct structural features, incentives, and dynamic.

Conclusion

Agreed competition is a unique, structurally derived and defined phenomenon of cyberspace that allows for a better understanding of the cyber strategic competitive space short of armed conflict. It helps explain the observed behavior of actors competing in the space and has implications for the strategies they are likely to employ. This framework is unique to the cyber domain because other operating domains do not share cyberspace's core structural feature of interconnectedness. Agreed competition does not characterize gray zone challenges, nor is it applicable to any reasonable description of multidomain gray zone competitive space. Further, it has only limited application to a comprehensive strategic global competitive space.

Managing cyber operations short of armed conflict should advance national interests while enhancing cybersecurity and global stability. To do that, we must understand the strategic environment in which the operations are being conducted. The concept of agreed competition allows for robust academic and policy analysis that can support the evolution of this increasingly critical international security domain into a stable arena of global politics.

References

Department of Defense. 2018. *Summary of the 2018 National Defense Strategy of the United States of America*. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Fischerkeller, M. P., and R. J. Harknett. 2017. Deterrence Is Not a Credible Strategy. *Orbis* 61, no. 3: 381–393. https://doi.org/10.1016/j.orbis.2017.05.003.

Kahn, H. 1965. *On Escalation: Metaphors and Scenarios*. New York, New York: Frederick A. Praeger.

Kapusta, P. 2015. "The Grey Zone." *Special Warfare* 28, no. 4: 18–25. https://www.soc.mil/SWCS/SWmag/archive/SW2804/October 2015 Special Warfare.pdf.

White House. 2017. *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

About the Authors

Michael Fischerkeller is a member of the research staff in the Information Technology and Systems Division in IDA's Systems and Analyses Center. He holds a PhD in international security from The Ohio State University.

Richard Harknett leads the Department of Political Science at the University of Cincinnati, co-directs the Ohio Cyber Range Institute, and chairs the Center for Cyber Strategy and Policy. He earned a PhD in political science from Johns Hopkins University.

Michael and Richard are frequent collaborators who previously won the 2018 Welch Award for their article "Deterrence Is Not a Credible Strategy for Cyberspace," published in *Orbis* in 2017.