A German infantryman participates in a Combined Georgian special operations force exercise for *Noble Partner 18*, the fourth iteration of the Georgian Armed Forces and U.S. Army Europe cooperatively-led exercise. "Strength through partnership" was the theme for this year's exercise, which also emphasized joint, combined planning for complex operations. (U.S. Army/ Kris Bonet)

Examining Complex Forms of Conflict

Gray Zone and Hybrid Challenges

By Frank G. Hoffman

The Joint Force, and the national security community as a whole, must be ready and able to respond to numerous challenges across the full spectrum of conflict including complex operations during peacetime and war. However, this presupposes a general acceptance of a well-understood taxonomy describing the elements that constitute the "continuum of conflict." The U.S. security community lacks this taxonomy, despite its engagement in a spate of diverse conflicts around the globe from the South China Sea, to Ukraine, Syria, Iraq, and beyond. Partially as a result of this conceptual challenge, we are falling behind in our readiness for the future. As the Chairman of the Joint Chiefs of Staff General Joseph Dunford has admitted "We're already behind in adapting to the changed character of war today in so many ways."[1] The U.S. national security establishment must devote greater attention to the range of challenges and adversaries it faces. The first step is recognizing the diversity of potential conflicts and understanding the relative risks of each.

American strategic culture is sometimes criticized for its emphasis on conventional, interstate war. This was acknowledged in a major 2012 lessons learned project produced by the U.S. Joint Chiefs of Staff that observed how a "big war" paradigm clouded our understanding and delayed the adaptation required for U.S. forces to succeed in Iraq and Afghanistan.[2] The tendency to ignore certain types of threats or forms of conflict has impeded U.S. strategic performance in the past, and will continue to do so until we grasp the full range of conflict types.[3] Without explicit recognition of diverse conflict types in U.S. strategy and doctrine, the armed services are likely to remain in a perpetual state of costly and reactive adaptation when called upon to address various threats.[4]

As should be expected in any attempt to describe something as complex as war, there is much debate over characterizations and definitions. The lexicon of national security and defense analysis has been strained lately, struggling to describe the emerging and ambiguous complex threats we face, most of which fall well short of conventional war. Indeed, some threats do not meet the current threshold of what we think of as war at all.

Embracing a narrow conventional conception of conflict does not prepare future leaders for the range of emerging threats we face, nor is it conducive to developing doctrine and training. A myopic focus on conventional threats obscures the complexity of the phenomena and oversimplifies the challenges. It may also be a way of overemphasizing a preferred mission set or a conventional, big war paradigm, which narrows our

Dr. Frank G. Hoffman is a Distinguished Research Fellow at National Defense University.

cognitive understanding of conflict.[5] That is a risk we have been bearing and for which we have paid a dear price for far too long.

As the Prussian theorist of war, Carl von Clausewitz argued, war is an ever-evolving, interactive phenomena.[6] Understanding the complexity and distinctions of various modes of warfare conducted across the continuum of conflict is critical, as is understanding our adversaries, their methods, and conceptions of victory. To navigate through the fog of complexity, a heuristic construct for conflict is presented in Figure 1.

Rather than perpetuate the binary peace/war distinction, this continuum of conflict depicts a range of different modes of conflict arrayed by increasing levels of violence, from measures short of armed conflict, to large-scale conventional wars, utilizing modality and scale of violence as distinguishing factors. A continuum is not a rigid tool, but rather an intellectual construct that opens our cognitive lens to the full-range of challenges we must understand, and will bring analytic coherence to both the complex array of contemporary security problems as well as the range of the military professional's domain within the national security arena.

Well-defined elements within the continuum of conflict facilitate our thinking about future and current opponents and their ways of war.[7] Though some scholars have rejected such parsing and argue for a unitary vision of war, war can take many forms.[8]

Back to the Future

The Joint Staff's projected security environment forecasts a future of contested norms in which adversaries will employ stratagems to gain influence and undermine U.S. interests with techniques well short of traditional armed conflict.[9] This is not unprecedented. During the Cold War, the United States faced persistent efforts to undermine order, weaken our alliances, and undercut our interests by activities well short of military violence. The former Soviet Union had well-established directorates in their intelligence organizations designed to sow discord, de-legitimize political opponents, and weaken the resolve of the North Atlantic Treaty Organization NATO alliance.[10]

Cold War and recent experience with Russia suggests that the mixture of political, economic, and subversive activity is a consistent element of their operational art.[11] Russia uses these tactics in Ukraine and elsewhere, a form of "simmering borscht" that seeks to extend Moscow's sphere of influence without triggering an armed response. The former Soviet Union frequently employed what it called "active measures" in the information domain, including forgery, propaganda, and false stories or "fake news."[12] Russia's interest in and

FIGURE 1: A HEURISTIC CONSTRUCT FOR CONFLICT.

application of active measures does not seem to have abated, and has perhaps even intensified via social media and proliferating fake news outlets in the last several years.[13] This includes the development of "social bots"—computer-generated online accounts implanted into sites like Facebook that masquerade as real users—to communicate and amplify narratives or disinformation streams. These can dominate or manipulate group pages and disseminate political advertisements. Facebook representatives testified to Congress that prior to the U.S. Presidential election in 2016 a Russian "troll farm" with ties to the Russian Government paid $100,000 for advertisements that produced thousands of Facebook and Instagram posts, to which more than 125 million users could have been exposed. The same Russian firm, the Internet Research Agency, has made widespread use of bots in its attempts to manipulate public opinion through the use of social media.[14] This is the 21st century version of classical Soviet *dezinformatsiya*.[15]

Russia's current leaders emerged from Soviet intelligence entities and seem experienced in the use of covert approaches and the use of distortion, disinformation, subversion, and propaganda.[16] Russian meddling in U.S. electoral campaigns has received much attention lately, but such influence efforts have been a routine part of their arsenal of trade tricks.[17] Russia has also directed its cyber mischief activities at Estonia, Georgia, and Ukraine.[18] Moscow's interference in European political parties, and its development of soft power "false front" organizations is also noteworthy.[19]

Russia's toolkit has always included the exploitation of non-military aggression.[20] Experts have identified the extent to which Russia appears willing to go to project influence and sow confusion within U.S. and European democracies.[21] While Russia's cyber and propaganda intrusions are intensifying, the U. S. Government is neither effectively organized nor conceptually prepared to address Russia's information weapons.[22]

More recently, China's use of diplomatic assertions, deliberate use of fishery/maritime law enforcement forces, and aggressive seizures of disputed islands in the Pacific offer another modern case study.[23] China's assertiveness in the South China Sea appears designed to erode the existing international order and change the norms of international behavior by acts of latent coercion. Maritime militia forces have allowed China not only to disrupt foreign survey, energy development, and commercial fishing operations, but to extend and consolidate areas it views as Chinese territory with low escalatory risks.[24] China strikes with all instruments of national power, and has particularly intensified its use of military diplomacy since 2009.[25] China has also learned to wield influence using funding to both incentivize and coerce academic and media voices.[26]

