Innovation and the Proper Context of Cyber Operations

The path to avoid cyber war

by Brandon Valeriano & Benjamin Jensen

>Dr. Valeriano serves as a member of the Bren Chair of Military Innovation, Krulak Center, Marine Corps University.

>>Mr. Jensen serves as a Professor, School of Advanced Warfighting, Marine Corps University.

Misunderstanding Innovation and the Future Battlefield

Most stories of innovation and invention for the military are filled with messianic projections about the evolving future of warfare. The slap of reality destroys these projections with the dirigible and drone as twin examples of the failure of new innovations to alter how coercion occurs on the battlefield. Instead these options are/were better served for reconnaissance and espionage than war. The dreams of the future provided few hints for what was to come.

The idea of a coming Cyber Pearl Harbor is more than just a warning, it has become trope built on an intellectual fallacy.[1] The Cyberspace Solarium Commission (which we served on) understood that many of its critical recommendations on cyber security reform would only be implemented after a cyber disaster, a break glass in case of emergency scenario that would change everything.[2]

The grand cyber wars everyone fears never materialize because the military, strategic, and policy community fail to understand the utility of cyber weapons. In this article, we will examine the utility of cyber operations in the context of crisis bargaining and warfare outlining the limited coercive potential of cyber weapons. Instead, cyber operations can provide pathways to de-escalate conflicts minimizing the possibility of war.

Why have we not experienced the "Cyber Armageddon" envisioned and predicted since the early 1980s? *(Photo by SSgt Jacob Osborne.)*

Cyber Doom

The United States acquired cyber technology quite some time ago. Reaching popular consciousness with the 1982 movie *Wargames*, Ronald Regan began outlining the origins of a cyber strategy.[3] The dangers of cyber catastrophe were illustrated quite vividly with the fear associated with Y2K at the turn of the millennium.[4] Fast forward through the War on Terror, and we are back where we began, waiting for Cyber Armageddon to unleash doom on the international system.

Why have we failed to witness cyber doom?[5] Rather than being used as a tool to disseminate the opposition, cyber capabilities instead do more mundane things like leveraging left of launch operations in the hopes of disrupting the

math of our adversaries.[6] Some have begun to argue that cyber operations just represent an intelligence contest or operate mainly in the domain of espionage.[7]

The reality of cyber operations is much different than the prognosticators of the new might lead one to believe. The mythical cyber war everyone fears will never come to fruition because analysts have continually misunderstood the nature of innovation and fail to apply critical analysis required to evaluate perceived offset technologies. Cyber operations act as substitutes or complements for other options in the foreign policy toolkit.[8] When substituted for military operations, cyber options can provide pathways to peace and enable de-escalation of an emerging crisis.

The Failure of the Offense in Cyber Security

The real world comes for us all at some point, and it must come for the strategic community as it confronts the reality and purpose of cyber operations.[9] We are not "under siege" on all sides in cyber security.[10] Cyber operations instead flow with the course of international politics, ebbing and rising with the strategic currents of the international system.[11] Discard an agreement with an adversary and that same adversary will respond with increased cyber actions. End negotiations on trade and the target responds by increasing their attacks globally to demonstrate strategic will and credibility. It is not complicated.

Cyber operations are not tools of coercion or power projection, rather cyber operations are forms of deception and espionage that seek to attack information, command and control, and manipulate perceptions.[12] To understand the nature of cyber conflict, we have to understand the purpose of cyber operations. If cyber options are useless in changing the behavior of an adversary, then they are not especially useful as tools of coercion central to the conduct of warfare.

Too often we conceive of strategy as a means to an end without considering how that end is achieved. If cyber operations are the means, what are the ends? What is the goal exactly? It is not clear what the goal is with the vision of persistent engagement; there is no end state identified by the strategy.[13] This is likely because cyber operations have a limited ability to impact the outcome of battles. Cyber options can change things around the edges, help shape a battle, deceive decision makers, but rarely will these sort of modern forms of political warfare be decisive for victory.

Cyber operations fail to trigger escalation dynamics, and instead offer a pathway away from war during crisis interactions.[14] Escalation is simply an increase of intensity or the tempo of a conflict suggesting rising hostility over time.[15] Generally, cyber operations do not even provoke responses, let alone escalatory responses in or out of domain limiting the potential for escalation.[16]

Overall, there is a limited utility of offensive cyber operations in the cyber domain.[17] Cyber options failed to make much of a dent on the operations of terrorists because actors like ISIS do not depend on digital methods of communication or power projection.[18] A nibble and low-tech adversary is not a suitable test case for cyber operations.

