U.S. Marines practice "combat gliding" during Integrated Training Exercise 2-15 at Camp Wilson on Twentynine Palms, California, January 2015 (U.S. Marine Corps/Kathryn Howard)

Crafting and Managing Effects

The Evolution of the Profession of Arms

By James G. Stavridis, Ervin J. Rokke, and Terry C. Pierce

Recent operations conducted against U.S. businesses and citizens have reemphasized a critical vulnerability in how the U.S. Government thinks about and defends itself against nonkinetic instruments of power. This is particularly true in the manmade domain of cyber. In December 2014, a high-profile breach of Sony Pictures Entertainment was linked to a state-sponsored cyber attack by North Korea. Apparently, North Korea was motivated by opposition to the film *The Interview*, a comedy about the assassination of North Korea's leader Kim Jong-un.[1] The Obama administration responded to Pyongyang's alleged cyber attacks on Sony by imposing sanctions against the country's lucrative arms industry.[2] It is too soon to tell whether this response was appropriate and effective. However, the apparent difficulties we faced in determining how best to respond indicate that the assumptions underlying the definitions and responsibilities of our military profession, most of which emerged following World War II and the beginning of the Cold War, are badly in need of updating to accommodate new forms of warfare.

Admiral James G. Stavridis, USN (Ret.), Ph.D., is Dean of the Fletcher School of Law and Diplomacy at Tufts University. Lieutenant General Ervin J. Rokke, USAF (Ret.), Ph.D., is the Senior Scholar in the Center for Character and Leadership Development at the U.S. Air Force Academy. Captain Terry C. Pierce, USN (Ret.), Ph.D., is Director of the Department of Homeland Security Center of Innovation at the U.S. Air Force Academy.

The end of World War II and emergence of the Cold War resulted in a surge of brilliant academic scholarship concerning the profession of arms. In 1957, for example, Harvard political science professor Samuel Huntington published his seminal book, *The Soldier and the State*. This was a monumental effort explaining why and how the modern military officer corps represents a profession in the same sense as those of law, clergy, and medicine.[3] Two key themes emerged from Huntington's work. First, the optimal means for civilian control of the military was to professionalize it. Second, Huntington argued that the central skill of military competence, unique to its profession, was best summed up by Harold Lasswell's phrase, "the management of violence."[4] In short, for Huntington as well as other nationally recognized scholars of his time, the unique professional expertise of military officers was focused on the achievement of successful armed combat.[5]

We believe the first part of Huntington's theory still holds. In a democratic society, the military is a profession requiring civilian control. We argue, however, that the Huntington assertion of "management of violence" as the unique expertise of the profession of arms needs to be updated from his 1957 model. We maintain that members of today's profession of arms are "the managers of effects" while the primary responsibility for defining the desired effects, particularly in the strategic arena, lies with civilian leadership at the national level. This assertion builds upon the concept of soft power introduced by Professor Joseph Nye in 1990, which argued that "winning the hearts and minds has always been important, but it is even more so in a global information age."[6] Since 1990, soft power has grown in importance as information-age technologies advance. More importantly, the information revolution is changing the nature of power and increasing its diffusion, both vertically and horizontally, marking the decline of the sovereign state and the rise of a new feudal-type world.[7] Finally, we maintain that these hard and soft effects could be generated not only in the natural domains of land, sea, air, and space, but also in the increasingly significant manmade domain of cyber.

Huntington's World: Civil-Military Relationships

The profession of arms as we know it owes much to Huntington's ground-breaking framework for civil-military relations and national security. *The Soldier and the State* is rooted in a bipolar world where most of the destructive military power was possessed by the United States and Soviet Union. A key tenet of Huntington's work is a complex relationship between civilian and military authorities, with the military subordinated to civilian control. He offers several prescriptions for achieving and maintaining the stability and the utility of this relationship. The output of Huntington's theory includes an intellectual framework for analyzing the extent to which the system of civil-military relations in a society tends to enhance or detract from the military security of that society.[8]

Huntington's focus is on the nation-state with its responsibility to thwart threats arising from other independent states.[9] For him, achieving a stable and productive relationship between civilian and military authorities is essential for maximum security of the state. A key assumption of Huntington's model is that violence almost always originated with a nation-state and was directed toward another nation-state. In this environment, the threat or actual use of force embodied in national armies, navies, and air forces is the best way to keep the peace. Thus, Huntington asserts that the unique expertise of the military profession is to manage violence.

Huntington's model proved useful for half a century, during which security depended largely on national capacities for managing violence in the natural domains of land, sea, air, and space. His model, however, falls short with the emergence of nonkinetic instruments of foreign policy to include those within the cyber domain. Particularly within that domain, nation-states and their militaries are no longer the sole managers for instruments of force. A new assortment of nonkinetic actors using soft power in the cyber as well as the natural domains can achieve hard-power kinetic effects.