China is well-organized to conduct operations short of military conflict.[27] As the scholar Stefan Halper perceptively noted in a study from 2014 for the Pentagon, China "employs diplomatic pressure, rumor, false narratives, and harassment to express displeasure, assert hegemony and convey threats."[28] Guided by the doctrinal principle of "disintegrating enemies," political warfare promotes the suppression of perceived threats to China by using psychological operations as a means of leading international discourse and influencing policies of friends and foes. Propaganda, carried out during both peacetime and in armed conflict, amplifies or attenuates the political effects of the military instrument of national power.[29] Recent reports that China is operating deep inside Australia to destabilize the Australian government and turn it toward Chinese aims suggest that Beijing's doctrine is more than merely academic.[30]

Some analysts from the Chinese People's Liberation Army (PLA) argue that future wars will be marked by the "three non" warfares: non-contact (*fei jierong*), non-linear (*fei xianshi*), and non-symmetric (*fei duicheng*). In non-contact warfare the more advanced adversary exploits

its advantage by staying outside the reach of the other side's weapons, while retaining the ability to directly target and strike its rival.[31] Chinese conceptions of "quasi-war" and "three warfares," as depicted in Figure 2, embrace legal, psychological, and information activities short of war.[32] China's growing conventional military power suggests that it is employing these techniques as it builds up its national power and extends its military reach. To what degree will it retain an interest in non-contact and indirect methods when it has obtained regional parity? Recent research suggests that a convergence of China and Russian tactics is occurring, emanating from Chinese interpretations of Russia's actions in the Crimea and in the cyber domain. This is not authoritative but we should also expect Russia (and others) to absorb lessons from the South China Sea.[33]

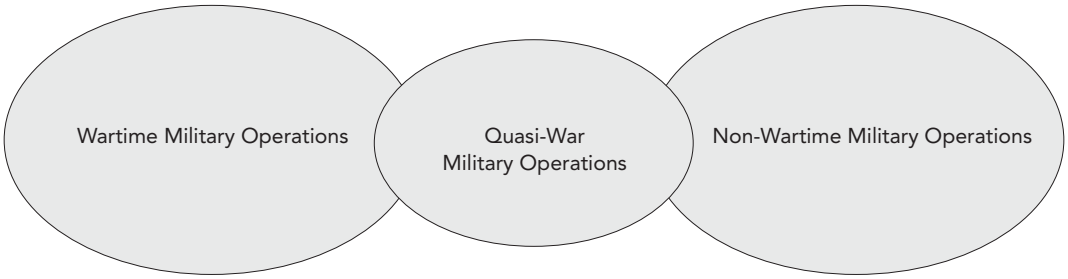
Clarity and Unclarity in the Gray Zone

The need to compete with greater agility at lower levels short of war, against multi-functional or multi-dimensional threats is belatedly recognized today. The gap has existed for some time and was deemed decades ago to be a shortfall in U.S. strategic culture.[34] More recently, a security scholar noted,

> *By failing to understand that the space between war and peace is not an empty one—but a landscape churning with political, economic, and security competitions that require constant attention—American foreign policy risks being reduced to a reactive and tactical emphasis on the military instrument by default.*[35]

This suggests that the U.S. security or policy community does not recognize the importance of competing in this arena. However, an examination of any regional or theater commander's engagement plans would suggest this view is somewhat exaggerated. Theater security cooperation plans, military-to-military engagement, military aid or support, exercises and various forms of engagement are routinely employed by our regional commands to compete for influence and signal U.S. commitment.[36] The United States has recently been heavily engaged in many failing states and regions employing what might be best described as the constructive and stabilizing instruments of traditional statecraft. We may need to better understand and execute these missions, and scholars have recently noted that our assistance

FIGURE 2: WAR, QUASI-WAR, AND NON-WAR, AS EXPRESSED IN A PLA TEXT FROM 2009.



Source: Liu Xiaoli, *Military Response to Significant Sudden Incidents and Crises: Research on Military Operations Other than War*, 8. Adapted from Alison A. Kaufman and Daniel M. Hartnett, *Managing Conflict: Examining Recent PLA Writings on Escalation Control* (Arlington, VA: CNA, 2016), 26.

TABLE 1: FORMS OF STATECRAFT AND INFLUENCE.

Traditional/Legitimate	Non-traditional/Illegitimate
Security cooperation and foreign military sales	Political subversion by penetration or false-front organizations
Economic sanctions	Economic corruption
Public diplomacy and support for IGO/NGO	Propaganda/psychological operations/disinformation
Military presence/engagements/exercises	Cyber intrusions/cyber corruption/disruption
Foreign internal defense	Sponsored criminal activity
Freedom of navigation exercise (maritime or aerospace domains)	Electoral interference

programs can be improved.[37] It is the character of tools used that distinguishes us from other powers. Some of the tools used by others are more ambiguous and nontraditional instruments of statecraft, and may be of nefarious or of questionable legitimacy. The salient questions are: "are we doing the right things? are we doing enough? and, are the right agencies doing it?" Table 1 presents a sample list contrasting these two sets of tools.

Scholars and practitioners within the Department of Defense, and the U.S. Special Operations community in particular, have examined various case studies to better understand how to conceptualize the problem set and respond accordingly. Some recall U.S. diplomat George Kennan urging the use of political warfare to counter adversary activities.[38] Kennan defined political warfare as "the employment of all the means at a nation's command, short of war."[39] His understanding of the problem was informed by a deep understanding of Russian strategic culture and its preference for indirect methods. But his definition was too expansive ("all means") and mislabeled as a form of warfare despite its focus on activities "short of war." The term was used during the Cold War with a general understanding, though eventually displaced by covert action (or activities). It has generally been dropped from governmental usage.[40] Kennan himself recognized this in his lectures on "Measures Short of War" during the 1950s at the National War College.[41]

The conflict mode which Kennan originally referred to as political warfare has recently been re-anointed as "gray zone conflict." Actors in the gray zone are,

> *employing sequences of gradual steps to secure strategic leverage. The efforts remain below thresholds that would generate a powerful U.S. or international response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time.*[42]

As noted this is not unprecedented; in fact, it rather resembles classical "salami-slicing" strategies, fortified with a range of unconventional techniques—from cyberattacks to information campaigns to energy diplomacy. One scholar lists numerous current relevant examples, including the ongoing crisis in eastern Ukraine. But Ukraine—particularly the fighting in Donbas—has blown past being an ambiguous "no-man's land" or gray zone, given the violent scope of the conflict (10,000 dead) and the overt use of advanced conventional power (armor, rockets, missiles).