What has been cited as the great testing ground for cyber operations in modern warfare, the ongoing conflict between Ukraine and Russia has rather resulted in stalemate.[19] Instead, Russia attacks power plants for a few hours or devastates the tax software of Ukraine causing global confusion but not advancing an inch on the battlefield.[20] There is no great strategic advance enabled by cyber operations in an active combat zone.[21]

Cyber for the Defense

The real innovation in cyber strategy will come when the community moves away from grand projections of cyber offensive operations and focuses more on the ability of cyber options to enable defensive bulwarks and to manipulate information asymmetries between disputing powers.[22] By making it near impossible to attack, the aggressor is forced to resort to other traditional options to destabilize the target.[23]

Enabling defense by denial is but one of the few strategic advances on offer from cyber tools. Rather than expanding attack surfaces, cyber options instead can make it more likely that an attack will never happen in the first place if the target is hardened. Chris Krebs, former head of the Cyberspace and Infrastructure Security Agency, noted that the core strategy of protecting the United States during the election of 2020 was not hunt forward operations but deterrence by denial.[24]

Too often we conceive of strategy as a means to an end without considering how that end is achieved. If cyber operations are the means, what are the ends?

Even in discussing recent USCYBERCOM hunt forward operations in Estonia during the 2020 election, the main point seems to be to discover and splash out Russian malware tools into the public domain to prevent these options from being used on the attack.[25] Signaling knowledge of the opposition actors capability sometimes is enough to prevent further violation. Cyber operations paradoxically provide for methods of de-escalation in an ongoing conflict.

Cyber Operations as Off-Ramps from War

Cyber operations are not prone to escalation, in fact, cyber operations are likely off-ramps from the road to war.[26] The role of cyber operations during a crises or conflict event is either as a substitute for more traditional options that might be escalatory, such strategic bombing, or as a complement to ongoing operations, like ammunition or fuel. Cyber options either add or subtract,

they do not multiply or divide, a perspective that has enormous ramifications for cyber strategy moving forward.

Cyber operations expand the range of strategic options, moving beyond the typical construction of DiME: diplomatic, information, military, and economic. The manipulation of digital signals makes the information component of strategy more meaningful through added options, but it does not fundamentally revolutionize the nature or character of war. The effects tend to be fleeting or limited due to the ambiguous nature of covert operations, which include cyber and information operations.[27] As weak signals that can be denied, cyber operations preserve flexibility in a crisis situation demonstrating resolve in the face of opposition.

When challenged by a provocative move the by the opposition, the defender has many options to respond. If the desire is escalation to maintain dominance against the opposition, a military option is obviously the choice. But this assumes a desire for war that few would ascribe to, given the complexities and dangers of modern battle. If the choice is to respond and demonstrate capability in the face of opposition so the adversary backs down, diplomatic, or economic options are limited and demonstrate a weak commitment. Military options are too escalatory, but information options are just right in the Goldilocks sense. By signaling to the opposition commitment and limiting their ability to respond with further military measures, a limited amount of force can be applied to shape the conflict away from escalation.

We discovered this unexpected pattern during a series wargame experiments while doing research for our next book. With a sample of 400 individual wargame decisions bolstered by an experimental treatment of 3,000 international respondents to an experimental survey battery, we have been able to demonstrate the stabilizing influence of cyber operations.[28] We knew that cyber operations were unlikely to be escalatory based on past research but were unsure just how this process occurred.[29]

In a scenario where there was a high likelihood of escalation (long-term rivalry over territorial claims), respondents who leveraged cyber options intended to respond proportionally and manage escalation because they did not see the initial violations as worthy of escalation towards war.[30] Respondents tended to use information warfare options, including cyber options, more often than military options to respond to an initial cyber operation because the violation was not series enough to necessitate a conventional response.

A simple demonstration of our theory comes from an examination of the U.S.-Iranian Summer Crisis of 2019. A long simmering rivalry in the region seemed to escalate after the United States pulled out of the Joint Comprehensive Plan of Action in 2018. Concern about Iran's use of proxy forces in the region, particularly Yemen, and fears of a nuclear weapons program animated the animosity directed at Iran. Attacks on shipping in the region lead to the deployment thousands of troops the region including an aircraft carrier.

Cyberspace is likely not a domain of coercion and warfare.