Both national and nonstate actors operating in the cyber domain have targeted Iranian oil ministers' computers, foreign financial institutions and energy sectors, and even senior political and military leaders, causing significant damage.[10] In 2011, Chairman of the Joint Chiefs of Staff Admiral Mike Mullen stated that cyber was "the single biggest existential threat that's out there" because "cyber, actually more than theoretically, can attack our infrastructure and our financial systems."[11] Cell phones, for example, are an essential tool for economic prosperity as well as for financing and planning terrorist operations. Significantly, such cell phones costing $400 today match the computing power of the fastest $5 million supercomputer in 1975.[12]

New Answers to Three Questions

Our call to update Huntington's definitions and prescriptions for the profession of arms is driven by the emergence of new answers to three fundamental questions that have been traditionally used to define a global security situation: Who are the major actors? What can they do to one another? What do they wish to do to one another? Scholars of international politics and national security, beginning with Professor Stanley Hoffmann of Harvard University, have taught us that when the answers to these questions change in significant ways, the global security environment is fundamentally altered.[13] Historical examples include the Peace of Westphalia (1648), French Revolution (1789), Congress of Vienna (1815), unification of Germany (1870), and the end of World War II (1945).

Thus, the emergence of new actors (the United States and Soviet Union), capabilities (nuclear weapons), and intentions (propelled by the ideological split between democratic and communist ideologies) formed the intellectual platform and inspiration for "new thinking" about the profession of arms by early

President Obama at Rural Council meeting in Eisenhower Executive Office Building, February 2016 (The White House/Pete Souza)

Cold War scholars. Quite properly, their analyses and policy prescriptions were based on "new realities" of the postwar period and ultimately came to reflect the desired effect of "containment," which was conceived and developed by civilian leadership at the national level.

Realities of the 21st Century

Now we must come to grips with the new realities of the 21st century that emerged with the fall of communism and the Soviet Empire in the 1990s. With such additional dynamics as the incredible advances in technology and communications as well as the end of the Cold War, the global security system clearly has once again faced new answers to Professor Hoffmann's three fundamental questions. As in 1789, 1815, 1870, and 1945, the global world of national security has been turned on its head.

Who Are the New Actors? Some actors on the international scene have disappeared, while others, to include a variety of non–nation state entities, have emerged. Many of the traditional major actors emerged with the Peace of Westphalia in 1648, the treaty ending the Thirty Years' War.[14] This agreement set the stage for the previous warfighting entities such as families, tribes, religions, cities, and even commercial organizations to consolidate and fight under the monopoly of the nation-state militaries.[15] Until recently, such state-versus-state warfare remained the standard model. However, we are now witnessing a partial resurgence of the pre-Westphalia model as nonstate actors such as the Islamic State of Iraq and the Levant, al Qaeda, Hamas, Hizballah, and others—including drug cartels and crime syndicates—have emerged as very real participants in the international security environment.

What Can They Do to Each Other? As demonstrated by the 9/11 attacks, these nonstate actors are capable of global terrorism using various means of attacking nation-states, from suicide operations to decapitation of individual citizens. Ironically, these new actors are in some important ways "returning to the way war worked before the rise of the state."[16] Many of the nonstate actors also are adept at using modern, nonkinetic instruments such as social media and other tools emerging from the cyber domain to achieve their desired effects. By using these cyber tools, they have, in effect, revitalized and bolstered Sun Tzu's notion of "getting into your opponent's head." They have expanded the battlefield beyond the traditional domains of land, sea, air, and space to accommodate more effectively than ever before the battles of wits.

What Do They Wish to Do to Each Other? Nation-state actors still appear focused primarily on traditional goals of maintaining and expanding their power and influence, but they generally

Secretary-General Ban Ki-moon pays respects to victims of terrorist attack in Paris (United Nations/Eskinder Debebe)

follow internationally accepted Geneva Conventions for conducting war. This is not the case, however, with the new nonstate actors, who frequently have eschewed conventions accepted by the more traditional nation-state actors since Westphalia. For them, the battlefield has taken on a wider range of options with less regard for such notions as just war theory. Indeed, recent attacks involving malware tools for hacking into corporate entities such as banks and large merchandise sales entities (Target, The Home Depot, Sony, and others) as well as Internet accounts of private individuals demonstrate a departure from traditional emphases by combatants on enemy military targets.