Others argue that,

> *the gray zone is characterized by intense political, economic, informational, and*

> *military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war.*[43]

Yet others note that gray zone conflicts,

> *involve some aggression or use of force, but in many aspects their defining characteristic is ambiguity—about the ultimate objectives, the participants, whether international treaties and norms have been violated, and the role that military forces should play in response.*[44]

They list Russia's annexation of Crimea, its support of separatists in eastern Ukraine; the Islamic State of Iraq and the Levant (ISIL) advances; Boko Haram's insurgency in Nigeria, among others, as gray zone conflicts. That range includes very distinct conflicts and asks a lot of the concept. Russia's war inside Ukraine is hardly covert or ambiguous. Similarly, ISIL is responsible for an estimated 20,000 fatalities, and an estimated 10,000 casualties in Nigeria have been attributed to Boko Haram. These belligerents appear to worry little about crossing lines or facing escalation from the international community. Clearly these are not gray or ambiguous acts.

The definition of gray zone conflicts remains both expansive and elusive. Definitions found in recent literature are applied very inconsistently and do not contribute to analytic coherence as they cover such a vast portion of the conflict spectrum, overlooking different historical contexts, methods, and best practices. These over-wide definitions rob gray zone conflict of analytical utility, as they mask more than they reveal. Indeed, this new term captures more a failure in U.S. military and security culture than it characterizes any new method or form of conflict. The real gray zone is "between our ears," in our faulty models and education about what conflict entails. Enshrining our intellectual fault line as an opponent's method is not enlightening. As John Arquilla, a professor and Chair of Defense Analysis at the Naval Postgraduate School, has convincingly argued, instead of creating an imaginary zone, we should understand that all of this activity is an essential part of the realm of human conflict.[45]

The importance of the measures addressed by these scholars is valid even as they struggle to define it. This area has been consistently highlighted by strategic assessments of the U.S. Intelligence Community and cannot be ignored.[46] The only issue is whether the use of these tactics will dissipate or increase in the future.

Conceptual progress requires clear and distinct definitions, and vague terms like political warfare or gray zone are of limited help.[47] This is not war in the classic sense, but we should not misconstrue the fundamental element of conflict inherent to this part of the security environment.

A formal definition of gray zone tactics is offered:

> *Those covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage.*

This definition emphasizes the actual activities over intent. Placing this to the far left of the proposed continuum of conflict, short of violent military force or war, represented by the thick red line, positions it clearly along the continuum of challenges that our security policy must address.

Defining Hybrid Warfare

Nearly 15 years ago, analysts in the Department of Defense and at the Marine Corps' Warfighting Lab identified trends and evidence of deliberate efforts to blur and blend methods of war. Their forecast suggested that the prevailing technological advantage of the American-dominated Revolution

in Military Affairs would produce a counter-revolution that would exploit the convergence of different modes of conflict. This threat hypothesis evolved into a theory of hybrid threats.[48] The projection was affirmed in the summer of 2006 in Southern Lebanon by the actions of Hezbollah, and appears to be relevant to other conflicts as well.[49] Three U.S. Secretaries of Defense, including the incumbent, have found the hybrid warfare concept useful and have warned of the emergence of hybrid adversaries.[50]

Military leaders as well, including Chiefs of Staff of the Army and several Joint leaders, have recognized that current categories do not match contemporary conflict.[51] Hybrid threats are frequently referred to in the 2010 Quadrennial Defense Review, national-level intelligence reports on the future character of war, and in various top-level documents of other countries.[52] The Futures Study Group at NATO–Allied Command Transformation (ACT) also anticipated this threat in 2007.[53] Numerous policymakers and military leaders have agreed, as shown in Figure 3.

A hybrid threat transcends a blend of regular and irregular tactics. More than a decade ago, it was defined as an adversary that "simultaneously and adaptively employs a fused mix

FIGURE 3: HYBRID WARFARE, AS MENTIONED BY SELECT U.S. DEFENSE AND POLICY OFFICIALS.

Hybrid warfare will be a defining feature of the future security environment.

—the Honorable Michele Flournoy, then U.S. Under Secretary of Defense for Policy, along with Special Advisor Shawn Brimley, in their article on "The Defense Inheritance: Challenges and Choices for the Next Pentagon Team," *The Washington Quarterly* 30 (Autumn 2008).

In reality, as [academic] Colin Gray has noted, the categories of warfare are blurring and do not fit into tidy boxes. We can expect to see more tools and tactics of destruction—from the sophisticated to the simple—being employed simultaneously in hybrid and more complex forms of warfare.

—the Honorable Robert Gates, then U.S. Secretary of Defense, in his article "The National Defense Strategy: Striking the Right Balance," *Joint Force Quarterly* 52, no.1 (2009).

Rarely are such conflicts decided on conventional battlefields by traditional armies. They become hybrid wars—'a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battlespace.'

—the Honorable Joseph S. Nye, Jr., former Undersecretary of State and Chairman of the National Intelligence Council, in *The Future of Power: Its Changing Nature and Use in the Twenty-First Century* published by PublicAffairs (©2011).

. . . one of the most costly lessons . . . learned over the last decade: how to deal with the challenge of hybrid warfare. It will be increasingly common for the army to operate in environments with both regular military and irregular paramilitary or civilian adversaries, with the potential for terrorism, criminality and other complications.

—General Raymond T. Odierno, then Chief of Staff of the U.S. Army, in his article on "The U.S. Army in a Time of Transition: Building a Flexible Force," *Foreign Affairs* 90, no.3 (May–June 2012).

But if the streets of Baghdad and the valleys of Afghanistan were a laboratory for irregular warfare, I believe that ground force will increasingly need to prepare for future hybrid warfare.

—the Honorable Robert O. Work, then U.S. Deputy Secretary of Defense, in a speech delivered at a U.S. Army War College Strategy Conference in April, 2015.

Future wars could have conventional forces, Special Forces, guerrillas, terrorists, criminals all mixed together in a highly complex terrain environment, with potentially high densities of civilians.

—General Mark A. Milley, 39th Chief of Staff of the U.S. Army as quoted by journalist Helen Cooper in "The War of the Future? Picture Big Armies and Many Fronts," *New York Times*, June 10, 2016.

of conventional weapons, irregular tactics, catastrophic terrorism, and criminal behavior in the battlespace to obtain desired political objectives."[54] The criminal, or more broadly "socially disruptive behavior," and mass terrorism aspects should not be overlooked, but the fusion of advanced military capabilities with irregular forces and tactics is key, and has appeared repeatedly during the past decade from Hezbollah to the Russian campaigns in Georgia and Ukraine.[55] Hezbollah's method of fighting Israel as is described by its leader Hassan Nasrallah, is an organic response to its security dilemma and "not a conventional army and not a guerrilla force, it is something in between."[56] As lethal as Hezbollah has been in the past decade, we should be concerned about the lessons it is learning in Syria from the Russians.[57]

Hybrid threats can also be created by a state actor using a proxy force. A proxy force sponsored by a major power can generate hybrid threats readily using advanced military capabilities provided by the sponsor. Proxy wars, appealing to some as "warfare on the cheap" are historically ubiquitous but chronically understudied.[58]

