UNITED STATES ARMY SPECIAL OPERATIONS COMMAND

25TH ANNIVERSARY

1989 - 2014

SINE PARI

Counter-Unconventional Warfare

White Paper

26 September 2014

Contents

Chapter 1
Introduction

Seizing the Unconventional Initiative to Counter Hybrid Threats

During the last decade, the U.S. military, along with its interagency and international partners, has generated significant capability to counter the irregular threats presented by non-state terrorists, insurgents, and criminal groups. During these same years, a distinct challenge to America and its partners in NATO and beyond has arisen through an innovative mix of such irregular threats. This challenge is Hybrid Warfare combining conventional, irregular, and asymmetric means, to include the persistent manipulation of political and ideological conflict. Foreshadowed by Iranian actions throughout the Middle East and by Chinese "unrestricted warfare" strategists in the 1990s, Hybrid Warfare has now reached its most brazen form in Russia's support for separatist insurgents in Ukraine.

Hybrid Warfare involves a state or state-like actor's use of all available diplomatic, informational, military, and economic means to destabilize an adversary. Whole-of-government by nature, Hybrid Warfare as seen in the Russian and Iranian cases places a particular premium on unconventional warfare (UW). As such, a response capitalizing on America's own irregular and unconventional warfare skills, as part of a whole-of-government and multinational strategy, can best counter actions of emergent adversaries to destabilize global security. Counter-Unconventional Warfare (C-UW) should thus prove central to U.S./NATO security policy and practice over the next several decades.

The Geopolitical Context: From Resurgent UW to Counter-UW

C-UW is a relatively new term coined by veterans of global special operations, who have combined a keen grasp of emerging challenges to international security with lessons learned from our struggle against violent extremism from rising states and non-state actors. C-UW begins with an understanding of unconventional warfare (UW) itself, defined in Joint doctrine as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[1] Central to Irregular Warfare (IW), UW involves external parties aiding indigenous actors against governments. Such aid can involve training, organizing, recruiting, operational advising, coordinated diplomatic support, and even use of kinetic action and logistical support to increase the advantage of indigenous insurgents or rebels.

Over the past decade, both states and non-state actors in Iraq, Syria, Afghanistan, Georgia, and other areas have conducted this kind of UW to coerce, disrupt, and overthrow established governments. Novel forms of UW persist even to the present moment. Among non-state actors, Sunni Jihadi extremists claiming a boundless “Islamic State”[2] now seek to overthrow national governments, local administrations, and social-political structures in a wide swathe from eastern Syria to northwestern Iraq, replacing them with a Muslim Caliphate across the region.

Among state actors and on the very frontiers of NATO, Russia’s actions in Ukraine embrace UW fully. Russia currently employs special operations forces, intelligence agents, political provocateurs, and media representatives, as well as transnational criminal elements in eastern and southern Ukraine. Funded by the Kremlin and operating with differing degrees of deniability or even acknowledgement, the Russian government uses “little green men” for classic UW objectives. These objectives include causing chaos and disrupting civil order, while seeking to provoke excessive responses by the state’s security organs—thus delegitimizing the Kiev government. Additionally, Russian elements have organized pro-Russian separatists, filling out their ranks with advisors and fighters. Russia’s UW has also included funding, arming, tactical coordination, and fire support for separatist operations.[3] While enabling a frequency of tactical success against Ukrainian forces putting the latter at a distinct strategic disadvantage, insurgency aided by Russian UW has gained local supporters, while intimidating dissenters into acquiescing to a separation from the government in Kiev.[4]

Russian UW is thus the central, most game-changing component of a Hybrid Warfare effort involving conventional forces, economic intimidation of regional countries, influence operations, force-posturing all along NATO borders, and diplomatic intervention. Sponsorship of separatist insurgency in Ukraine accords well with current Russian military doctrine and strategy, which embrace “asymmetrical actions… [including] special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state.”[5]

While the “Islamic State” crisis demonstrates just how cascadingly disruptive non-state UW can be, the brazen audacity of UW within Russian Hybrid Warfare has produced urgent concern among America’s NATO and non-NATO partners that Russia may apply similar approaches to other regional countries in the region with dissenting Russophile populations, such as the Baltic States, Moldova, and Georgia (Refer to Appendix B for more details on Russian doctrine).

Together, examples of state- and non-state-sponsored UW over the past decade have highlighted the requirement for C-UW expertise to meet the challenges of insurgency, Hybrid Warfare, and the shocks to international security these produce. Among the concept’s chief advocates, retired Special Forces COL David Maxwell describes counter-unconventional warfare as “operations and activities conducted by the U.S. Government and supported by SOF [special operations forces] against an adversarial state or non-state sponsor of unconventional warfare.” These SOF-supported government initiatives can “decrease the sponsor’s capacity to employ unconventional warfare to achieve strategic aims.” As C-UW campaigns are likely “protracted and psychological-centric in nature” they should “comprehensively employ political, economic, military, and psychological pressure” in order to degrade both the will and capability of an adversary to sponsor unconventional warfare.[6] The chief advantage of C-UW is thus its focus on decreasing an adversary's ability and will to persist in Hybrid Warfare or to support elements of a resistance or insurgency.[7]

Given its "comprehensive" nature, effective C-UW calls for an adaptive, holistic U.S. Government approach embracing local partners. Successful C-UW will thus emerge from dedicated policies; strategies informed by a thorough grasp of UW itself; and operations implemented patiently through regional and global networks of Joint, Interagency, Intergovernmental, and Multinational (JIIM) partners.

Though not a traditional focus of the U.S., meeting the C-UW challenge is by no means beyond our capability. The past twelve years demonstrated the ability of the Joint Force, and SOF in particular, to adapt. During this time, our superiority in traditional warfare[8] was evident during Operation Iraqi Freedom where U.S. and coalition conventional forces supported by SOF quickly overwhelmed Iraqi forces, defeating them at every turn. When extended conflict in Afghanistan and Iraq revealed a systemic U.S. deficiency in counterinsurgency (COIN) operations, senior leaders initiated the development of a new Field Manual (FM) 3-24 Counterinsurgency in 2006. This was accompanied by the subsequent U.S. Government Counterinsurgency Guide to provide interagency decision makers a broad framework and practical guidelines for a whole-of-government approach to COIN.[9] Learning from Afghanistan, Iraq, and global counterterror operations has thus driven adaptation and improvement in COIN as well as certain core activities of irregular warfare (IW),[10] including counterterrorism (CT) and stability operations (SO).

These capabilities gained by the Joint Force and broader U.S. government in COIN, CT, stability operations, and security sector assistance are remarkable. Yet, by themselves, these advances are not able meet the challenge of Russian conduct of UW in Ukraine. Though the U.S. government is able to help partners to contain domestic challenges to state sovereignty, the joint and interagency community has yet to present a credible strategic-level ability to interdict and roll back external sponsorship of insurgent and separatist movements. Yet, similar to Iranian support of Shiite militias in Lebanon and Iraq, the current challenge of Russian involvement in Ukraine demonstrates that it is this external sponsorship—UW by another name—which frequently provides the foundational motivation, resources, and support to elements destabilizing international security in regions of particular concern to the U.S.

When executed a part of a broader Hybrid Warfare campaign as is the case for Russia in Ukraine, UW will continue to frustrate the attainment of U.S. national security goals as long as we lack a C-UW approach linking policy, strategy, and operational implementation. Conversely, once possessed of a credible C-UW capability, the U.S. and its JIIM partners will be well-positioned to attrit and defeat those insurgent, separatist, and terrorist movements which rely on external support.[11]

Any conceptual framework for C-UW must therefore embrace a whole-of-government approach. This whole-of-government approach must bring focused capabilities to bear by employing diplomatic, informational, economic, financial, and legal instruments of national power alongside military instruments optimized for hybrid and irregular warfare. These instruments must function in coordinated synergy, in order to undermine the will of adversaries who sponsor resistance movements against American allies and partners. Through developing a coordinated, synergistic whole of government C-UW strategy, the organs of American government will provide our national leadership with a range of viable policy options to meet the challenges of the future operating environment.

Chapter 2
Future Operating Environment

Over the next several decades, U.S. national security practitioners are likely to confront persistent global instability. Emerging from dynamics visible today, the future operating environment (FOE) will feature an increasing role for non-state actors; the diffusion of power manifested in a multipolar world; demographic shifts including accelerated urbanization; and increasingly adversarial competition for global resources. The spread of rapidly advancing information and weapons technologies will further enable this diffusion of power and adversarial competition, involving frequently changing combinations of state and non-state actors.[12]

As such, while the two-century-old trend of increasing irregular conflict will likely continue,[13] the threat of major state-on-state confrontation will endure. The U.S. Armed Forces must therefore further develop both its traditional and irregular warfare capabilities. As unconventional warfare (UW) will likely feature prominently in both forms of conflict, U.S. national security strategy must come to embrace Counter-UW, prosecuted against state and non-state adversaries.

