Supremacy by Accelerated Warfare through the Comprehension Barrier and Beyond: Reaching the Zero Domain and Cyberspace Singularity

Dr. Jan Kallberg

"In The Land Of The Blind, The One-Eyed Man Is King."
Erasmus Of Rotterdam, 16TH Century

INTRODUCTION

It is questionable and even unlikely that cyber supremacy could be reached by overwhelming capabilities manifested by stacking more technical capacity and adding attack vectors. The alternative is to use time as the vehicle to supremacy by accelerating the engagements' velocity beyond the enemy's ability to target and precisely execute and comprehend the events as they unfold. The space created beyond the adversary's comprehension is called the Zero Domain. Military strategists traditionally see the battle space as land, sea, air, space, and cyber domains. When fighting a battle beyond the adversary's comprehension, the conflict occurs in the Zero Domain, not in a traditional warfighting domain.

In the Zero Domain, cyberspace superiority surfaces as the outcome of the accelerated time and a digital space-separated singularity that benefit the more-rapid actor. The Zero Domain has a time-space and digital landscape that are accessible only by rapid actors, and a digital landscape that is not accessible by slower actors due to the execution velocity in enhanced accelerated warfare. Velocity achieves cyber Anti-Access/Area Denial (A2/AD), which can be achieved without active initial interchanges by accelerating the execution and cyber ability in a solitaire state. During this process, any adversarial probing engagements only affect the actor on the approach to the Comprehension Barrier; once arrived in the Zero Domain, a complete state of A2/AD is present.

Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Before joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His website is www.cyberdefense.com.

From that point forward, the actor that reached the Zero Domain has cyberspace singularity and is the only actor who can understand the digital landscape, engage unilaterally without an adversarial ability to counterattack or interfere, and hold the ability to decide when, how, and where to attack. In the Zero Domain, the accelerated singularity controls the battlefield by denying adversarial cyber operations and enacting destruction, extraction, corruption, and exploitation of targeted adversarial digital assets.

Breaking through the comprehension barrier

There is a point along the trajectory of accelerated warfare where only one warfighting nation comprehends what is unfolding and appreciates the cyber terrain. This is the upper barrier for comprehension where the acceleration makes the cyber engagement unilateral. The Comprehension Barrier is dependent on one sides abilities, technical maturity, and institutional structure, and the enemies' weaknesses. Adversaries forged in organizational fear cultures and a strict command structure could, even if technically cognizant and competent, struggle to competitively accelerate the warfare against the more agile and less technically capable opponent. The engagements that accelerate toward the Comprehension Barrier have increased intensity, as they are faster, more forceful, and less restrained when the stress of acceleration degrades the OODA (Observe, Orient, Decide, and Act) loop.

Once the warfighter breaks through the Comprehension Barrier with maintained control, the conflict changes from a contested cyberspace battle to space singularity. The cyber ability in the Zero Domain battle is derived from a single source. At that point, any engagement can affect only the slower party and not the owner of the

singularity; this is due to the slower attacker's inability to understand the factual battle landscape and target, arrange its resources and conduct warfare at the velocity that occurs on the other side of the Comprehension Barrier. If we use real-life references, the warfighter beyond the Comprehension Barrier has full access to situational awareness, can see the landscape and target, and can act as if the war occurred under normal conditions, while the slower warfighter never reached the Comprehension Barrier is floating weightless in pure darkness. Accelerated warfare beyond the Comprehension Barrier robs the slower party of the ability to understand, sense, order, and coordinate operations. When breaking the Comprehension Barrier, the first of the adversary's final points of comprehension is human deliberation, directly followed by pre-authorization and machine learning, and then these final points of comprehension are passed, and the more-rapid actor enters the Zero Domain.

Time and the lost space

In accelerated cyberwar, time is to cyber what combined time and place were for Clausewitz[1] because the Zero Domain nullifies the importance of other warfighting domains and creates a parsimonious singularity through the absence of a common battlespace. Space matters only before the Comprehension Barrier is crossed. The traditional concentration of forces—*where* and *when*—is replaced with *then,* because the singularity occurs first in the Zero Domain. As noted strategist Edward N. Luttwak stated, strategies without the ability to execute are pointless exercises.[2] The accelerated warfare beyond the Comprehension Barrier eradicates the influence of the opponent's cyber strategy because singularity in the Zero Domain removes the opponent's ability to execute.

The evaporated OODA loop

From an operational standpoint, action beyond the Comprehension Barrier evaporates and nullifies the traditional command and control (C2) scheme. In general terms, military C2 follows the steps of the OODA loop developed by U.S. Air Force Colonel John Boyd in the 1960s (Fig. 1).[3] Accelerated warfare beyond the Comprehension Barrier nullifies the adversary's OODA loop because the rapid-actor leaves the adversary with nothing to accurately observe, no targets to orient toward, no information nor situational awareness with which to make a decision, and the ability to act is limited to spurious actions with no relation to the unfolding events. The unique tenets of cyber undermine the utility of the OODA loop.[4] The OODA loop requires the ability to assess ongoing events (as in the initial step of "observe"), but under conditions of anonymity, computational speed in cyber execution, and no object permanence, the observations feeding the loop are likely to be inaccurate, if not spurious, as acceleration starts. In accelerated warfare, the OODA loop disappears in the engagement for the slower party if the faster actor breaks the Comprehension Barrier. The rapid-actor maintains its OODA loop in the Zero Domain, and conversely, if the rapid-actor is no longer able to keep its position in the Zero Domain,

the OODA loop will reemerge for the slower actor as the formerly rapid-actor is unable to maintain velocity beyond the Comprehension Barrier.