The hybrid threat concept captures the ongoing implications of globalization, the diffusion of military-related technologies, and the information revolution. Hybrid threats are qualitatively different from less complex irregular or militia forces. They, by and large, cannot be defeated simply by Western counterterrorism tactics or protracted counterinsurgency techniques. Hybrid threats are more lethal than irregular forces conducting simple ambushes using crude improvised explosive devices, but they

A cyber warfare operations officer reviews visualization data as analysts review log files and provide a cyber threat update. (U.S. Air Force/ J.M. Eddins, Jr.)

are not unfamiliar to Western forces and can be defeated with sufficient combat power.[59]

Events in the Crimea and eastern Ukraine have led European security officials to pay greater attention to Russia's assertive behavior and its ways of war. For this reason, hybrid warfare is now an explicit discussion point among NATO military and civilian leaders.[60] In the Crimea, Russia demonstrated that it had learned from its performance in Georgia in 2008 and employed inherently conventional methods, but with better agility and illegal methods.[61] This was hardly new or ambiguous but it was effective under circumstances that are not easily replicated.

Numerous foreign sources describe President Vladimir Putin's preferred method as "hybrid warfare," a blend of hard and soft power. A combination of instruments, some military and some non-military, choreographed to surprise, confuse and wear down an opponent, hybrid warfare is ambiguous in both source and intent, making it hard for multinational bodies such as NATO and the EU to craft a response.[62] This is not novel, especially in Russia. These are actually time-tested methods with which the U.S. security community has experience, albeit not for several decades.[63]

European military analysts, prompted by Russia's behavior, have also embraced the hybrid phenomenon as a feature of contemporary conflict.[64] However the NATO interpretation of hybrid warfare is much broader, depicting it as a mixture of military means with non-military tools including propaganda and cyber activity. This differs from the earlier American definition, and is much closer to the so-called gray zone conflicts described earlier. The distinction between indirect and less violent gray zone conflicts and the more violent methods of hybrid threats has been noted by several scholars.[65] Key NATO leaders define hybrid threats as "a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design."[66] This broad definition could describe just about all wars, which tend to contain combinations of military and non-military activity in an integrated plan. The NATO definition reflects a combination of methods, and clearly emphasizes a purposeful design to achieve desired outcomes, but it does not necessarily include kinetic applications of violent force.

A historical case study illuminates the distinctions between the original, American view of hybrid threats and its more recent NATO interpretation. While Russia's efforts to influence Ukraine's efforts to reach out to the EU constitute an example of a gray zone conflict, clearly competing well short of traditional armed conflict, the ongoing violence in eastern Ukraine is a classical form of hybrid warfare within an integrated design that has produced a costly conflict with more than 10,000 fatalities.[67] The fusion of the various forces or means employed in the Donetsk and Luhansk oblasts (combinations of separatists, Spestnaz special forces, Russian regulars with advanced military capabilities, electronic warfare, drones, large volume rocket launchers, and some armor) is distinctly representative of hybrid warfare.[68] The employment of political repression, influence over food supplies to control the local population, and the accidental catastrophic act of killing of 217 passengers aboard MH–17 suggest a less conventional character closer to the middle of the conflict spectrum, and all are elements consistent with hybrid threat methods. The evidence of rampant corruption and suppression of employment and economic security evince all the elements of a hybrid operational context which appear to be part of a deliberate design.[69] Those who have repeatedly visited Ukraine and Donbas confirm the conflict as inherently hybrid in accordance with the original definition.[70]

As a recent RAND Corporation report noted, Chief of the General Staff of the Armed Forces of Russia Valery Gerasimov's article described the current character of warfare, rather than outlining a particular doctrine or institutional approach.[71] The Russian understanding of conflict constitutes

a full spectrum approach, which means it can include measures short of war or more violent hybrid approaches as appropriate to the situation.[72] Historically, Russia's approach has appreciated the value of indirect approaches and non-military instruments. We would do well to better re-learn Russia's strategic culture and history.[73]

The NATO Defense College has been at the forefront of thinking on this topic, and other European analysts are carefully examining the implications.[74] These analyses are primarily focused on the intelligence agencies that make routine use of the criminal underworld for "services" including cyberattacks and violence. As U.K scholar Mark Galeotti has noted, "one of Russia's tactics for waging war is using organized crime as an instrument of statecraft abroad."[75] The malign influence of criminal activity and the corrupting nature of illicit networks in the battlespace is growing and merits greater study.[76] It should be made clear that Russia would employ these criminal networks in both measures short of armed conflict and in more violent contingencies.

We should also be concerned about Hezbollah and the lessons it may be absorbing from its stint in Syria.[77] Hezbollah has always been more than a well-armed guerilla movement and constituted a more classical hybrid threat. Now, though it has suffered significant combat losses, it has also been exposed to an extensive learning cycle from the Russian special operations advisors supporting the Assad regime. Hezbollah's own special forces may have mastered the integration of cyber, combined arms, and intelligence operations at an even higher level than before. Thus, even if ISIL is defeated and Syria is stabilized into a stalemate, our allies in Israel may face a greater threat than before.

To update our understanding and better distinguish hybrid conflict from irregular warfare, a revised definition of the former is offered:

> *The purposeful and tailored violent application of advanced conventional military capabilities with irregular tactics, with terrorism and criminal activities, or combination of regular and irregular forces, operating as part of a common design in the same battlespace.*

The major distinction here is the addition of "violent" to the definition to clarify its placement in the continuum, and to further distinguish it from activities short of violent conflict.

Looking Forward—So What?

All elements of the U.S. national security community must assess and prepare for the complete array of challenges they face in today's dynamic environment. As Clausewitz said in probably his most oft-quoted passage,

> *. . . the first, the supreme, the most far reaching act of judgment that the statesman and commander have to make is to establish . . . the kind of war on which they are embarking.*[78]

One cannot make this supreme judgment without a deep understanding of history, of war and the various ways in which it is waged. Lacking that understanding increases the risk of mistaking the essential nature of the conflict being considered or those we must adapt to as a result of the ever-evolving character of warfare.[79] The continuum concept and hybrid threats remain controversial since they distract from the efforts of "big wars" and great power competition advocates.[80]

The new U.S. National Defense Strategy (NDS) identifies China and Russia as our primary competitors and threats.[81] Some analysts misread the NDS as embracing great power wars of a conventional type. This misinterpretation of the strategy reflects a lack of appreciation for both Chinese and Russian strategic culture, which both recognize unconventional methods and non-military conflict. The Secretary of Defense and his NDS explicitly recognize a full

spectrum of conflict and warn against over-investing in a single and preclusive form of warfare, a mistake an adversary will surely exploit.[82] We face an array of different threats and require a comprehensive suite of options to address the full range of conflict we may face. Joint doctrine recognizes a conflict continuum, yet fails to define it in detail.[83] Doctrinal efforts to address that are in progress.