Diffusion of Global Power. The U.S. National Intelligence Council (NIC) currently projects a much greater diffusion of global power in the near future, with the resultant multipolarity driving geopolitical instability. According to the NIC, "by 2030, no country—whether the U.S., China, or any other large country—will be a hegemonic power."[14] Rising regional states such as China, Russia, India, Brazil, Indonesia, Turkey and Iran will assert growing power and influence regionally and globally to secure their political, social, or economic interests. The U.S. national leadership will thus employ the elements of national power in an international environment where alliances change more frequently and adversarial relationships are more common than in the past.

Increased Prominence for Non-State Actors. The diffusion of global power will also manifest itself as an increasing role of non-state actors seeking greater influence from the local-to-global level. The rapid spread of ever-improving weapons and information technology will prove an enabler in this respect: "individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence—a capability formerly the monopoly of states."[15] Violent extremists

Russia's campaign in Ukraine today is a prominent example of hybrid warfare. In the previous decade, however, during the 2008 Russia-Georgia conflict in the breakaway regions of Abkhazia and South Ossetia, both sides used combinations of regular forces, irregular forces, and criminal elements. Prior to the war, Russian military forces operating in Georgia as "peacekeepers" sustained a flourishing smuggling network in partnership with various Abkhaz, Ossetian, and Georgian criminal groups. Alongside Russian forces, this smuggling network moved into Georgia, while cooperating with separatist militias used by Russian forces to ethnically cleanse Georgians from the two breakaway regions. Similarly, Georgian military forces cooperated with guerillas operating in the area. Both sides thereby blurred the distinction between regular government forces, criminal elements, and militias.

as well as criminal organizations will to use these tools with little restraint in order to achieve their desired effects. Indeed, the cyber domain in particular will permit small groups and individuals to achieve truly disproportionate effects.

Hybrid Threats. For at least the past half-decade, Joint Force strategists have advocated for greater attention to hybrid threats emerging from states and other actors.[16] These hybrid threats constitute a diverse array of options through which America's adversaries will confront us and our global partners. Among the most pressing challenges to global security, future adversaries will employ proxies, while activating surrogates including terrorist and criminal networks. Iran, for example, employs an array of very capable proxy forces to extend and solidify its influence abroad, to include Hezbollah in Lebanon, Hamas in Gaza, and various groups in Afghanistan, Yemen, Iraq, and the Caucasus.[17]   Additionally, as Russia has amply shown in the Baltics, Central and Southern Europe, as well as in Central Asia, states will manipulate access to energy resources and markets, exploiting perceived economic and diplomatic leverage to disrupt the freedom and stability sought by the U.S. and her allies. Likewise, non-state actors such as Hezbollah, Hamas, and other violent groups will leverage operational concepts and high-end capabilities traditionally associated with state actors.

While the Joint Force must prepare for protracted conflict with increasingly powerful non-state actors, we must also counter state adversaries who use modern military technologies as well as proxies and surrogates,[18]   Difficult to detect in a timely fashion via conventional methods, countering these hybrid threats will place a premium on broad-based intelligence efforts, rapid, coordinated innovation and adaptation, and a commitment to undermining the means and will of adversaries to persist in conduct inimical to U.S. and allied interests.

Chapter 3
From the UW Challenge of Hybrid Warfare to a Comprehensive C-UW Strategy

Given the centrality of foreign support to historical insurgences and the prominence of UW in hybrid warfare, the U.S. military must furnish national security leaders with a strategy and capability appropriate to countering our adversaries' UW efforts—anywhere in the world. In short, the Joint Force must generate the ability to design, plan, and execute a comprehensive C-UW approach, thereby providing our elected leaders with successful policy options for the future operating environment.

The Basic Idea and Core Elements

To prove successful, C-UW must be strategic in conception and scope. It therefore must encompass the whole-of-government while employing the full range of synchronized IW functions in order to defeat an adversary's unconventional warfare activities. Whole-of-government C-UW through synchronized IW must also persistently integrate joint, interagency, intergovernmental, and multinational (JIIM) partner efforts.

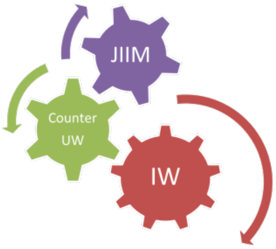

Figure 3-1. Counter-UW Synchronization. *Counter UW synchronizes the effects of IW and our JIIM partners.*

Of course, at the core of the whole-of-government approach is cooperation among the various military and civilian organizations representing national power—and that is likely to present the most formidable challenge to attaining a credible C-UW capability. Parochial organizational interests tend to prevail unless national leadership enforces mutual cooperation. Yet, America has achieved whole-of-government national security collaboration in the past even outside a major war, including George Kennan's 1940s strategy to contain and defeat Communism (discussed below). More recently, effective coordination and cooperation among military and civilian agencies emerged after the 9/11 attacks. As part of the overall global war on terror (GWOT) strategy, the U.S. has fought terrorist organizations through economic and financial channels to identify and cut off their funding; through diplomatic means to isolate and punish state sponsorship; through refocused intelligence methods to identify leadership and infrastructure; and through surgical military strikes to eliminate leaders and operatives.[19]

To capitalize on these recent gains, U.S. leaders need to ensure a coordinated whole-of-government effort to facilitate successes in C-UW at a level equivalent to the success enjoyed in America's global CT operations. Successful C-UW is not, however, merely successful CT rebranded. While CT activities tend toward short-term operations which are reactive in nature, successful C-UW is both proactive and protracted, requiring patience to plan, execute, and coordinate activities. Likewise, where metrics were often relatively easy to find in CT operations (e.g., the terrorist leader was captured or killed), C-UW will struggle with the dilemma of reporting success in negative terms—such as the number of regions not under insurgent control compared to regions that would be dominated by insurgents if C-UW activities had not been conducted. Though the difficulty in measuring success typically makes it hard for U.S. leaders to persist in protracted undertakings, they and the American people were able to do so for over forty years while spearheading and international alliance during the Cold War.

An initial step towards enabling proactive and protracted C-UW as a national security policy option is to develop a framework providing a common lexicon, thought process, communications procedures, and operational guidance for SOF and JIIM partners.[20] With this framework and processes, the Joint Force will employ scalable IW mission command structures that integrate JIIM and other partners into the planning and coordinated execution of C-UW campaigns anywhere in the world, to include across Geographical Combatant Command (GCC) lines. Likewise, in order to plan and execute effective C-UW campaigns, IW mission command structures require tools and methodologies optimized for analyzing the "human domain," so critical to C-UW success.[21] In this fashion, C-UW will unify the required constellation of SOF and JIIM partners in a strategy to achieve regional and global effects.

In the C-UW context, IW's operations and activities are integral to a holistic approach reducing the effectiveness and will behind an adversary's sponsorship of armed elements among neighbors. This is evident in Table 3-1, which describes the five IW operations and activities in terms of primary actors and the U.S. contribution.

Description	Prime Mover	U.S. Role	Footprint	Low Signature
Unconventional Warfare	Insurgent	Advisory	Small	Yes
Foreign Internal Defense	HN Government	Advisory with the exception of "Armed FID"[22]	Small to Very Large	Possibly

Counterinsurgency	U.S. Government	Support to HN Government countering an insurgency	Large to Very Large	No
Stability Operations	HN Government	Stabilize an unstable HN Government	Small to Very Large	No
Counterterrorism	U.S. Government or HN Government	Disrupt clandestine networks which employ terror as a tactic	Small	Yes

Table 3-1. The Operations and Activities of IW—A Comparison

The pillars of IW are also interrelated. During Operation Iraqi Freedom, for example, SOF enabled the Kurdish Peshmerga resistance to liberate large areas of Northern Iraq in a classic UW operation. Later, as a new Iraqi government began to emerge, the U.S. fought a bitter and protracted COIN campaign. After the new Iraqi Government became a reality, the U.S. engaged in an SO campaign, restoring infrastructure, training the Iraqi government and military while battling insurgents. Finally, in 2012 U.S. forces transitioned to Foreign Internal Defense (FID) in a purely advisory capacity. This interrelationship among IW activities amounts can energize C-UW holism.

C-UW's Critical Components and Supporting Concepts

An effective C-UW strategy features certain critical components and supporting concepts. At base, C-UW practitioners must understand the UW approaches of the adversary itself. Next they must assess current organizational structures to ensure appropriate capabilities are dedicated to countering adversary actions the right capacity and capability. Finally, those responsible for conducting C-UW must seek adequate capacity and resources for these dedicated capabilities at the strategic, operational, and tactical levels.

