AIR & SPACE POWER JOURNAL - COMMENTARY

Is It Time to Forget about Cyber Deterrence?

Maj Cameron Ross, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

On 7 August 1945, one of the nation's foremost naval strategists drove to the local drugstore with his wife to pick up a copy of the *New York Times*. When he opened the paper, he was taken aback by the headline "First Atomic Bomb Dropped on Japan." After quickly scanning a few paragraphs, he turned to his wife and bluntly said, "Everything I have written is obsolete."[1]

Bernard Brodie immediately grasped that the atomic bomb necessitated a fundamental change to military strategy. For most of human history before 1945, military conflict and security planning focused on the back and forth of offensive and defensive capabilities. While war was to be avoided if practicable, it was universally recognized that it was *possible,* and thus, nations needed to prepare to fight. Accordingly, the military forces' primary organizing principle was war fighting—offensive operations to inflict cost and defensive actions to blunt damage.[2] In the offense-defense framework, the state's security rested on its ability to understand the balance of its war-fighting capabilities in relation to its rivals and choose the approach that would achieve the best outcomes.

The arrival of nuclear weapons dramatically altered the balance between offense and defense and created the ultimate offense-dominant environment.[3] In a nuclear war, the defense would always lose, and the cost of the war would be catastrophic for mankind. The horrifically destructive and undisputable nature of the weapon demanded an entirely new strategic framework to manage the atomic age. Brodie's 1946 classic, *The Absolute Weapon: Atomic Power and World Order,* advanced the concept of nuclear deterrence, which would serve as the foundation of US security throughout the Cold War and into the twenty-first century. Deterrence itself was not a new idea—traditional statehood included elements of conventional deterrence to achieve national objectives or avoid war. For example, forces could be deployed to borders to signal resolve and dissuade an adversary from attacking. However, Brodie recognized that nuclear weapons represented incontestable threats of unacceptable cost, so strategists had to completely change how they approached deterrence and military affairs. As he famously stated, "Thus far, the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."[4]

As a result, the dominant organizing agenda for military forces became deterrence and the avoidance of war. Theorists introduced a radical concept that a nation's security would no longer rest in its offensive and defensive abilities but rather in its opponent's mind. Further, the purpose of possessing military weapons (in this case, nuclear weapons) was to never use them.[5] The massive cost of these incontestable weapons became the source of deterrence stability and maintenance of peace between nuclear powers. Ever since, deterrence has served as the primary strategic framework for America's national security.

Consequently, ideas about cyber deterrence have naturally accompanied the growth of cyberspace and cyber operations. The disruptive and revolutionary nature of cyber and its potential for massive effect resembled the arrival of nuclear weapons in many ways. However, many theorists and strategists quickly noted the challenges to reconciling cyber with ideas of classical deterrence. During the Cold War, deterrence was straightforward. For example, it was easy to know who launched an attack; there was a significant scientific barrier to creating nuclear weapons; every bomb could be as powerful as the first; any use of a nuclear weapon crossed an acknowledged threshold; redlines were usually grounded in geography and easy to conceptualize; and motives were generally discernable and tied to strategic interests.[6] Almost none of these apply to the world of cyber. Attribution can be incredibly difficult and usually takes an inordinate amount of time—if one can discern the origins of the attack at all. The low barrier to entry enables many actors, and what would deter each actor is almost as varied as the actors themselves. The use of a cyber weapon makes it less likely that it will be effective in the future as defenders patch the vulnerability. Defining substantive thresholds and redlines is almost impossible. Yet, despite all the barriers to effective deterrence, most authors believe it is possible and should be pursued. But is deterrence the right framework for approaching cyberspace? Perhaps the friction strategists face is indicative of the need for a paradigm shift.[7]

A handful of thinkers have begun to argue just that. They maintain that anchoring America's cybersecurity capabilities around a primary strategic objective of war avoidance is not achievable in any sustained manner.[8] In addition to the challenges already noted, their analysis of the nature of cyber operations points to a framework more akin to offense-defense than deterrence. Just as conventional deterrence is less stable than nuclear deterrence because of the contestability of conventional weapons, the highly contestable nature of cyberspace makes cyber deterrence even less stable.[9] Further, by definition, cyberspace is interconnected, which means that action is never absent and that national security actors are in constant contact with adversaries as well as numerous nongovernmental entities.[10] Finally, every new version of software, hardware, and integration configuration presents new opportunities for offense and new challenges for defense. The lack of any steady-state in cyber "terrain" means there is no steady state of defense. Instead, "defense is a dynamic construct relative to the offensive opportunities that emerge with each 2.0 or 3.0 of the terrain."[11] The combination of contestability, interconnectedness, constant action, and ever-changing terrain creates an entirely new strategic environment: one of offensive-persistence.[12]