The "orient" stage in the OODA loop—reacting to unfolding events and positioning for
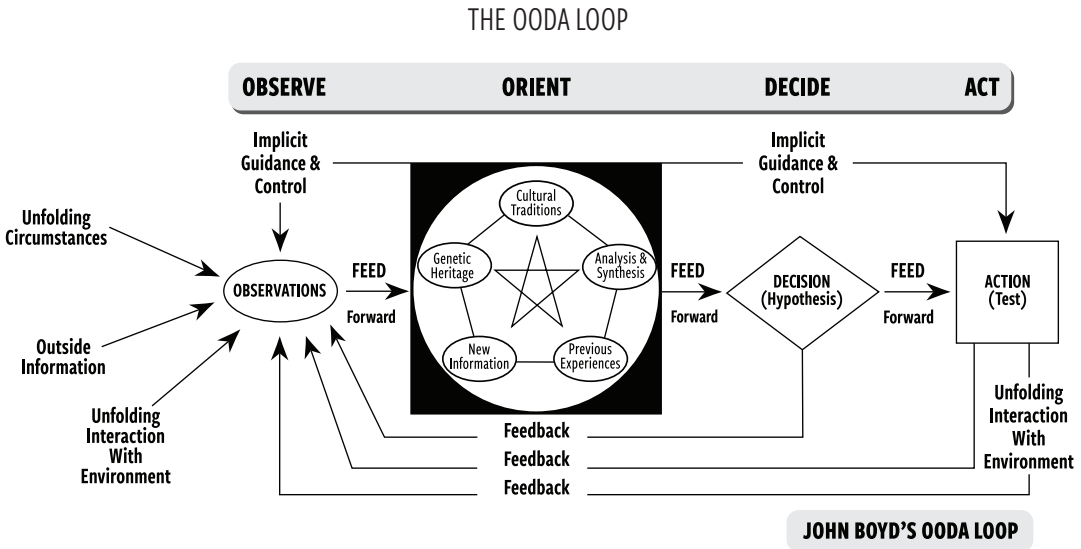
THE OODA LOOP

Figure 1. by Patrick Edwin Moran - own work. Licensed under CC BY 3.0 via Wikimedia Commons.

a better outcome—assumes a maneuverable space with favorable positions, but the lack of object permanence in cyber brings an ever-changing battlefield and permanent dis-orientation rather than re-orientation. When these nodes—ever-changing spaces lacking object permanence—are accelerated beyond the Comprehension Barrier, environmental information cannot be structurally understood or ordered outside of the Zero Domain. If the "observe" and "orient" stages are not relevant to the facts of the engagement, then the "decide" stage will fail to deliver the proper course of action and thus lead to an in-effective "act" stage. Computational speed exacerbates the inability to assess and act, and the increasingly shortened time frames likely to be found in future cyber conflicts will dis-allow any significant human deliberation. Enemy deliberation, either through leadership or pre-authorization, are ultimately ineffective once the Comprehension Barrier is passed.

The key to victory historically has been the concept of being able to get inside the opponent's OODA loop, and thereby distort, degrade, and derail the opponent's OODA assessments. [5] In accelerated warfare beyond the Comprehension Barrier, there is no need to be inside the opponent's OODA loop because the accelerated warfare concept removes the OODA loop for the opponent and thereby disabling the opponent's ability to coordinate, seek effect, and command.

The Zero Domain

The five traditional battlespace domains are contested spaces (land, sea, air, space, and cyber) where parties interact, engage, have interchanges through which they can structure their understanding of the battle environment to make decisions. When both parties are present in the engagement, and even if one is weaker and less able to challenge, there is a mutual perception of the framing of the fight. The Zero Domain is the battle space beyond the Comprehension Barrier where battle space singularity occurs, and only one actor has access to the OODA loop. The Zero Domain is the warfighting space where accelerated velocity in the warfighting operations removes the enemy's presence. It is the domain with zero opponents. It is not an area denial, because the enemy is unable to accelerate to the level where it could enter the battle space, and it is not access denial because the enemy is not part of the fight once the Comprehension Barrier is broken. Instead, it is a state of cyber A2/AD, but there is no challenge to this state in the Zero Domain because it is an outfall of the establishment of the Zero Domain.

SHORT CONCLUSION

As a research note, these ideas and concepts are under development and are not the final output. The purpose of the note is to introduce new concepts, open up the discussion, and catalyze comments.🛡

NOTES

1. C. von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

2. E. Luttwak, *The Grand Strategy of the Roman Empire: From the First Century CE to the Third.* Baltimore, MD: Johns Hopkins University Press, 2016.

3. F. P. B. Osinga, *Science, strategy and war: The strategic theory of John Boyd.* New York, NY: Routledge, 2007.

4. J. Kallberg and T. S. Cook, "The unfitness of traditional military thinking in cyber: Four cyber tenets that undermine traditional strategies," *IEEE Access,* vol. 5, pp. 8126-8130, April 2017. [Online]. Available: ResearchGate, https://www.researchgate.net/publication/317328999_Unfitnesstraditionalthinking, accessed August 12, 2018.

5. J. R. Boyd, "The essence of winning and losing," unpublished.