Additionally, integrating allies and other partners for C-UW success requires a global network, as well as CONUS-based elements operationalized to support mission execution. Finally, the high likelihood of operations in politically sensitive, hostile, and denied environments necessitates comprehensive assessments of current authorities and permissions across the range of military operations to ensure long-term C-UW campaigns are not hampered by legal gaps.

Develop Strategies and Policies. We have seen that the future operating environment will feature state competition for regional and global influence, frequently in the form of ideological battles in the human domain. Russia, China, and Iran currently conduct political warfare activities to further their individual goals. By contrast, the U.S. has "gotten out of the habit of waging political warfare since the end of the Cold War" focusing instead on "public diplomacy aimed at 'telling America's story.'"[23] C-UW should thus be scoped as a strategy enabling the U.S. to influence local struggles in a positive direction, and policies should be developed assigning political warfare as a core mission of government agencies responsible for C-UW doctrines and capabilities.[24] Several synergistic initiatives serve this goal:

> *Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP [the Marshall Plan]), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.*
>
> George Kennan
> "Policy Planning Memorandum," May 4, 1948

1) Establish Political Warfare Strategies. George Kennan's definition of political warfare emphasizes both overt and covert activities "short of war." There are many such activities applicable to countering adversary strategies. The following comprises a sampling:

- Economic sanctions against countries, groups, and individuals, as well as coercive trade policies
- Diplomacy, including boycotting international events, establishing treaties or alliances to counter adversary UW, severing diplomatic relations, or excluding offending states from membership in international forums
- Support for "friendly" insurgent groups to coerce, disrupt, or overthrow an adversary regime,
- Support for friendly governments to counter adversary political warfare activities,
- Support for foreign political actors and parties opposing adversarial regimes
- Strategic communications and information operations to expose adversary activities.

2) Designate a Lead Organization to Coordinate and Synchronize Efforts. Whole-of-government political warfare efforts must have a designated lead organization to coordinate and synchronize planning and execution to achieve unified action. Presidential Policy Directive (PPD) 23 *U.S. Security Sector Assistance Policy* advocates strengthening allies and partner nations to build their own security capacity. To do that, officials must "foster United States Government policy coherence and interagency collaboration." Further,

> Transparency and coordination across the United States Government are needed to integrate security sector assistance into broader strategies, synchronize

> agency efforts, reduce redundancies, minimize assistance-delivery timelines, ensure considerations of the full range of policy and operational equities, improve data collection, measure effectiveness, enhance and sustain the United States Government's security sector assistance knowledge and skills, and identify gaps.[25]

Related to this Directive, the Council on Foreign Relations recommends the current counterterrorism apparatus as a useful example of what might serve for political warfare. It suggests the following key points at the strategic level:

- Assign a political warfare coordinator in the National Security Council (NSC),
- Create a strategic hub—an interagency coordinating body that pulls all of the local efforts together—in the State Department, and
- Create political warfare career tracks in the Department of State (DOS), Department of Defense (DOD), U.S. Agency for International Development (USAID), and the Central Intelligence Agency (CIA).[26]

3) Develop Political Warfare and C-UW Strategies Nested across Multiple Echelons. Political warfare and C-UW strategies and policies must be planned, coordinated, and synchronized from the strategic national level down to the tactical level. Kennan is again suggestive in this regard. At the strategic level, he recommended a covert political warfare operations directorate or board under the NSC Secretariat, with the director designated by and responsible to the Secretary of State. In this approach, the directorate's staff would be divided equally between State Department and Defense Department representatives selected by the Secretaries, and the directorate would have complete authority over covert political warfare operations.[27]

Taking an approach inspired by Kennan's suggestions, an NSC director for political warfare or C-UW activities should oversee development of policies and directives; prioritize efforts and manage interagency concerns; coordinate activities and funding across the government; and provide oversight for the implementation of Presidential Policies or Directives. The Department of State would be the lead for political warfare and C-UW activities, with other Departments and Agencies in a supporting role.

Given State Department leadership in C-UW, in appropriate countries, The U.S. Country Team, , should be the focal point to plan, coordinate, and synchronize political warfare and C-UW activities. Led by the Ambassador, The Country Team will develop specific country plans and strategies for U.S unilateral activities, integrating host nation activities to obtain mutual objectives.

The National Security Council system would then ensure the coordination and synchronization of strategic political warfare and C-UW policies and directives among theater and operational level organizations. In turn, the Geographical Combatant Command would coordinate and synchronize political warfare and C-UW activities within a region. This would occur through the Joint Interagency Coordination Group (JIACG), staffed with DOD personnel and representatives of other Departments and Agencies who collaborate, plan, and synchronize interagency efforts to achieve U.S. objectives.[28] Properly staffed and resourced, the JIACG can be the regional hub for political warfare and C-UW activities. The JIACG construct provides for more effective planning, coordination, and integration of partner efforts to achieve objectives, and features leveraging expertise and capabilities of each participating organization through a reach back capability to Departments and Agencies.[29]

At the lower tactical level of command or task force level, the interagency coordination can be exercised through Liaison Officers (LNOs) dispatched from selected Departments or Agencies for specific mission purposes. Recently, Joint Interagency Task Force West (JIATF West) provided a successful example of JIIM coordination and execution to achieve mutual objectives. Including approximately 166 active duty, reserve, DOD civilian, contractor, and U.S. and foreign law enforcement agency personnel, JIATF West is the U.S. Pacific Command Executive Agent for DOD support to law enforcement for counterdrug and drug-related activities.[30]

4) Leverage SOF Special Warfare and Surgical Strike Capabilities. Within DOD, SOF is a key component of political warfare activities because of their ability to conduct low visibility, low-footprint operations. The United States Special Operations Command (USSOCOM) will plan, coordinate, and synchronize global SOF political warfare supporting campaigns with interagency partners, Geographic Combatant Commands, and Theater Special Operations Commands. The Geographic Combatant Command will design regional campaigns for the military instrument of national power to support political warfare in their respective regions. The Theater Special Operations Command (TSOC) will plan SOF's support to their GCCs theater campaign plan.

ARSOF will be a key supporting component of the TSOC's plan as ARSOF units are manned, trained, and equipped to conduct IW operations and activities to support political warfare objectives. ARSOF's two critical capabilities—special warfare and surgical strike—provide lethal and nonlethal skill sets instrumental to achieving political warfare objectives. ARSOF can provide scalable force packages ranging from single operators, to small teams, to regimental size forces. ARSOF can achieve political warfare objectives by unilaterally executing operations in a covert or clandestine manner, or through and with indigenous personnel in politically sensitive or hostile environments.

Gain the Initiative. Unlike the current counterterrorism apparatus, political warfare and C-UW strategies must be proactive rather than reactive. Strategists must identify trouble areas early in order to pinpoint problems that an adversary could exploit. They must also accurately identify current adversary activities and apply a strategy to address them. The keys to political warfare and C-UW strategies are patience and long-term thinking. The goal is a long-term change in the environment to a state more amenable to U.S. interests.

Develop Hybrid Structures with Regional and Global Focus. Joint forces understand how to establish mission command structures from the Combatant Command down to the tactical level of war. Operation Desert Storm and Operation Iraqi Freedom demonstrated the effectiveness of U.S. mission command structures in executing traditional warfare—state versus state military operations. The transition from traditional to irregular warfare activities in Operation Iraqi Freedom—due in no small part to Iranian proxy efforts in Iraq[31]— spotlighted significant challenges to the ability of traditional warfare command structures to synchronize objectives in a JIIM environment. Both in Iraq and Afghanistan, a lack of unity of effort between conventional and special operations forces characterized the operational and tactical levels.[32] This suggests the need for a joint force mission command structure specifically designed to plan and execute IW campaigns and C-UW operations.

A C-UW-optimized IW mission command structure should be hybrid in nature, led by a SOF or conventional commander. It should also include SOF, CF, and other partners based on the capabilities required to execute the C-UW campaign. The headquarters component should also be hybrid, as well as flexible and scalable from small elements up to a large Joint Task Force (JTF), adapting both to the scope of the effort and to partner capabilities. Hybrid structured headquarters must manage transitions of staff personnel as the command adds or subtracts JIIM partners for the campaign.

Thus structured, hybrid mission command allows the right capabilities and expertise to come together for effective application to a problem, enabled by a common operating picture generated through interoperable communications and information management. The seamless integration of all partners is critical to a successful IW campaign. In particular, countering adversary UW activities requires expertise across the U.S. government and partners to achieve objectives by shortening planning and execution timelines, reducing time needed to access effects and feedback, and increasing the speed to adjust plans and actions to meet new objectives.