The Secretary of Defense and his NDS explicitly recognize a full spectrum of conflict and warn against over-investing in a single and preclusive form of warfare, a mistake an adversary will surely exploit.[82] We face an array of different threats and require a comprehensive suite of options to address the full range of conflict we may face. Joint doctrine recognizes a conflict continuum, yet fails to define it in detail.[83] Doctrinal efforts to address that are in progress.

Yes, we are facing an era of great power competition, but that competition is not inherently limited to one point in the continuum. The first step in generating an effective response to the challenge our adversaries may present along the continuum is defining what that continuum consists of, with some granularity.[84] Until we do so we will continue to be outplayed at influence competitions and will remain surprised at the ingenuity of our adversaries and their evolving ways of warfare.[85] We should also remain cognizant of the reality that major adversaries now have the means to directly attack our political will and the resilience of our societies and will attempt to do so in any form of conflict, well to the left of armed conflict or during high-intensity conflict.[86]

Countering measures short of armed conflict is the subject of various new studies, and the U.S. defense policy community and military are belatedly devoting significant intellectual capital to this issue.[87] But countering this method of conflict will require more than traditional military strategy responses and must incorporate more than special operations forces. We must establish a broader framework for conflict short of violent warfare that incorporates a wider range of tools than the traditional set, and special forces, or paramilitary operations.[88] For example, how do we counter manipulation of elections and efforts to sow discord via cyber intrusions and the deliberate distribution of false information?[89] How do we ensure that forms of subversion or disinformation, at home and abroad, are neutralized? Getting beyond the operational or tactical perspective is surely warranted as suggested by the U.K. scholar, Dr. Robert Johnson of Oxford's Changing Character of War Programme.[90]

Political Aims

A particularly valid point is the need to consider the political dynamics of conflict, not just its methods or modes. This is not simply a statement of the obvious.[91] It addresses a longstanding deficiency in the American way of war. "Too often governments miss critical components of their adversary's strategy, typically because of a near-exclusive focus on its use of violence. Partial responses such as these can be counterproductive."[92] This is the largest deficiency in hybrid threat theory; its emphasis on "how" the adversary applies violence overlooks the

"why," which is ultimately more critical to counter–strategies and conflict resolution.

Intelligence

U.S. analysts should continue to explore past and current doctrine of our major competitors. Ongoing changes in the Russian way of war, and how their mental model is adjusting under Putin's leadership, are worthy of detailed assessment.[93] But this work should go beyond military articles and speeches that will offer little insight into a decisionmaking circle that is centered on President Putin and a clique largely comprised of former KGB officers. A broader evaluation of Russian history and nonconventional methods is more appropriate to compete with Moscow's propensity to target seams and institutional gaps with its active measures.

Organization

Once we ascertain the relative scope of the problem, structural issues must be addressed, along with authorities. How should we organize ourselves to address this challenge?[94] Is this a function for the State Department, or is an interagency model similar to the National Counterterrorism Center needed to better integrate activities in intelligence, campaign design, and assessment in counter–influence activities? This may be another place where the Special Operations community can apply its unique skill sets in the post–counterterrorism world.[95]

Multi-Dimensional Partnerships

What is evident is the changing character of conflict today, which demands both a mindset and an organizational approach that is creative and multi-dimensional. The capacity to generate and execute effective strategies across government lines, including private sector and international organizational contributions, is especially salient in complex contingencies. The relative weight of intelligence, law enforcement, development, information activity, and military security will vary depending on the contingency, but there is no doubt that complex conflicts require more than sheer conventional military might.[96] Both field experience and scholarship on networked and multi-dimensional problems demonstrate that we will require equally inventive solutions.[97]

Understanding our future security challenges demands that we reflect and interpret the past, understand the present, and think rigorously about what lies over the horizon in order to adapt to the changing character of conflict.[98] This requires keeping an open and informed mind about the breadth of the various modes of conflict that exist. The wars of the 21st century may take many forms. As conflict reflects a greater degree of convergence and complexity, so must our mental models and frameworks. PRISM

Notes

[1] General Joseph Dunford, USMC, remarks at National Defense University Graduation Ceremony, Ft. McNair, DC, June 10, 2016. Available at <http://www.jcs.mil/Media/Speeches/Article/797847/gen-dunfords-remarks-at-the-national-defense-university-graduation/>.

[2] U.S. Joint Chiefs of Staff, *Decade of War: Vol. 1: Enduring Lessons from the Last Decade of Operations*, Suffolk, VA: Joint and Coalition Operational Analysis, June 15, 2012.

[3] Frank G. Hoffman, "Small Wars Revisited: The United States and Nontraditional War," *Journal of Strategic Studies*, Vol. 28, no. 6 (December 2005); David Johnson, *Doing What You Know: The United States and 250 Years of Irregular War*, Washington DC: Center for Strategic and Budgetary Assessment, August 2017.

[4] Jan K. Gleiman, "The American Counterculture of War: Supporting Foreign Insurgencies and the American Discourse of War," *Special Operations Journal*, Vol. 1, no. 1 (2015), 19–36.

[5] For an argument for a general unitary conception of warfare see Dr. Al Palazzo, "Forging Australian Land Power: A Primer," Directorate of Future Land Warfare, Australian Army, *Army Research Papers no. 7*, (December 2015), 8–9.

[6] Christopher Mewett, "Understanding War's Enduring Nature," *War on the Rocks*, January 21, 2014, available at <http://warontherocks.com/2014/01/

understanding-wars-enduring-nature-alongside-its-changing-character/>.

[7] See the arguments against categories from a strategic theorist, Colin Gray, "Categorical Confusion, The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional," Carlisle, PA: Strategic Studies Institute, February 2012.

[8] On an argument in favor of a unitary perspective see Hew Strachan, *The Direction of War: Contemporary Strategy in Historical Perspective* (New York: Cambridge University Press, 2012), 112.

[9] VADM Kevin Scott, USN, *Joint Operating Environment 2035*, Washington, DC: Joint Chiefs of Staff/J7, July 14, 2016, ii.

[10] Christopher Andrew and Vasili Mitrokhin, T*he Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB,* 1999; Christopher Andrew and Oleg Gordievsky, *Comrade Kryuchkov's Instructions, Top Secret Files on KGB Foreign Operations, 1975-1985*, Stanford, CA: Stanford UP, 2005.

[11] Victor Madeira, "Russian Subversion: Haven't We Been Here Before?," July 30, 2014, available at <http://www.statecraft.org.uk/research/russian-subversion-havent-we-been-here>; David Maxwell, "Taking a Spoon to a Gunfight," *War on the Rocks,* April 2, 2014.

[12] Vasily Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officer Handbook* (London: Frank Cass, 1992), 13. On Russian historical cases see Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, McLean, VA: Pergamon-Brassey's, 1984; U.S. Information Agency, *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*, Washington DC: USIA, June 1992. Events in the fall of 2016 suggest that the Russians have continued their practices, see Craig Timberg, "Research ties 'fake news' to Russia," *The Washington Post*, November 25, 2016, A1, A15.