The Need for a Wider Lens

Cognitive psychologists tell us that when faced with complex problem sets, we are "wired" to simplify our task by using "frameworks, lenses, or concepts" to reduce the problem scope to a more manageable, "bite-size" challenge. Most certainly, this pertains to the analysis of predicaments that nations face on a continuing basis in the arena of national security. Such analysis is at the heart of John Boyd's "orientation phase," the most critical component of his famous "observe, orient, decide, and act" cycle (the OODA loop).[17] It is the stage in the cognitive process at which the participants attempt to define the "reality" of their problem set. Quite understandably, the simplifying lens traditionally used by leaders in the national security arena has focused on the military weapons of the time. Indeed, this tradition has been employed since at least the Chinese Spring and Autumn periods of the 8th through the 4th centuries BCE. Today, it exists in the form of the combined arms warfare (CAW) concept with its focus being ships, planes, tanks, and missiles.

Cognitive psychologists also tell us that such simplifying lenses inevitably turn out to be inadequate for comprehending realities faced in complex problem sets. We have previously argued that the CAW concept encounters this difficulty when used as a lens.[18] In our current security arena, for example, it fails to accommodate the emerging cyber domain as well as nonkinetic instruments of power resident in the traditional land, sea, air, and space domains. Because the CAW concept limits "vision" to the traditional instruments of military force, new forms of power, to include those emerging from the cyber domain, are anomalies and excluded from our concept of reality. Understanding the power of these anomalies requires a new way of thinking and thus a new and wider lens beyond the traditional CAW lens with its focus on the natural domain weapons systems. The new lens we have offered might properly be called combined effects power (CEP).

The CEP construct is a way to maximize and harmonize the effects of kinetic and nonkinetic power. The key issue it tackles is what effects we want to achieve using both hard and soft power.[19]

In a thoughtful piece titled "Winning Battles, Losing Wars," Lieutenant General James Dubik, USA (Ret.), suggests that this dilemma has characterized virtually all post-9/11 wars and attributes it in large part to the "civil-military nexus that underpins how America wages war."[20] We agree with this assertion and believe that the problem emerges with the very first challenge in international conflicts: the selection of proper war aims. Too often, our war aims (desired effects) are neither crisp and coherent nor realistic in terms of their demands on the American people for blood and treasure. One need only review the predicaments we face or have recently faced in Syria, Iraq, Iran, Afghanistan, and North Korea to understand how battles can be won while their wars are lost.

War aims go wrong when they are based on faulty assessments of reality. Assessments of reality are wrong when the concepts or "lenses" we use to help us understand our security predicaments are unable to accommodate complex challenges. In short, we cannot adequately address the complicated, nonlinear aspects of international conflict in today's world if we rely on the linear CAW approaches designed for the simpler hard-power era of the Cold War. Huntington's 1957 framework was brilliant in its hard-power design and has served us well. The time has come, however, to flesh it out with new realities, including soft power, that square more accurately with the 21st century. We must come to grips with the facts that the post–Cold War era has yielded fundamentally new answers to Professor Hoffmann's three questions.

The Need for a New Way of Thinking

We believe that the first step in this process is to change the initial question that is often asked for addressing emerging challenges in the national security arena. In place of the traditional focus on how we might best combine our military instruments to successfully fight wars of destruction, we must first have an answer to a foundational challenge: What is the *effect* that we wish to achieve? In most situations, particularly at the strategic level, this is a question for our senior civilian policymakers. They must be the primary *determiners* of desired effects. Equally important, they must understand that without a coherent definition of *desired effects*, the military and other entities with foreign policy tools are not in a position to craft effective responses beyond the CAW model. This is true regardless of how accurate their assessments of the security challenge might be.

In sum, we believe Huntington's concept of civilian control, with its emphasis on the professional development of our military, remains vital to a democratic society. Also required is a capability and willingness of our national-level civilian leadership to assume a primary role in determining and articulating desired effects. For its part, the military profession must be capable of managing the full spectrum of capabilities within its purview, both kinetic and nonkinetic, to accomplish the desired effects. This may well require some expansion of the traditional professional development process for military personnel. They will need the expertise for an improved capacity to manage a broad spectrum of tools for achieving desired effects as well as the less complex challenge of Huntington's 1957 notions about managing violence.

And so it is that a new first question—"What is the desired effect at the strategic level?"—can open the door to a more holistic assessment of and response to the security predicaments in which we find ourselves. As such, it broadens our perspective to go beyond a traditional focus on military instruments to include a more balanced appreciation for nonkinetic alternatives in the natural domains of land, sea, air, and space and, equally important, the emerging cyber domain. Once our national security leadership has developed desired effects, they become touchstones that can enable military professionals to go about the task of arraying, selecting, and implementing appropriate strategies and instruments of power. Needless to say, desired effects exist at the operational and tactical as well as the strategic level. Civilian leadership is likely to call for greater military involvement in the development of desired effects at these less strategic levels.