As such, a Hybrid IW headquarters conducting C-UW must establish communication and information sharing mechanisms. Since not all partners need to share equally in all information, Foreign Disclosure Officers will need to determine the substance and procedures for information sharing with multinational partners. Likewise, the headquarters must develop techniques and procedures to communicate with and control proxies or surrogates supporting the campaign.

SOF is a logical choice to form the core of a hybrid-structured headquarters to counter IW threats. The unique special warfare and surgical strike capabilities resident in United States Army Special Operations Forces (ARSOF) encompass IW activities. Additionally, ARSOF possess unique expertise in the human domain, FID, UW, and the practical mechanics of working through and with indigenous partners. Further, ARSOF operators have cultivated an intimate understanding of the interagency. ARSOF can also deploy scalable mission command elements capable of providing the core for a hybrid structured headquarters.[33]

This kind of headquarters may need to integrate and synchronize a C-UW campaign that crosses GCC boundaries. For example, countering Russia's UW activities might entail global C-UW activities across the European, Central and Pacific Combatant Commands. This kind of C-UW necessitates maintaining both a regional and global focus. As scalable headquarters well suited for mission command of IW campaigns, a Special Operations Task Force (SOTF) or Special Operations Joint Task Force (SOJTF) would be able to maintain such a focus due to streamlined command and control relationships with theater-level commands.

Facilitate a JIIM C-UW Complexion. As the above discussion of C-UW mission command hybridity implies, the U.S. must maintain current partner relationships and expand the pool of global partners. Partners can provide information and intelligence, financial support, forces, and sustainment support for C-UW operations. To benefit from such advantages, the U.S. must embrace a long-term approach optimized for building both the capabilities and capacity of partners while simultaneously aiding the preservation of the latters' stability. Additionally, any U.S. C-UW force must recognize that solving any problem in a JIIM environment requires patience, flexibility, and adaptability to reconcile various partners' differing goals, objectives, and methods.

***Counter-Organize to Defeat the Adversary UW Campaign*.** Effective C-UW campaigns require an understanding of how the adversary organizes and operates across the strategic-to-tactical continuum. SOF must understand the adversary's UW organizational structure and counter-organize to defeat it. A full understanding of how the adversary recruits, and how it establishes intelligence, transportation, logistical, and propaganda cells and guerilla forces helps to develop indicators and templates for determining potential areas that may be used as future sanctuaries. Furthermore, understanding adversary UW methods allows a C-UW organization to determine whether it possesses the right capabilities and capacity itself—and whether it is organized appropriately—to overcome the adversary. In this regard, identifying gaps is integral to developing the means to defeat that adversary UW. Improved means could include additional capabilities within current structures, reorganizing current capabilities to optimize efficiency, or programming new capabilities to fill gaps.[34]

> *It seems that rebellion must have an unassailable base, something guarded not merely from attack, but from fear of it.*
>
> T.E. Lawrence

A capabilities-based analysis of this sort should adopt a whole-of-government perspective to ensure Departments and Agencies can support a comprehensive approach to countering adversarial UW activities. The analysis could lead to a restructuring of Departments and Agencies according to the principles of hybrid-type organizations to more effectively apply capabilities to counter adversaries through holistic C-UW.

Improve SOF Operational Art and Campaign Planning. Though current Joint Force methods of planning and decision-making are proven military-centric systems for traditional warfare campaigns and operations,[35] they are ill-suited for planning and executing long-term IW campaigns. SOF planners and doctrine-writers thus need to work with CF counterparts to develop and inculcate a new kind of dedicated IW planning process. The latter should feature a detailed analysis of the human domain, and then drive complex IW operations integrating unified action partners. To accommodate such an IW planning process, the Joint Force will need to refocus operational art and design on IW itself, thereby enhancing the effectiveness of C-UW operations and activities.

Integral to this refocused optional art is influence. Indeed, Kennan's political warfare definition emphasizes psychological warfare and encouraging underground resistance movements in hostile states. Aligned with Kennan's emphasis, ARSOF's Military Information Support Operations (MISO) personnel are trained and equipped to conduct influence operations against a foreign target audience and can support State Department strategic communications plans. Furthermore, ARSOF's Special Forces are skilled at integrating activities with MISO and civil affairs (CA) operations to achieve desired effects particular to working through and with resistance movements in politically sensitive and hostile environments.

In addition to influence, operational art and campaign planning must account for hybrid command structures. Taking advantage of lessons learned from today's joint and interagency task forces, operational art and campaign design can meet the challenges of long-term irregular warfare campaigns. Likewise, best practices learned over the past decade of war should serve as a template to build processes and procedures based on the premise of hybrid mission command, in order to ensure effective planning with reduced friction in an environment with diverse JIIM partners.

Operationalize the CONUS Base. ARSOF's deployable command element[36] possesses regionally expert components to provide continuous, proactive support to forward deployed forces and personnel, in addition to a coordination center leveraging expertise from other government agencies, the private sector, and academia. By establishing mechanisms and leveraging technology, C-UW efforts can further operationalize CONUS-based expertise through the following initiatives:

- The Military Information Support Operations Command Effects Group (MEG) and the Unconventional Warfare Social Theory Academy (UWSTA) provide regional MISO expertise to deployed forces. The MEG integrates and synchronizes long duration, whole-of-government influence efforts, and can enable TSOC/GCC initiatives by pulling forward intellectual, technical and organizational capabilities as part of a broader influence network. The effects group also collaboratively develops innovative solutions to specialized problems at the request of TSOCs and GCCs. The UWSTA conducts research, theory development, testing, and policy formulation for the use of the Internet, social media, and emergent communication technologies and capabilities.[37]

- CONUS-based force packages deployable as tailored Special Warfare Task Forces provide a capability to support national-level influence operations.[38] Special warfare planning teams can be deployed to provide their expertise in support of GCCs, TSOCs, and Country Teams to better integrate special operations capabilities.
- The Civil Military Advisory Group (CMAG) coordinates and leverages civilian U.S. government expertise through a global Civil-Military Operations Center.[39] By leveraging expertise across the government, private sector, and academia, CMAG support includes operational reach back for GCCs, TSOC, Country Teams, and deployed forces; analysis and fusion of country-by-country civil information; and advisory and planning support to Ambassadors and military commanders.

Strengthen Alliances and Coalition Partners to Defeat UW Activities Abroad. Presidential Policy Directive 23 recognizes the need for allies and partners to work collaboratively in order to counter the complex threats to U.S. interests.[40] The collaboration necessary for C-UW will drive the need for long term relationships with our strategic partners. The U.S. should develop strategic agendas for cooperative action with other main centers of global power. In concert with like-minded states and international organizations, the U.S. will be better capable of waging C-UW against state-sponsored and non-state aggressors.

> *… The United States must improve its ability to enable partners in providing security and justice for their own people and responding to common security challenges.*
>
> Presidential Policy Directive 23

The U.S. will seek to maintain current relationships and build new relationships through the Global SOF Network embedded in the broader Global Landpower Network (GLN). The GLN concept envisions a “framework of relationships between governments, organizations, and relevant state and non-state actors, where a geographic or appropriate functional combatant commander can leverage resources to foster partnership creation, build partner capability and capacity, and promote interoperability and alignment. In times of crisis, the network can be leveraged to provide strategic options to U.S. and partner leadership, and increase the speed of a coherent unified response."[41] The development of these enduring global networks will contribute to countering adversary UW proactively.

Trust takes time to develop and cannot be surged in a crisis. To deter or prevent conflict, the U.S. must engage early to develop networked relationships to shape the environment of potential trouble areas. These networks will allow the U.S. to leverage partner capabilities to rapidly employ U.S. and partner assets for global contingency operations. The U.S. can sustain and build such networked relationships through security cooperation activities, security assistance programs, and exchange programs. The resulting partnerships will enable U.S. freedom of action by providing access to forward basing, airspace, sustainment of forces, and partners prepared to employ forces for mutually supporting objectives.[42] The wars in Afghanistan and

Iraq furnish an example of how the U.S. assembled a coalition of forces to achieve mutual security objectives. In this respect, ARSOF's deployable mission command element is specifically organized, manned, trained, and equipped to build partnerships with indigenous elements in politically sensitive and hostile environments by working through the Theater Special Operations Command (TSOC).

Expose and Attack Adversary UW Strategy. In many cases, merely publicizing an ongoing adversary UW campaign can significantly curtail its effectiveness. Enhanced awareness can enable regional partners, coalition governments, and non-governmental agencies to undermine the effectiveness of an adversary UW effort. Exposing adversary UW operations and activities requires a thorough understanding of the environment and of the adversary's UW methodologies. This necessitates a broad range of information and intelligence which Joint and ARSOF preparation of the environment can furnish.[43] To be fully effective, the U.S must fuse intelligence from Joint and ARSOF preparatory activities with insights from JIIM partners.[44] Once the fused intelligence identifies the adversary strategy, the U.S. and JIIM partners can develop plans to attack the strategy augmented by additional international support against the adversary through a strategic communications and information operations campaign that exposes the adversary's activities.