On 20 June 2019, Iran shot down a U.S. R1-4 Global Hawk UAV.[31] President Trump first ordered a military strike that was called off due to either the threat of collateral damage or the fear of escalation to war, or both.[32] Instead of escalating, the United States responded proportionately by using cyber tools to disable Iran's ability to track ships in the region.[33] Another operation hacked Iran's missile defense systems making it vulnerable to an attack.[34]

The cyber operations signaled risk to the Iranians and preserve further options for the United States if the situation escalated. Instead, the conflict de-escalated over the summer until on 27 December 2019 when a rocket attack on a U.S. base in Iraq killed a contractor.[35] On 3 January, Gen Solemani was assassinated, which then led to Iran launching a conventional missile strike on U.S. facilities—injuring many. While there was limited escalation in the Winter of 2019, the Summer crises of 2019 was distinctly different and separated by over six months, suggesting the Winter crisis was an entirely new phase of the conflict.

During the summer crisis, cyber options substituted for military options allowing both sides for space to maneuver away from outright war. When challenged with a continuing series of provocations in the region, the United States responded with cyber actions that limited the conflict and served as pathways toward de-escalation.

Evidence seems clear that cyber actions can dampen a crisis, helping states locked in competition avoid dangerous conflict spirals. Others are discovering similar patterns, noting that there is a decreased demand for retaliation in response to a cyber operation.[36] Mutual vulnerability can promote mutual stability over time as operations in the gray zone can convey information and signal intent to the opposition, lessening the fog of war. Cyber options can create new risk profiles, but they can also mitigate risk by demonstrating resolve pushing the other side to either de-escalate or respond with proportional moves that do not escalate the competition.

The Impact on the Marine Corps and USCYBERCOM

What exactly all this means for the Marine Corps and the DOD is an open question. Cyberspace is likely not a domain of coercion and warfare. Instead the domain is developing up much differently than the futures community thought. It is likely that the competition space will be dictated more by the dynamics of political warfare than outright warfare, moving around the edges of conflict manipulating information asymmetries.[37]

Marine capabilities in cyberspace need to be enhanced and developed through MARFORCYBER, but we also need to shift position. Instead of a domain that "is under siege," we must recognize that ongoing fires contain communications and information about adversary intentions. Understood as such, cyber becomes a domain of information management helping signal

expectations and shaping the future of the battlefield.

Properly understood as an adjunct capability that can substitute for more escalatory options, cyber operations have a clear role to play in modern conflict. Maintaining and enhancing capability is critical because falling behind to a more advanced technological adversary promotes weakness and overreaction to unknown threats. Losing a digital edge can lead to a state acting like a cornered animal with few strategic options.

The force needs to enhance its cyber capabilities to remain relevant and complement convention operations. More importantly, a modern military force needs to maintain cyber capabilities to deny digital attack paths to the adversary. The disasters envisioned through the loss of command and control due to digital intervention will be a consequence of inadequate defense, not the ingenuity of the attacker. Cyber operations provide a method of defensive control over lines of communication and method of modern reconnaissance that can be used to understand adversary intentions.

Technology and Innovation

There is a difference between a technology being innovative for society and a technology becoming a transformative for military conflict. Digital communication and the internet surely are transforming society, reshaping how we connect, work, and view the world. Yet, just how important has cyber technologies been for transforming war? There is little evidence much has changed at all so far, 30–40 years into the use of the technology. Even if we consider cyber immature and start our new era in 2001 or 2010, there is little evidence in a change in the methods of coercion enabled through cyber pathways.

The joy in innovation often comes through the unexpected developments. We all can envision a fantasy world where cyber technologies reshape conflict, this is typical in our popular fiction from *Battlestar Galactica* (2004) to even the *Fast and the Furious* (2001–) series. But actualizing these transformations on the battlefield is difficult when the innovation of cyber technologies is broken down to its bare bones.

We must ask how the means can achieve an end, answering this question through the framework of cyber operations leads to intellectual dead-ends. Properly understood, the innovation of cyber operations is to limit and forestall escalation leading to stability. Not at all what we expected when we started this research and likely not the final word on the subject.

Notes

1. Sean Lawson and Michael Middleton, "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016," *First Monday,* (March 2019), available at https://firstmonday.org.

2. U.S. Cyberspace Solarium Commission, available at https://www.solarium.gov.

3. Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York, NY: Simon and Schuster, 2016).

4. Murray E. Jennex, "Emergency Response Systems: The Utility Y2K Experience," *Journal of Information Technology Theory and Application (JITTA)*, (Atlanta, GA: Association for Information Systems, 2004).