[13] Martin Kragh and Sebastian Asberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, January 5, 2017, available at <http://dx.doi.org/10.1080/01402390.2016.1273830>.

[14] Craig Timberg and Elizabeth Dwoskin, "Russian content on Facebook, Google and Twitter reached far more users than companies first disclosed," *The Washington Post*, October 30, 2017, available at <https://www.washingtonpost.com/business/technology/2017/10/30/4509587e-bd84-11e7-97d9-bdab5a0ab381_story.html?utm_term=.08451ccd09c6>.

[15] Adam Taylor, "Before 'fake news,' there was Soviet 'disinformation'," *The Washington Post*, November 26, 2016.

[16] Jolanta Darczewska, "The Anatomy of Russian Information Warfare, The Crimean Operation," *Point of View*, Warsaw: Centre for Eastern Studies, May 2014.

[17] Mark Kramer, "The Soviet Roots of Meddling in U.S. Politics," *PONARS Eurasia Policy Memo # 452*, Washington, DC, January, 2017, available at <http://www.ponarseurasia.org/memo/soviet-roots-meddling-us-politics>.

[18] Michael Birnbaum, "Russian's Tactics Roil Europe," *The Washington Post*, August 14, 2016, 1; and the joint statement from the Department of Homeland Security and Director of National Intelligence, Washington, DC, October 7, 2016 available at <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.

[19] Orysia Lutsevych, *Agents of the Russian World (Proxy Groups)* (London: Royal United Services Institute, April 2016).

[20] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" Vol. 27, no. 1, *Journal of Slavic Military Studies*, 2014, online at <http://www.tandfonline.com/doi/abs/10.1080/13518046.2014.874845>; Kier Giles et al, *The Russian Challenge*, London: Royal Institute of International Affairs, Chatham House Report, June 2015; Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare," Vol. 160, no. 4 *RUSI Journal* (Fall 2015), 40–48.

[21] For assessment on Russian mastery of information distortion in multiple mediums see: Clint Watts, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns." Statement prepared for the Senate Select Committee on Intelligence, March 30, 2017. Available at <https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf>; Clint Watts. "Cyber-enabled Information Operations." Statement prepared for the Senate Committee on the Armed Services, Subcommittee on Cybersecurity, April 27, 2017, available at <https://www.armed-services.senate.gov/download/watts_04-27-17>; Clint Watts, "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions," Statement prepared for the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, October 31, 2017, available at <https://www.fpri.org/article/2017/10/extremist-content-russian-disinformation-online-working-tech-find-solutions/>.

[22] Mike Rogers, "America Is Ill-Prepared to Counter Russia's Information Warfare," *Wall Street Journal*, March 28, 2017, A17.

[23] Andrew S. Erickson, Connor M. Kennedy, "Beware of China's "Little Blue Men" in the South China Sea," *The National Interest*, September 15, 2015, available at <http://nationalinterest.org/blog/the-buzz/beware-chinas-little-blue-men-the-south-china-sea-13846>.

[24] See Andrew S. Erickson and Connor M. Kennedy, "Countering China's Third Sea Force: Unmask Maritime Militia before They're Used Again," *The National Interest*, July 6, 2016, available at <http://nationalinterest.org/feature/countering-chinas-third-sea-force-unmask-maritime-militia-16860?page=show>.

[25] Kenneth Allen, Phillip C. Saunders, and John Chen "Chinese Military Diplomacy, 2003–2016: Trends and Implications." Washington, DC: Center for the Study of Chinese Military Affairs, *China Strategic Perspectives 11*, 2017.

[26] "China's Foreign Influence Operations Are Causing Alarm in Washington," *Washington Post* December 11, 2107, at <https://www.washingtonpost.com/opinions/global-opinions/chinas-foreign-influencers-are-causing-alarm-in-washington/2017/12/10/98227264-dc58-11e7-b859-fb0995360725_story.html?utm_term=.c0b74b7e2aff>; Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov, and Gabriela Pleschová, "Sharp Power, Rising Authoritarian Influence," National Endowment for Democracy, December 2017, available at <https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf>.

[27] Mark Stokes and Russell Hsiao, *The People's Liberation Army General Political Department Political Warfare with Chinese Characteristics*, Washington, DC: Project 2049 Institute, October 14, 2013. For an earlier study see J. Michael Waller, "Chinese Political Warfare Strategy Against the US," *Institute of World Politics Insight*, April 23, 2001, available at <http://www.iwp.edu/news_publications/detail/chinese-political-warfare-strategy-against-the-us>.

[28] Quoted in Peter Navarro, "China's Non-kinetic Three Warfares Against America," Center for National Interest's The Buzz (blog), January 5, 2016, available at <http://nationalinterest.org/blog/the-buzz/chinas-non-kinetic-three-warfares-against-america-14808>.

[29] Li Yan, "Implementing 'Four Transformations' in Peacetime Political Mobilization," *China Military Online*, May 7, 2012, available at <http://chn.chinamil.com.cn/yby/2012-05/07/content_4854257.htm>; Timothy L. Thomas, "New Developments in Chinese Strategic Psychological Warfare," *Special Warfare*, April 2003.

[30] Irene Luo, "Former Chinese Diplomat On China's Infiltration of Australia," *Epoch Times*, July 7, 2017; Harry Krejsa, *Under Pressure: The Growing Reach of Chinese Influence Campaigns in Democratic Societies* (Washington, DC: Center for a New American Security, April 2018).

[31] Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare," Washington DC: Heritage Foundation, *Backgrounder No.2692*, May 21, 2012; Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response," Washington DC: Heritage Foundation, *Backgrounder No. 2745*, November 26, 2012.

[32] Stephan Halper, "China: The Three Warfares," May 2013, available at <http://images.smh.com.au/file/2014/04/11/5343124/China_%2520The%2520three%2520warfares.pdf?rand=1397212645609>. Sangkuk Lee, "China's Three Warfares, Origins, Applications, and Organizations," *Journal of Strategic Studies*, Vol. 37, no. 2 (April 2014), 198–220.

[33] Lora Sallman, "Little Grey Men: China and the Ukraine Crisis,", Vol. 58, Issue 6 *Survival* (2016), 135–156.

[34] See David Tucker and Christopher J. Lamb, "Peacetime Engagement" in Sam Sarkesian and Robert Connor, *America's Armed Forces, A Handbook of Current and Future Capabilities* (Westport, CT: Greenwood Press, 1996).

[35] Nadia Schadlow, "Peace and War, the Space Between," *War on the Rock*, August 18, 2014, available at <http://warontherocks.com/2014/08/peace-and-war-the-space-between/>.

[36] On the role and complexity of signaling through exercises see Beatrice Heuser, Tormod Heier, and Guillaume Lasconjarias, eds., *Military Exercises: Political Messaging and Strategic Impact* (Rome: NATO Defence College, 2018).