Conduct Remote Area Operations. Remote area operations normally involve the use of host nation (HN) regular, specially trained paramilitary, or irregular forces in insurgent-controlled or contested areas. These forces can establish pockets of popular support for the HN government and to deny support to insurgents.[45] Remote area operations may establish bases in sparsely populated, minority-populated, or unpopulated areas where insurgent forces have staging, training, and rest areas, in addition to logistic facilities or command posts. Such regions may be in the interior of the HN or near border areas where major infiltration routes exist. The precise composition of the forces employed depends on the objective, regional characteristics, local attitudes, political considerations, and the equipment and logistical support available.

Operations in remote areas may include civil military operations, intelligence, population and resources control, and advisory assistance operations.[46] Remote area operations require a mission command structure that thoroughly understands the adversary's strategy and tactics in the context of the local environment; it must also integrate unified action partner tools.

SOF are trained and equipped to support remote area operations to interdict insurgent activity, destroy insurgent base areas in the remote area, and demonstrate that the HN government has not conceded control to the insurgents. They also collect and report information concerning insurgent intentions in more populated areas. In this case, SOF teams advise and assist HN irregular forces operating in a manner similar to the insurgents themselves, but with access to superior combat enablers and sustainment forces.

Leverage Law Enforcement. Law enforcement is a valuable tool to C-UW campaigns. United States law enforcement can support operations oversees to train, advise and assist partner law enforcement elements to identify, disrupt, and defeat underground networks; and to deny sanctuary, resources, mobility, and popular support for threat organizations.[47] Furthermore, U.S. law enforcement agencies can support partner nation law enforcement operations overseas with information regarding local individuals and groups located within the U.S. that have connections to foreign threat groups. Federal law enforcement agencies have long established networks abroad which support such activities. Additionally, these law enforcement networks may provide information that can support U.S. or partner nation military operations. Therefore, to build partner nation law enforcement and capability, the U.S. should include them in all planning processes and consider them as an integral part of a campaign whenever feasible.

Often, partner nation law enforcement will already be engaged in combatting the threat. Therefore, the U.S. government should leverage their capabilities as well as those of other international law enforcement mechanisms to apprehend insurgent leaders and strip legitimacy from the insurgent movement by exposing them as criminal or terrorists. Likewise, working with SOF, local law enforcement can support in-country C-UW operations through an intimate grasp of the local environment, as well as established informant networks. Recognizing that establishing law and order within an area is key to long-term stability, SOF can mentor local law enforcement to the point that the HN military is able to turn security operations over to them.

A thorough understanding of partner nation legal and political constraints must precede operations. To bolster the legitimacy of local governance, the U.S. and partner nations must aggressively but lawfully pursue, prosecute, and interdict subversion, lawlessness, insurgency, terrorism, and other threats. Before establishing C-UW plans, commanders must draw on their legal staff's expertise and the sociopolitical expertise of SF, MISO, and CA personnel as well as the law enforcement expertise of military police. Army legal advisors must review all sensitive aspects of C-UW planning and execution to ensure compliance with U.S. and international law.

As an example of leveraging global law enforcement to increase the legitimacy of local governance, the UN International Criminal Tribunal for the Former Yugoslavia effectively used the international legal system to indict key Serbian political and military leaders for war crimes. This weakened their claims to legitimacy and isolated them in the eyes of the international community.

Gain Intelligence. Intelligence support is vital to counter-UW operations. Because of the covert or clandestine nature of subversion, lawlessness, insurgency, and terrorism, adversary UW elements function as compartmented networks. This compartmentalization frustrates outsiders' understanding of the UW adversary. This challenge is not insurmountable, but it requires the intelligence system employ appropriate tools to collect and process all-source information into actionable user-level intelligence. In particular, C-UW efforts require the collection and analysis of information typically of little interest to conventional forces prosecuting state-on-state warfare. The challenges of intelligence support to C-UW thus require unconventional, critical thinking to counter an adaptive adversary whose strategy is frequently indistinct and unpredictable, based on an asymmetric approach to gain an advantage.

Persistent intelligence fusion is likewise critical to successful C-UW. Though usually ad hoc and beset with many challenges in a JIIM environment, intelligence fusion should be the norm and not an exception for JIIM-augmented headquarters environment, necessitating policies and procedures to fuse intelligence during operations with partners. Likewise, the fusion cell itself must consider how to integrate JIIM partners into the planning process, developing collection plans based on information gaps and all available U.S. and JIIM intelligence assets.

Leverage Authorities and Permissions.   Counter-UW campaigns will require numerous execution authorities across the range of military operations. This may include clarifying or adding to the existing authorities under Titles 10, 22, or 50 of the U.S. Code. All C-UW campaigns feature several statutory responsibilities. Staffs must clearly outline the authorities used for each operation; delineate the lead department or agency; define processes for requesting authorities in the interagency environment; and establish approval levels for actions. An analogous example is cyber operations. The approving authority must clearly outline who has authority to execute operations, what type of operations those designated execution authorities cover, the procedures to request additional authorities, and the level of approval required for actions.

Authorities provided in U.S. Code are not sufficient for individuals or organizations to execute every activity on their own, since specific, case-based permissions may be required to use authorities. An Execution Order from the Secretary of Defense (SECDEF) may authorize activities or rules of engagement but may require permission from the GCC, SECDEF, or President to actually execute the activity in a specific operational setting. For example, a unit may be conducting operations against an adversary unit near an international border when the enemy retreats across the border. The unit has the authority to execute operations in the partner nation but may have to request permission to pursue the enemy across the border or use fire support to engage the targets across the border. Requiring permissions for authorized activities thus provides a measure of control to prevent escalation of a conflict.

The relationship between operational authorities and permissions resembles elements of the budgeting process for the Department of Defense. For example, Congress may pass a National Defense Authorization Act giving the Department the authority to purchase body armor. In the Department of Defense Appropriations Act, however, Congress could restrict the amount of funds as well as the duration of time that can be used to purchase the body armor.

Chapter 4
Counter-UW's Operational Core

Introduction

Five principal IW operations and activities may comprise a comprehensive counter-UW campaign. These include unconventional warfare, foreign internal defense, counterinsurgency, stability operations, and counterterrorism. They may be executed in a single country or simultaneously in multiple countries. While the exact scale and type of operations will be determined by U.S. and partner nation(s) political considerations and objectives, they are scalable, with footprints ranging from individuals, to small groups, or large formations. Notably, C-UW campaigns may be SOF-specific, SOF-centric, or even conventional in nature, depending on the scale of operations and political sensitivities.

Unconventional Warfare (UW)

Unconventional Warfare includes "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow an occupying power or government by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[48] SOF can conduct UW with a small footprint and ideally with a very low signature because the insurgent is the prime mover in UW. However, UW does require SOF to possess a covert or clandestine infrastructure and mechanisms for both security and force protection. Depending upon the applicable title of US Code, the lead agency can be Department of Defense or an Other Government Agency. UW operations can support a C-UW campaign by enabling a resistance movement or insurgency to coerce, disrupt, or overthrow a government or power conducting UW against a U.S. ally.

Foreign Internal Defense (FID)

Foreign Internal Defense entails "participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security."[49] FID operations are instrumental to strengthening partner nations sufficiently so they may counter adversary UW campaigns within their borders. FID operations can be accomplished with a small footprint and a relatively small budget. FID efforts to support a country's internal defense and development programs may involve all instruments of national power—diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL).[50] The Department of State is normally the lead agency for FID operations and the Country Team coordinates and synchronizes interagency activities.

The U.S. effort in El Salvador during the 1980s epitomizes successful small footprint, low-budget FID. Aided by 55 U.S. advisors and the expenditure of no more than $6 billion from 1980 to 1992,[1] the El Salvadorian Government soundly defeated the communist backed Frente Farabundo Martí para la Liberación Nacional (FMLN) insurgents.

Counterinsurgency (COIN)

Counterinsurgency (COIN) is "a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes."[51] COIN operations require a whole-of-government approach to support a host nation's internal defense and development program to enhance governance and security operations to defeat an insurgency. The U.S. must identify potential areas globally that have the potential for insurgent activities in order to develop a comprehensive plan to address the problem of instability in the earlier stages of the movement. The DOS would lead this effort to identify problem areas and integrate other Department and Agency capabilities to identify an emerging insurgency and synchronize efforts addressing the causes of instability.