5. Sean T. Lawson, *Cybersecurity Discourse in the United States: Cyber-doom Rhetoric and Beyond*, (New York, NY, Routledge/Taylor & Francis Group: 2020).

6. Brandon Valeriano, Heather Roff, and Sean Lawson, "Dropping the Cyber Bomb? Spectacular Claims and Unremarkable Effects," *Council on Foreign Relations,* (New York, NY: Council on Foreign Relations, 2016).

7. Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*, (New York, NY: Oxford University Press, 2018); and J. Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, (2019), available at https://warontherocks.com.

8. Brandon Valeriano and Benjamin Jensen, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War," in *Cyber Peace*, (Cambridge: Cambridge University Press, 2021).

9. Brandon Valeriano and Ryan Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (Oxford: Oxford University Press, 2015).

10. Gordon Lubold and Dustin Volz, "Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts," *The Wall Street Journal*, (March 2019), available at https://www.wsj.com.

11. *Cyber War versus Cyber Realities.*

12. Erik Gartzke and Jon Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, (Milton Park: Taylor & Francis, 2015); and *Cyber Strategy*.

13. U.S Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command," (2018), available at https://www.cybercom.mil.

14. "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War."

15. Herman Kahn, *On Escalation: Metaphors and Scenarios*, (New York, NY: Routledge, 2017).

16. Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Cyber Restraint," *Cato Institute Policy Analysis*, (Washington, DC: CATO Institute, 2019).

17. Ibid.

18. Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," *Belfer Center for Science and International Affairs,* (October 2017), available at https://www.belfercenter.org.

19. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, (June 2016), available at https://www.wired.com.

20. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, (3 March 2016), available at https://www.wired.com; and Andy Greenburg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, (August 2018), available at https://www.wired.com.

21. Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution,* (Washington, DC: SAGE Publications, 2019).

22. "The Myth of the Cyber Offense: The Case for Cyber Restraint."

23. Robert Morgus, et al., "Deterrence by Denial: The Missing Element of U.S. Cyber Strategy," *Lawfare*, (March 2020), available at https://www.lawfareblog.com.

24. David E. Sanger and Julian E. Barnes, "U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came," *The New York Times*, (November 2020), available at https://www.nytimes.com.

25. Julian E. Barnes, "U.S. Cyberforce Was Deployed to Estonia to Hunt for Russian Hackers," *The New York Times*, (December 2020), available at https://www.nytimes.com.

26. Much of this research originally will appear in Brandon Valeriano and Benjamin Jensen, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War," in *Cyber Peace*, (Cambridge: Cambridge University Press, 2021).

27. Cyber Strategy; Austin Carson and Karen Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret," *Security Studies* 26, no. 1, (2017); and A. Carson, *Secret Wars: Covert Conflict in International Politics*, (Princeton, NJ: Princeton University Press, 2020).

28. Benjamin Jensen and Brandon Valeriano, "What Do We Know About Cyber Escalation? Observations from Simulations and Surveys," *Atlantic Council*, (22 November 2019), available at https://www.atlanticcouncil.org; and Benjamin Jensen and Brandon Valeriano, "Cyber Escalation Dynamics: Results from War Game Experiments International Studies Association, Annual Meeting Panel: War Gaming and Simulations in International Conflict March 27, 2019," *ISA,* (2019), available at http://web.isanet.org.

29. *Cyber Strategy.*

30. "What Do We Know About Cyber Escalation? Observations from Simulations and Surveys."

31. Lily Newman, "The Drone Iran Shot Down Was a $220M Surveilance Monster," *Wired*, (June 2019), available at https://www.wired.com.

32. Toluse Olorunnipa, et al., "'I Stopped It': Inside Trump's Last-minute Reversal on Stirking Iran," *Washington Post*, (June 2019), available at https://www.washingtonpost.com.

33. Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *The New York Times*, (August 2019), available at https://www.nytimes.com.

34. Ellen Nakashima, "Trump Approved Cyber-strikes Against Iran's Missile Systems," *The Washington Post*, (June 2019), available at https://www.washingtonpost.com.

35. Julian E. Barnes, "American Contractor Killed in Rocket Attack in Iraq," *The New York Times*, (December 2019), available at https://www.nytimes.com.

36. Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics," *Journal of Cybersecurity*, (Oxford, Oxford University Press, 2019).

37. Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown J. World Aff., (n.d.)*, available at http://bjwa.brown.edu.