[37] Marla E. Karlin, *Building Militaries in Fragile States Challenges for the United States* (Philadelphia: University of Pennsylvania Press 2018).

[38] Max Boot and Michael Doran, "Political Warfare: Changing America's Approach to the Middle East," Brookings, June 28, 2013, available at http://www.brookings.edu/research/opinions/2013/06/28-political-warfare-us-middle-east-counterterrorism-doran-boot. On the application of Political Warfare in the 21st Century, see the White Paper, *SOF Support to Political Warfare*, U.S. Army Special Operations Commander, Ft. Bragg, NC, March 10, 2015.

[39] For Kennan's policy memo promoting this initiative under the auspices of the State Department, see: <http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm>.

[40] For an unsuccessful attempt to defend the term see Jeffrey V. Dickey, Thomas B. Everett, Zane M. Galvach, Matthew J. Mesko and Anton V. Soltis, *Russian Political Warfare: Origins, Evolution and Application*, Monterrey, CA: Naval Postgraduate School, unpublished M.A. thesis, June 2015.

[41] Giles D. Harlow and George C. Maerz, eds., *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-47* (Washington, DC:

NDU Press, 1990), 6–8. He noted that "The varieties of skullduggery which make up the repertoire of the totalitarian government are just about as unlimited as human ingenuity itself, and just about as unpleasant."

[42] Michael Mazarr, "Mastering the Gray Zone," Carlisle, PA: Strategic Studies Institute, 2015.

[43] General Joseph L. Votel, statement before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, March 18, 2015; Captain Philip Kapusta, U.S. Special Operations Command (USSOCOM) white paper, "Defining Gray Zone Challenges," April 2015.

[44] David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks*, May 19, 2015.

[45] John Arguilla, "Perils of the Gray Zone, Paradigms Lost, Paradoxes Regained," Vol. 7 no. 2, *PRISM*, 2018, 124.

[46] Office of the Director of National Intelligence, *Global Trends: Paradox of Progress* (Washington, DC: National Intelligence Council, 2017).

[47] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Chicago, IL: Quadrangle, 1964), 41–77;William Roseau, *Subversion and Insurgency,* Santa Monica, CA: RAND, Counterinsurgency Study Occasional Paper, 2007, 4.

[48] William. J. Nemeth, USMC, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterrey, CA: Naval Postgraduate School, Master's Thesis, June 2002; James N. Mattis and Frank Hoffman, "Hybrid Threats and the Four Block War," *Proceedings*, September 2005; Frank Hoffman, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict," *Strategic Forum 240*, Washington, DC: Institute for National Strategic Studies, April 2009.

[49] David Johnson, *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza* (Santa Monica, CA: RAND, 2010).

[50] Robert M. Gates "The National Defense Strategy: Striking the Right Balance," *Joint Force Quarterly* (1st Quarter 2009), 2–7; Leon Panetta, Remarks at the Woodrow Wilson Center, Washington, DC, October 11, 2011, available at <at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4903>.

[51] General James T. Conway, USMC, Admiral Gary Roughead, USN and Admiral Thad W. Allen, USCG, *A Cooperative Strategy For Maritime Security*, Washington, DC, October 2007; James Conway, *Marine Corps Vision and Strategy 2025*, Washington DC: Headquarters, U.S. Marine Corps, June 2008; General Martin Dempsey, "Versatility as an Institutional Imperative," *Small Wars Journal*, March 10, 2009; General James Amos, USMC, *Commandant's Planning Guidance*, November 2010; Raymond T. Odierno, "The U.S. Army in a Time of Transition," *Foreign Affairs*, May/June 2012, 10.

[52] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, DC: Director of National Intelligence, April 2012), 65.

[53] NATO Multiple Futures Report, (Norfolk, VA: Allied Command Transformation, 2007).

[54] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 14, 58.

[55] Anders Fogh Rasmussen quoted in Mark Landler and Michael Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine," *The New York Times*, July 8, 2014.

[56] Quoted in Matt Mathews, *We Were Caught Unprepared, the 2006 Hezbollah-Israeli War*, Ft. Leavenworth, KS: Combat Studies Institute Press, 2008.

[57] Dima Adamsky, "Russia's Intervention in Syria—Strategic Implications and Warfare Lessons." *Ma'arakhot*, November 1, 2016.

[58]Andrew Mumford "Proxy Warfare and the Future of Conflict," *The RUSI Journal*, Vol. 158, no. 2 (2013), 40–46, published online April 28, 2013.

[59] David E. Johnson, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica, CA: RAND Corporation, 2011), 148–149, available <http://www.rand.org/content/dam/rand/pubs/monographs/2011/RAND_MG1085.sum.pdf>; David E. Johnson, "An Overview of Land Warfare" in Dakota Wood, ed., *2018 Index of U.S. Military Strength*, Washington, DC: Heritage Foundation, October 2017.

[60] Anders Fogh Rasmussen quoted in Mark Landler and Michael Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine," *The New York Times*, July 8, 2014, A1.

[61] Sam Jones, "Ukraine: Russia's new art of war," *FT.Com*, August 28, 2014, accessed at <http://www.ft.com/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html#ixzz3O01r9qjy>; Yuri Drazdow "Modern hybrid war, by Russia's rules," *Minsk Herald*, Nov. 3, 2014, available at <http://minskherald.com/2014/11/russian-new-military-doctrine/>.

[62] "What Russia Wants: From Cold War to Hot War," *Economist*, Feb. 14, 2015, available at <http://www.economist.com/news/briefing/21643220-russias-aggression-ukraine-part-broader-and-more-dangerous-confrontation>.

[63] Ben Connable, Jason H. Campbell, and Dan Madden, *Stretching and Exploiting Thresholds for High-Order War* (Santa Monica, CA: RAND, 2016).

[64] *Strategic Survey 2014, The Annual Review of World Affairs*, London: Institute for International Strategic Studies, 2014, 53–64; "Hybrid Warfare: Challenge and Response," *Military Balance*, London: Institute for International Strategic Studies, 2015, 17–20.

[65] Mazarr, "Mastering the Gray Zone, 44–46;

Michael Kofman and Matthew Rojansky. "A Closer Look at Russia's Hybrid War," *Kennan Cable No. 7*, Washington, DC: Woodrow Wilson Center, April, 2015.

[66] Wales NATO Summit Communique, North Atlantic Treaty Organization, September 4, 2014, accessed at <http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en>.

[67] For analysis drawn from field research and direct observations, see Dr. Philip A. Karber, "Lessons Learned from the Russo-Ukrainian War," paper delivered at the Historical Lessons Learned Workshop conducted at Johns Hopkins Applied Physics Laboratory, July 2015. UN statistics cited available at <http://euromaidanpress.com/2016/09/21/real-human-costs-of-russian-aggression-in-ukraine-still-uncounted-un-says/>.