As opposed to the environment of nuclear weapons, where the presumption is that the defense will lose, an offensive-persistent environment presumes that the defense can lose, but it is not structurally inevitable. Defense is possible in any specific moment within the dynamic terrain of cyberspace and can be sustained over periods of time through active adjustments to the environment. However, defense can never be decisive. "The defense can achieve tactical and operational success, but the offense will persist, the contact with the enemy will remain constant, and the defense will need to adjust as the terrain to defend and the vectors to attack evolve."[13] Just as the unique strategic environment of nuclear conflict necessitated a change in strategy to address it, cyberspace policy and operations must address the distinctive nature of cyberspace. As Richard Harknett explains, "Strategic frameworks must map to the realities of strategic environments; the reverse is not possible."[14]

The framework Harknett and Michael Firsherkeller propose for the offense-persistent environment of cyberspace is cyber persistence. They maintain that the current approach of cyber deterrence, and its associated operational restraint until norms can be established, has created a strategic deficit as others operate without similar concerns and gain advantage. By adopting an approach of cyber persistence, the US would seek to "use cyber operations, activities, and actions (as opposed to the threat of force) to generate through persistent operational contact (as opposed to avoiding contact) continuous tactical, operational, and strategic advantage in cyberspace so that the United States could ultimately deliver direct effects in, through, and from cyberspace at a time and place of its choosing."[15] Cyber persistence focuses on gaining and retaining initiative and includes active engagement with an active operational domain.[16] Instead of a threat-based strategy, which focuses on who might threaten the US, they suggest a capabilities-based strategy that anticipates our vulnerabilities while simultaneously leveraging the vulnerabilities of others. This framework echoes the ebb and flow of offense-defense as opposed to the lack of offensive activity in deterrence. Of course, the activities involved with cyber persistence may cause an opponent to pause in their consideration of the next steps—in essence, creating a deterrence residual. But it would not "change the attacker's decision calculus from one seeking to achieve objectives through aggression to one that seeks the same objectives while avoiding war (the difference between an offense-defense strategic environment and a deterrence dominated strategic environment)."[17]

There is much more work to be done in exploring these ideas. Characterizing the strategic environment as offense-persistent deserves further assessment. The same is true for the applicability of previous research on offense-defense theory to cyberspace operations. Moreover, if cyberspace requires a nondeterrence framework, there must be additional thought applied to how the US would integrate multiple strategic frameworks, as deterrence is still necessary for nuclear warfare and its associated conventional warfare. This requirement is particularly important since the traditional domains of air, land, and sea rely on and regularly interact with cyberspace. However, this framework suggests the time has come for cyber strategy and thought to receive fresh consideration outside the confines of a deterrence approach. The success of deterrence theory with one new technology has led many to try and apply it to another, but we seem to have reached the point where it is inhibiting progress in cyberspace rather than advancing it. Rather than attempting to make deterrence work within cyberspace, perhaps now is the time to devote more effort to understanding the nature of the environment and then work to develop a framework that matches it. As Harknett said, let us use these friction points not to "resuscitate and stretch deterrence thinking, but to logically and creatively move beyond it."[18] ✪

Maj Cameron Ross, USAF

Major Ross (BS, USAFA; MA, Biola University) is a deputy division chief within the 566th Intelligence Squadron at Buckley AFB, Colorado. He is an intelligence officer with extensive expertise in signals and cyber intelligence and a graduate of the Junior Officer Cryptologic Career Program.

Notes

[1] Details of the event are from Fred Kaplan, *The Wizards of Armageddon* (Palo Alto, CA: Stanford University Press, 1991), 9–10. However, I was introduced to the material through Richard Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2 (Spring 2016), 81, https://www.jinfowar.com/.

[2] Richard Harknett, John Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management* 7, no. 1 (January 2010), https://www.researchgate.net/.

[3] Harknett and Goldman, "The Search for Cyber Fundamentals," 86.

4. Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt and Brace, 1946), 76.

5. Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," *Fifth Domain, 19* July 2017, https://www.fifthdomain.com/.

6. These challenges are documented in almost every discussion about the difficulties of cyber deterrence. However, the following provide great summaries: Martin C. Libiki, *Cyberdeterrence and Cyberwar (Santa Monica, CA: Rand Corporation, 2009)*; Dorothy Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly* 77, no. 2 (April–June 2015); and Joseph Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016–17), https://www.mitpressjournals.org/.

7. Richard Harknett, "Correspondence: Is Deterrence Possible in Cyberspace?," *International Security* 42, no. 2 (Fall 2017), 196, https://www.belfercenter.org.

8. Harknett, Callaghan, and Kauffman, "Leaving Deterrence Behind," 15.

9. Williams, "Meet the Scholar Challenging the Cyber Deterrence."

10. Harknett, "Correspondence: Is Deterrence Possible," 198.

11. Harknett and Goldman, "The Search for Cyber Fundamentals," 85.

12. Harknett, "Correspondence: Is Deterrence Possible," 198.

13. Harknett and Goldman, "The Search for Cyber Fundamentals," 86.

14. Michael Firsherkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (Summer 2017), 386, https://www.fpri.org/.

15. Firsherkeller and Harknett, "Deterrence is Not a Credible Strategy," 389.

16. Williams, "Meet the Scholar Challenging the Cyber Deterrence."

17. Harknett, Callaghan, and Kauffman, "Leaving Deterrence Behind," 15.

18. Harknett, "Correspondence: Is Deterrence Possible," 198.