The Need to Update Huntington's Framework: The Sony Example

As we wrote this article, our national leadership's response to the challenge of the cyber strike against Sony Corporation could be described as perplexed, if not confused. Whether it was an attack on a vital American interest or, less seriously, an act of vandalism was unclear. The strike was apparently the product of a national decision by North Korea, but the target was a nonstate actor (Sony), and the location of the strike force could well have been a third country. The attack, while not violent in a traditional way, was serious in its costly impact of some $300 million in damages as well as its negative impact on an American First Amendment core value. In short, it represented major new answers to at least two of the fundamental questions asked by Professor Hoffmann: What can the actors do to one another? What do the actors wish to do to one another? From a traditional perspective, North Korea was not a new participant in our nation's historical arena of conflict, but it was clearly acting in a new cyber domain, which made its fundamental character very different from what we faced when it invaded South Korea in 1950. As such, there may or may not have been a new answer to Hoffmann's third question.

Whatever the case, the 1957 vintage Huntington model was proved an inadequate framework for dealing with the North Korean strike against Sony. Indeed, its narrow focus on traditional instruments of force seemed to suggest only two alternatives, both of which were unacceptable. Few, including the President of the United States, were willing to respond with kinetic instruments of power. At the same time, the United States wanted to make clear to North

Korea and the world that the strike against Sony would not go unpunished. Perhaps this notion of punishment was the "desired effect." If so, the instruments of power to create such punishment fell largely outside the traditional tools relevant to Huntington's definition of the "unique military expertise" as the "management of violence."

Conclusion

National security conflicts are increasingly a battle of wits, and we must update the way we use them to match the increasingly complicated world in which we live. The challenge goes well beyond *what* we think; it is also *how* we think about problem sets that rests on new realities and principles that render traditional linear approaches insufficient, if not irrelevant. Against this background, Huntington's classic framework has proved inadequate for accommodating the cognitive and operational pathways required for meeting today's challenges of the orientation and subsequent phases of Boyd's OODA loop. The Sony crisis can, however, provide an important learning experience for dealing with even more serious situations of a similar nature in the future.

General Dubik's assertion that our modern dichotomy of winning battles and losing wars can be attributed at least in part to the "civil-military nexus that underpins how America wages war" has substantial merit. Waging war involves selecting proper war aims; we see this as the crafting of desired effects and consider it to be primarily the responsibility of senior civilian policy leaders as an initial step in their decision matrix. Such desired effects rise above the selection of kinetic and nonkinetic instruments for their achievement. As such, they provide a critical context for the selection of relevant instruments and their operational deployment. This, we believe, is a managerial and leadership responsibility of the military profession.

In summary, we are calling for a new way of thinking on the part of our senior national security leaders, both military and civilian, to accommodate new answers to Professor Hoffmann's three salient questions. This new way of thinking requires us to adapt our simplifying lens to the more complicated world of the 21st century. It also requires us to ask a new question at the outset: What effects do we want to achieve using both hard and soft power? Fortunately, as cognitive psychologists tell us, we are "wired" to do this. **JFQ**

Thousands of people take part in Madrid rally against terror and war, November 2015 (Adolfo Lujan)

Notes

[1] Don Clark and Nathan Olivarez-Giles, "Hackers Hit Sony, Microsoft Videogame Services," *Wall Street Journal*, December 27–28, 2014, B1.

[2] Carol Lee and Jay Solomon, "North Korean Arms Dealers Targeted," *Wall Street Journal*, January 3–4, 2015, A1.

[3] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: The Belknap Press, 1957), 7.

[4] Ibid., 11.

[5] Ibid.

[6] Joseph S. Nye, Jr., *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004), 1.

[7] Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 113–114.

[8] Huntington, viii.

[9] Ibid, 1.

[10] Isaac Porche, Jerry Sollinger, and Shawn McKay, "An Enemy Without Boundaries," United States Naval Institute *Proceedings* 138, no. 10 (October 2012), 35.

[11] Jason Healey, "No, Cyberwarfare Isn't as Dangerous as Nuclear War," *U.S. News and World Report*, March 20, 2013.

[12] James Manyika et al., *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy* (New York: McKinsey Global Institute, May 2013).

[13] Stanley Hoffmann, *The State of War: Essays on the Theory and Practice of International Politics* (New York: Praeger, 1965), 92–93.

[14] William S. Lind, "Understanding Fourth Generation War," *Military Review*, September–October 2004, 12.

[15] Ibid.

[16] Ibid., 12–16.

[17] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston: Back Bay Books, 2002), 327–344.

[18] Ervin J. Rokke, Thomas A. Drohan, and Terry C. Pierce, "Combined Effects Power," *Joint Force Quarterly* 73 (2nd Quarter 2014).

[19] Ibid.

[20] James Dubik, "Winning Battles, Losing Wars," *Army Magazine*, December 2014, 16–17.