[68] Phillip A. Karber, "Russian Style Hybrid Warfare," McLean, VA: The Potomac Foundation, 2015.

[69] Vladimir Peshkov, "The Donbas: Back in the USSR," European Council on Foreign Relations, 2014. Valentin Torba,"The great tragedy of little Luhansk," European Council on Foreign Relations, January 15, 2016, available at <http://www.ecfr.eu/article/commentary_the_great_tragedy_of_little_luhansk>. In Ukraine, the net effect of the criminal activity is to control the population through access to food.

[70] Wes Clark and Jack Keane, "Ukraine's Hybrid War," *The Washington Times*, March 6, 2018.

[71] Michael Kofman, et al in *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND 2017), 77.

[72] Oscar Jonsson and Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal after Ukraine," Vol. 28, *Journal of Slavic Military Studies*, 2015.

[73] Ofer Fridman, *Russian 'Hybrid' Warfare*, London: Hurst, 2018 (forthcoming).

[74] Guillaume Lasconjarias and Jeffrey A. Larsen, eds. *NATO's Response to Hybrid Threats* (Rome: NATO Defense College, 2015). For a superb assessment, see András Rácz, "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist," *FIIA Report* 43 (Helsinki, Finland: The Finnish Institute of International Affairs, 2015).

[75] For an excellent look at Russian-based organized crime see Mark Galeotti, "CRIMINTERN: How the Kremlin Uses Russia's Criminal Networks in Europe," *Policy Brief*, European Council on Foreign Relations, London, April 2017. See also the insights by Claire Bigg, "Vostok Battalion, A Powerful New Player in Eastern Ukraine," Radio Free Europe/Radio Liberty, October 27, 2015. Accessed at <http://www.rferl.org/content/vostok-battalion-a-powerful-new-player-in-easternukraine/25404785.html>.

[76] Hilary Matfess and Michael Miklaucic, eds., *Beyond Convergence: World Without Order*, (Washington, DC: National Defense University, Center for Complex Operations, 2016).

[77] Brig. Gen. Muni Katz, IDF and Nadav Pollak, "Hezbollah's Russian Military Education in Syria," Washington, DC: Washington Institute, *Policy Watch 2541*, December 24, 2015; Barbara Opall-Rome, "Russian Influence on Hezbollah Raises Red Flag in Israel, *Defense News*, November 6, 2016, available at <https://www.defensenews.com/global/mideast-africa/2016/11/07/russian-influence-on-hezbollah-raises-red-flag-in-israel/>.

[78] Carl von Clausewitz, *On War*, Peter Paret and Michael Howard, eds. and trans. (Princeton, NJ: Princeton University Press, 1986), 88–89.

[79] H. R. McMaster, "Change and Continuity, The Army Operating Concept and Clear Thinking About Future War," *Military Review* (March/April, 2015), 6–18.

[80] Elizabeth Young, "Decade of War: Enduring Lessons from a Decade of Operations," Vol. 4, no. 2, *PRISM*, 2015, 126–27.

[81] James N. Mattis, *Synopsis of the National Defense Strategy, Sharpening the U.S. Military's Competitive Edge*, Washington, DC: Department of Defense, January 2018.

[82] "The paradox of war is that an enemy will attack a perceived weakness, so we cannot adopt a single preclusive form of warfare." James N. Mattis, transcript, Roll Out Speech for National Defense Strategy, School of Advanced International Studies, Johns Hopkins University, Washington, DC, January 19, 2018.

[83] Joint Chiefs of Staff, *Joint Operations*, (Washington, DC: Joint Staff, August 11, 2011), I-5.

[84] Alan Dupont, *Full-Spectrum Defense: Re-thinking the Fundamentals of Australian Defense Strategy* (Sidney, Australia: Lowy Institute, March 2015), available at <http://www.lowyinstitute.org/publications/full-spectrum-defence-re-thinking-fundamentals-australian-defence-strategy>.

[85] Nathan Freier, et al, *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: Army War College, Strategic Studies Institute, May 2016).

[86] Linton Wells, "Cognitive-Emotional Conflict, Adversary Will and Social Resilience," Vol. 7, no. 2, *PRISM*, 2017, 4–17.

[87] For ideas on countering coercive activities by China in Asia, see Patrick Cronin and Andrew Sullivan, *Preserving the Rules: Countering Coercion in Maritime Asia* (Washington, DC: Center for a New American Century, March 2015). US. Army Special Operations Command, "Counter-Unconventional Warfare," White Paper, Fort Bragg, NC, September 26, 2014. See also Joseph L Votel, Charles, T. Cleveland, Charles T. Connett, and Will Irwin, "Unconventional Warfare in the Gray Zone," *Joint Force*

Quarterly, Issue 80 (1st Quarter 2016), 101–110.

[88] Dickey et al, 256.

[89] As noted in a claim by the U.S. Government, available at <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.

[90] The various uses of some terminology is evident in the literature, for example see Robert Johnson, "Hybrid Warfare and its Countermeasures, A Critique of the Literature," *Small Wars and Insurgencies*, Vol. 29, no. 1 (2018), 141–163.

[91] See the valuable insights of David Ucko and Thomas Marks, "Violence in Context: Mapping the Strategies and Operational Art of Irregular Warfare," *Contemporary Security Policy*, Vol. 39, no. 2 (2018), 206–233.

[92] Ibid, 224.

[93] For an excellent example see Timothy L. Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* (July/August, 2017), 34–40.

[94] Robert R. Bowie and Richard H. Immerman, *Waging Peace: How Eisenhower Shaped an Enduring Cold War Strategy* (New York: Oxford University Press, 1998). On the Eisenhower era see James M. Ludes, *A Consistency of Purpose: Political Warfare and the National Security Strategy of the Eisenhower Administration*, Ph.D dissertation, Georgetown University, 2003. See also Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* (Washington, DC: NDU Press, June 2012).

[95] David Ellis, Charles Black and Mary Ann Nobles, "Thinking Dangerously, Imagining SOCOM in the Post-CT World," Vol. 6, no. 3, *PRISM*, 2016, 110–29.

[96] For a recent assessment of how the United States might adapt better see Linda Robinson et al *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018). For ideas on how the United States should begin to conceive of more comprehensive campaigning below the threshold of conventional war, see Joint Concept, Integrated Campaigning (Washington, DC: U.S. Joint Chiefs of Staff (J7) 2018).

[97] For key lessons about the need for and types of organizational innovation used recently see Christopher Fussell and D. W. Lee, "Networks at War: Organizational Innovation and Adaptation in the 21st Century," in Hilary Matfess and Michael Miklaucic, eds., *Beyond Convergence: World Without Order* (Washington, DC: National Defense University, Center for Complex Operations, 2016).

[98] Brian McAllister Linn, "The U.S. Armed Forces' View of War," Vol. 140, no. 3, *Daedalus* (Summer 2011), 34.