Stability Operations (SO)

Stability Operations are the "various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief."[52] As such, they allow a C-UW strategy to treat the root causes of instability and insurgency. Employing multiple instruments of national power to build partner nation internal capacity in a preventive mode, stability operations have three important roles in C-UW campaigns: they allow the U.S. to help the partner government to defend itself and maintain stability; they facilitate the transition of responsibility back to the partner nation after the defeat of an insurgency; or they bring stability to areas and peoples affected by natural or manmade disasters. SO may involve rebuilding infrastructure, supporting economic development, establishing the rule of law, building accountable governance, establishing essential services, or building a capable military responsive to civilian authority.[53] The U.S. government with DOS in the lead must coordinate and integrate JIIM partner efforts to achieve long-term stability within a partner nation.

Counterterrorism (CT)

Counterterrorism (CT) entails "actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks."[54] CT is a viable component of a C-UW campaign as it helps to undermine an adversary's power, will, credibility, and legitimacy by influencing the relevant population. CT operations are scalable and can be executed unilaterally or through partners in a covert, clandestine, or low visibility manner. CT operations can build partner CT capacity or can be used to conduct surgical strikes[55] in support of U.S. and allied interests to rapidly and precisely strike high-payoff targets, to rescue hostages, or to retrieve special materiel or items of interest. The U.S. Government lead for CT operations can vary based on the situation.

Chapter 5
Conclusion

Counter-UW describes an over-arching strategy that synchronizes IW and JIIM operations and activities to effectively counter adversary UW campaigns. Historical experience shows that IW has been the predominant form of warfare since 1775.[56] The trends in the NIC allow us to predict that it will continue to be so into the foreseeable future, with UW operations acting as a central component of an overall Hybrid Warfare campaign. The U.S. government lacks a cohesive IW strategy to counter adversary UW campaigns conducted by state and non-state actors, and this has hindered the U.S./NATO response to Russian aggression in Ukraine. The U.S. government must develop a comprehensive framework to plan and execute regional and global IW strategies and operations that counter adversary UW campaigns as part of a whole-of-government approach. This includes policies and procedures to establish roles, responsibilities, and established authorities to conduct IW campaigns to counter adversary UW operations.

Successful regional and global counter-UW campaigns are predicated on a whole-of-government effort enhanced through the coordination and integration of JIIM partners. Such coordination and integration will require persistent engagement to build partner capacity and proficiency, promote sharing of information and development of compatible communications systems to integrate activities and obtain a common operating picture. To develop effective IW campaign plans, the Joint Force must improve IW capabilities and develop operational art based upon effective planning tools which emphasize the human domain. To achieve long term success, the Joint Force must also develop IW mission command structures which are scalable and attuned to political sensitivities on the ground, and they must also integrate JIIM and other partners.

Appendix A
References

Army regulations, DA pamphlets, FMs and DA forms are available at http://www.usapa.army.mil. TRADOC publications and forms are available at http://tradoc.army.mil/tpubs. Joint publications are available at http://www.dtic.mil.

Section I
Required References

Irregular Warfare: Countering Irregular Threats, Joint Operating Concept, Version 2.0

Joint Publication (JP) 1
Doctrine for the Armed Forces of the United States

Section II
Related References

Army Doctrine Publication (ADP) 3-05
Special Operations

Berzins, Janis. “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.” Policy Paper 2. Center for Security and Strategic Research, National Defence Academy of Latvia. April 2014.

Boot, Max, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog. “Political Warfare.” Policy Innovation Memorandum No. 33. Council on Foreign Relations. June 2013. Accessed May 16, 2014. http://www.cfr.org/wars-and-warfare/political-warfare/p30894.

Clarke, Richard and Robert Knake. *Cyber War: The Next Threat To National Security and What To Do About It*. New York, NY: HarperCollins Publishers, 2010.

Department of Defense. “Annual Report on Military Power of Iran.” Executive Summary. April 2012. Accessed August 11, 2014. http://fas.org/man/eprint/dod-iran.pdf.

Department of Defense. “Annual Report on Military Power of Iran.” Executive Summary. January 2014. Accessed August 11, 2014. http://freebeacon.com/wp-content/uploads/2014/07/Iranmilitary.pdf

Department of Defense
Strategy for Homeland Defense and Defense Support of Civil Authorities

Department of Defense. Office of the Secretary of Defense. “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2011.” August 2011, 26. Accessed August 1, 2014. http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf.

Department of Defense. Office of the Secretary of Defense. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012." May 2012. Accessed August 1, 2014. http://www.defense.gov/pubs/pdfs/2012_cmpr_final.pdf.

Field Manual (FM) 3-05.2
Foreign Internal Defense

FM 3-24
Insurgencies and Countering Insurgencies

Gertz, Bill. *The China Threat: How the People's Republic Targets America.* Washington, D.C.: Regnery Publishing, 2000.

Hashim, Ahmed S. "The Evolution of Iran's Military Doctrine." Center for Strategic & International Studies. January 9, 2013. Accessed August 11, 2014. http://csis.org/files/attachments/130109_Summary_Hashim.pdf.

JP 2-01.3
Joint Intelligence Preparation of the Operational Environment

JP 3-0
Joint Operations

JP 3-05
Special Operations

JP 3-07
Stability Operations

JP 3-22
Foreign Internal Defense

JP 3-24
Counterinsurgency

JP 3-26
Counterterrorism

JP 5-0
Joint Operation Planning

Kennan, George. "Policy Planning Memorandum." May 4, 1948. National Archives and Records Administration. RG 273, Records of the National Security Council, NSC 10/2. Accessed June 9, 2014, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

Levitt, Matthew. "Hizballah and the Qods Force in Iran's Shadow War with the West." Policy Focus 123. Washington Institute For Near East Policy. January 2013.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare*. Translated by Foreign Broadcast Information Service. Beijing: PLA Literature and Arts Publishing House, 1999.

National Intelligence Council. *Global Trends 2030: Alternative Worlds*. Washington D.C.: U.S Government Printing Office, December 2012.

"The Military Doctrine of the Russian Federation." Text of report by Russian presidential website 5 February 2010. Carnegie Endowment for Peace. Accessed July 30, 2014, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

Training and Doctrine Command (TRADOC) G-2
Operational Environments to 2028: The Strategic Environment for Unified Land Operations

United States Army Special Operations Command
ARSOF 2022

United States Joint Forces Command
Commander's Handbook for the Joint Interagency Coordination Group

United States Joint Forces Command
Joint Operating Environment 2010

Appendix B
United States Major State Competitors Tactics, Techniques, and Procedures

B-1. Purpose.

The appendix highlights the United States' major nation state competitor's tactics, techniques and procedures. The appendix will present key points of Russian, Chinese, and Iranian doctrine to provide a basic understanding of how these countries conduct operations. A thorough understanding of an adversary's tactics, techniques, and procedures (TTPs) is essential in developing an effective strategy to counter adversary operations and activities.

B-2. Russia.

a. The Soviet previous military doctrine was based on the principle of *maskirovka*. *Maskirovka* is the art of using camouflage, denial, and deception to achieve desired effects. The key features of *maskirovka* are the maintenance of plausible deniability, concealment of forces, disinformation, and the use of decoy or dummy structures to confuse opponents' ability to predict and respond to actions.[57] Russia's New Generation Warfare incorporates many key principles of *maskirovka* by modernizing the principles through the use of new technologies.

b. Russia's current military operations in Ukraine and recent operations in the region provide examples of Russia's New Generation Warfare. Janis Berzins in his *Policy Paper Number Two* analyzed Russia's New Generation Warfare in Ukraine and the implications the new warfare has for Latvian Defense Policy. Berzins points out that Russia's view on modern warfare is "based on the idea that the main battle-space is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy's armed forces personnel and civil population."[58] Russia's new doctrine avoids western states conventional combat capacity to gain an advantage. Russia's Military Doctrine of the Russian Federation 2010 declares that the main external military danger is the North Atlantic Treaty Organization (NATO) moving military infrastructure closer to the borders of the Russian Federation, the attempt to expand membership, and extending the west's span of overmatching force capabilities.[59] Similarly, a main external military danger in the Russian 2010 doctrine is "the deployment (buildup) of troop contingents of foreign states (groups of states) on the territories of states contiguous with the Russian Federation and its allies and also in adjacent waters . . . " The Russian doctrine suggests they will pursue this approach to mitigate perceived encroachment and to expand their sphere of influence in support of national objectives.

c. The Russian New Generation Warfare is outlined into eight phases. Tchekinov and Bogdanov (2013) describe the following eight phases:

- First Phase: non-military asymmetric warfare (encompassing information, moral, psychological, ideology, diplomatic, and economic measures as part of a plan to establish a favorable political, economic, and military setup);
- Second Phase: special operations to mislead political and military leaders by coordinated measures carried out by diplomatic channels, media, and top government and military agencies by leaking false data, orders, directives, and instructions;
- Third Phase: intimidation, deceiving, and bribing government and military officers, with the objective of masking them abandon their service duties;
- Fourth Phase: destabilizing propaganda to increase discontent among the population, boosted by the arrival of Russian bands of militants, escalating subversion;
- Fifth Phase: establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private companies in close cooperation with armed opposition units;
- Sixth Phase: commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions. All types, forms, methods, and forces, including special operations forces, space, radio, radio engineering, electronic, diplomatic, and secret service intelligence, and industrial espionage;
- Seventh Phase: combination of targeted information operation, electronic warfare operations, aerospace operation, continuous airforce harassment, combined with the use of high-precision weapons launched from various platforms (long-range artillery, and weapons based on new physical principles, including microwaves, radiation, non-lethal biological weapons); and
- Eighth Phase: roll over the remaining points of resistance and destroy surviving enemy units by special operations conducted by reconnaissance units to spot which enemy units have survived and transmit their coordinates to the attacker’s missile and artillery units; fire barrages to annihilate the defender’s resisting army units by effective advanced weapons; air-drop operations to surround points of resistance; and territory mopping-up operations by ground troops.[60]

Russia’s New Generation Warfare places an emphasis on influence operations to reduce the requirement of military forces to achieve the objective and set the stage for follow-on military operations.

d. An analysis of Russia’s recent operations and activities in the region can add some context to Russia’s TTPs in implementing its new military doctrine. Stratfor conducted an analysis of Russia’s previous interventions and determined that Russia follows a “rigorous calculus and constraint-based strategy" in each case study.[61] The four case studies were Russian intervention in Lithuania 1990-1991, Moldova 1989-1992, Georgia 1989-1993 and 2008, and Ukraine 2014. The analysis of the case studies has shown some important parallels in each case and the summation of Russian TTPs are the following:

- Conduct detailed planning and preparation prior to major deployment; use exercises to preposition forces for action;
- Use proxies or surrogates for subversive activates and establish conditions for future military operations;
- Employed intelligence operatives to support separatist in Ukraine; recruit, organize, arm, and conduct sabotage and subversion;
- Present actions as operations of independent groups, whose interests merely happen to coincide with those of the Russian government;
- Issues passports to ethnic Russians to claim it is acting in the defense of its citizens authorizing the deployment of forces;
- Supports and stages demonstrations that are pro-Russian; flags and propaganda;
- Supports political leaders sympathetic to Russian interests;
- Employ forces with unmarked uniforms and denying their presence;
- Employed "peacekeepers" in Georgia to counter Georgian forces claiming self-defense;
- In Georgia 2008, employed state sponsored cyber operatives to disrupt Georgian government communications; and
- Apply economic pressure (e.g. threat to cut off gas supplies to Ukraine).[62]

The Russian TTPs extracted from the case studies are consistent with their current military doctrine.

e. The Russian New Generation Warfare and the TTPs extracted from the Stratfor case studies depict the cyber domain is used to create political and military effects. Russia is a major player in cyber warfare conducting espionage, political influence, and supporting conventional military operations. Russia is alleged to have conducted cyber-attacks against Estonia in 2007 and Georgia in 2008. Tensions between Russia and Estonia increased after Estonia declared independence from the former Soviet Union. In February 2007, the Estonia legislature passed a law to remove a Red Army statue leading to riots in April 2007.[63] Estonia was subjected to a distributed denial of service attack (DDOS) with tens of thousands (largest seen to this date) of computers sending pings to government webpages and the national bank impacting commercial and communications across the country.[64] The Estonian government claimed the controlling computers were located in Russia, but the Russian government denied any involvement in the cyber-attack. The large volume of attacks and the specific targeting of the national bank suggest the Russian government had a hand in the attack, and Russia's involvement seemed to be solidified when cyber-attacks were executed against Georgia.

Russia used cyber-attacks to support conventional military operations against Georgia in 2008. The Georgian government launched an attack against South Ossetia in response to missile attacks launched by rebels. The Russian Army launched an attack the next day supported by a DDOS cyber-attack targeted at government websites and media outlets preventing the flow of information.[65] The Georgian Government tried to counter the cyber-attacks; however, the Russian's were able to reroute the attack packets making them appear to come from China.[66] The controller computer was located in Moscow with botnets hosted on servers in Canada, Turkey and Estonia.[67] The Russian's had the botnets target the international banking system with attacks appearing to originate from Georgia causing a shutdown of the banking system in Georgia.[68] While the DDOS is an unsophisticated cyber-attack, Russia demonstrated to the world the potential of what its cyber-attack can accomplish. Russia most certainly has more sophisticated cyber-attack capabilities that could impact U.S. government and private sector infrastructure.

B-3. China.

a. Recent Chinese doctrine articulates the use of a wide spectrum of warfare against its adversaries, including the United States. The People's Liberation Army (PLA) Colonels Liang and Xiangsui outline China's vision on how China will attack the United States through a combination of military and nonmilitary actions. Qiao Liang states "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[69] Qiao Liang's rule suggests any method will be used to win the war at all cost. Liang's theory presents challenges because the United States must prepare for all worse case scenarios. According to Liang and Xiangsui, China will use a host of methods, many of which lie out of the realm of conventional warfare. These methods include trade warfare, financial warfare, ecological warfare, psychological warfare, smuggling warfare, media warfare, drug warfare, network warfare, technological warfare, fabrication warfare, resources warfare, economic aid warfare, cultural warfare, and international law warfare.[70]

b. An outgrowth of Unrestricted Warfare, China's three warfare's concept was approved by the Chinese Communist Party Central Committee and the Central Military Commission in 2003. A summary of the three warfares follows:

- Psychological Warfare seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations;

- Media Warfare is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests; and
- Legal Warfare uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions.[71]

China's Three Warfares are an asymmetrical approach to support conventional and nuclear warfare. A Pentagon May 2013 Report on China claims the Three Warfares are designed to counter U.S. power projection and states that "The United States is one of four key audiences targeted by the campaign, as part of China's broader military strategy of 'anti-access/area denial' in the South China Sea."[72]

c. China's psychological warfare is a "whole of government approach with political, economic, and diplomatic components" and employs psychological warfare to reduce enemy moral through various mediums including "television, radio broadcast, loudspeakers, leaflets, and calculated military operations."[73] Furthermore, psychological warfare includes "diplomatic pressure, rumors, false narratives, and harassment to 'express displeasure, assert hegemony, and convey threats."[74] Examples of economic based psychological warfare are China threatening to sell its large holdings of U.S. debt and leveraging its nature resources such as rare earth minerals.[75] An example of China leveraging its natural resources is the 2010 Senkaku Boat Collision Incident in disputed water territory between Japan. Japan arrested the crew of the Chinese boat provoking China to implement a two month export ban on rare earth minerals to Japan prompting the release of the crew.[76]

d. China uses media warfare to continually influence populations. Media warfare is "aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests."[77] The People's Liberation Army (PLA) seeks to control domestic information access and develops themes to guide public opinion. Likewise, China targets foreign media outlet to shape information to support national objectives. The Chinese state-controlled television station network CCTV has a White House pool reporter that could influence U.S. media reporting on China issues.[78] In addition, China targets its own people overseas with propaganda to promote the idea of transnational culture that "supports Chinese public diplomacy and espionage operations throughout the world in ethnic Chinese communities, university campuses, and cultural centers such as the Confucius Institutes."[79]

e. China's legal warfare "uses international and domestic law to claim the legal high ground or assert Chinese interests."[80] China has used legal warfare in its territorial disputes in the South China Sea causing friction between Vietnam, Philippines, and other states that lay claim to the same islands and the East China Sea territorial disputes with Japan. Similarly, China uses legal warfare to influence interpretation of international law, such as the United Nations Convention on the Law of Sea, pushing to expand its sovereign authority out to a 200 nautical mile Exclusive Economic Zone, including the airspace and potentially space within the zone.[81] This would benefit China greatly, pushing its territory authority beyond Taiwan into the Pacific Ocean and creating a larger buffer zone and sphere of influence.

f. China has a robust and active cyber warfare programs used to target the United States in the public and private sectors. Richard Clarke and Robert Knake in their book *Cyber War: The Next Threat to National Security and What to Do About It* outlines ten techniques the cyber warfare department of the People's Liberation Army (PLA) for offensive and defensive operations in cyberspace: "planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone (sic) information, organizing information defense, and establishing network spy stations."[82] The Department of Defense (DOD) Annual Report to Congress *Military and Security Developments Involving the People's Republic of China 2012* reports that China in 2011 has maintained investment in military cyberspace capabilities and China had an extensive cyber espionage program targeting "computer networks and systems around the world … to be targets of intrusions and data theft … some of the targeted systems were U.S. government-owned, others were commercial networks owned by private companies whose stolen data represents valuable intellectual property."[83] The DOD report asserts that, "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[84] China has clearly demonstrated that it is conducting some of these operations against the United States.

China is suspected in many cases of conducting cyber-attacks against the United States in the private and public sectors. Shane Harris reports that in 2003 the PLA is suspected of causing power outages in the northeastern United States and Florida. The largest blackout in American history occurred in August 2003 effecting Michigan, Ohio, New York, and Parts of Canada.[85] A computer virus disrupted communication lines used to control the power grid.[86] In the Florida case, the PLA is suspected of trying to map the Florida Power & Light's computer infrastructure, but inadvertently shut down a large portion of the Florida power grid in doing so.[87] Likewise, Cyber espionage in both government and the private sector is prevalent. Paul K. Martin, National Aeronautics and Space Administration's (NASA) inspector general, reported Chinese hackers gained control of NASA's Jet Propulsion Laboratory computer system, and he reported in 2010 and 2011that NASA had "5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems."[88] According to

Pierre Thomas and Olivia Katrandjian, hackers with Chinese military ties hacked into the Chamber of Commerce with access to “everything in the chamber computers, including, potentially, the entire U.S. trade policy playbook.”[89] In addition, the People’s Liberation Army is suspected of hacking into Pentagon computers impacting computer systems in the Office of the Secretary of Defense.[90] China’s cyber-attacks clearly show the vulnerabilities to the U.S. public and private sectors information and infrastructure security. States like Russia and China will continue to exploit weaknesses in cyberspace to gather information and influence others.

B-4. Iran.

a. Iran’s military doctrine is defensive in nature and combines the use of conventional, guerrilla, and special operations forces. Iran’s defensive military doctrine is described as a mosaic defense having flexibility and decentralized command and control.[91] The doctrine is designed to “deter an attack, survive an initial strike, retaliate against an aggressor, and force a diplomatic solution to hostilities while avoiding any concessions that challenge its core interests.”[92] Iran views the United States as its greatest threat and has adopted some doctrinal inspiration from China and North Korea after seeing how the two countries are able to balance against the United States.[93]

b. Iran's defensive doctrine to deter and retaliate against an aggressor includes programs to expand missile capabilities and the development of nuclear technologies. Iran is developing and fielding more capable ballistic missiles to counter threats from Israel and other actors in the region while developing the capability to launch intercontinental ballistic missiles.[94]

c. Iran will continue to develop its anti-access and area denial capabilities through symmetric and asymmetric means to protect its territory and control the Strait of Hormuz. Iran will use "hit and run attacks with sea and land-launched anti-ship cruise missiles, mines, mini-subs and suicide boats."[95] Iran is known to have used small high-speed boats to harass other boats in the region. In January 2012, U.S. Military officials reported two incidents involving harassment from Iranian speed boats. The first incident involved the USS New Orleans sailing through the Strait of Hormuz when three Iranian Navy speed boats approached within 500 yards without heading any warnings and eventually broke away.[96] The second incident involved the U.S. Coast Guard cutter Adak operating 75 miles east of Kuwait City when harassed by high-speed Iranian Navy boats with personnel carrying AK-47 rifles.[97]

d. Iran conducts covert activities through special operations forces to conduct terrorist activities and support proxy forces to support Iranian national objectives. The primary unit that conducts these activities is Iran's Islamic Revolutionary Guard Corps (IRGC) elite Qods force. The IRGC has a direct connect to the Supreme Leader bypassing the General Military Staff. The

IRGC is financial through government and commercial enterprises. The IRGC's $5 billion overt military budget is supplemented by smuggling income estimated at $13 billion per year.[98]

Through the Qods force, Iran provides "material support to terrorist or militant groups such as HAMAS, Lebanese Hezbollah, the Palestinian Islamic Jihad, the Taliban, and Iraqi Shia groups."[99] Hezbollah is the primary terrorists' proxy for Iran working together with a campaign of terror against Israel, the United States and other western nations.[100] Iran has attempted terrorist actions in the United States orchestrated by the Qods Force. Mansour Arbabsiar, an Iranian-American used-car salesman, pleaded guilty in October 2012 "to conspiring with Iranian agents to assassinate the Saudi ambassador to the United States."[101] Within Iraq, the Qods Force worked with Shia militia groups to counter U.S. objectives and diminish the presence and influence of Sunni groups. The special operations forces in Iraq have gained operational experience and "trained to attack critical infrastructure such as dams, power plants, and pipelines."[102] The Qods Force will be the primary Iranian unit operating outside its borders, which the U.S. will have to counter.

e. Iran has rapidly developed its defensive and offensive cyber capabilities over the past two years. Iran's past experience with the Stuxnet virus and the post-election riots in 2009 have demonstrated a need for a defensive cyber capability that has a multi-dimensional system with three main parts:

- Creating a defensive envelope against cyber attacks on critical infrastructures and sensitive information;
- Neutralizing cyber operations by opposition elements and regime opponents;
- Keeping Western ideas and content, which would contribute to the development of a "soft revolution" that would harm the stability of the regime, out of Iranian cyberspace.[103]

Iran's defensive internal cyber system worked during the June 2013 elections having considerable success controlling the discourse on the domestic internet.[104] Iran's cyber capabilities are not as developed as the United States and China, but Iran will continue to improve its defensive cyber capabilities.

f. Iran seeks a sophisticated offensive cyber capability to weaken adversaries to gain military superiority and to counter external actions and activities. An effective cyber capability allows Iran the ability to have effects on an adversary with plausible deniability, and those cyber actions may not reach the level of retaliatory reactions. In late 2012, U.S. intelligence officials believe Iran executed a denial of service attack against U.S. banks websites having debilitating effects.[105] In 2013, Iran hackers are alleged to have infiltrated the U.S. Navy and Marine Corps unclassified computer network resulting into a four month effort to recover from the breach.[106]

In addition, Iran is working to expand cyber capabilities with its allies. Iran is supporting the Syrian Electronic Army hacker's organization to create an effective system of proxies to work with then in the cyber domain.[107] The Director of National Intelligence James Clapper warned that Iran's "development of cyber espionage or attack capabilities might be used in an attempt to either provoke or destabilize the United States or its partners."[108] Iran will continue to expand its sphere of influence in the cyber domain by developing a more sophisticated capability for offensive and counter-strike actions in support of national objectives.

B-5 Conclusion.

Adversaries are using and growing capabilities, which avoid current western overmatching combat strengths. Adversaries will continue using asymmetrical approaches such as applications derived from technological proliferation, cyber operations, terrorist activities, information and media operations to diminish western advantages. Opportunities to bruise international law without consequence and vulnerabilities in a globalized economy provide seams where adversaries apply pressure. The synergy of these efforts creates a new battleground, requiring adaptation to confront the new challenge.

Glossary

Section I
Abbreviations

1st SFC (P)	1st Special Forces Command (Provisional)
ADP	Army Doctrine Publication
ARSOF	United States Army Special Operations Forces
CA	Civil Affairs
CENTCOM	United States Central Command
CF	conventional forces
CIA	Central Intelligence Agency
CMAG	Civil Military Advisory Group
COIN	counterinsurgency
CONUS	continental United States
CT	counterterrorism
C-UW	counter-unconventional warfare
DDOS	distributed denial of service
DIME	diplomatic, informational, military, and economic
DIMEFIL	diplomatic, informational, military, economic, financial, intelligence and law enforcement
DOD	Department of Defense
DOS	Department of State
EXORD	execute order
FID	foreign internal defense
FM	field manual
FMLN	Frente Farabundo Martí para la Liberación Nacional
FOE	future operating environment
GCC	Geographical Combatant Command
GLN	Global Landpower Network
GSN	Global Special Operations Forces Network
GWOT	Global War on Terrorism
HN	host nation
IRGC	Islamic Revolutionary Guard Corps
IW	irregular warfare
JIACG	Joint Interagency Coordination Group
JIATF-CT	Joint Interagency Task Force-Counterterrorism
JIIM	joint, interagency, intergovernmental, and multinational
JIPOE	Joint Intelligence Preparation of the Operational Environment
JOPES	Joint Operation Planning and Execution System
JOPP	Joint Operation Planning Process
JP	joint publication
JTF	joint task force

LNO	Liaison Officer
MDMP	Military Decision Making Process
MEG	MISOC Effects Group
MIS	Military Information Support
MISO	Military Information Support Operations
MISOC	Military Information Support Operations Command
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NIC	National Intelligence Council
NIMS	National Incident Management System
NRF	National Response Framework
NSC	National Security Council
OPCON	operational control
PE	preparation of the environment
PLA	People’s Liberation Army
PPD	Presidential Policy Directive
SECDEF	Secretary of Defense
SF	Special Forces
SO	stability operations
SOF	special operations forces
SOJTF	Special Operations Joint Task Force
SOTF	Special Operations Task Force
TRADOC	U.S. Army Training and Doctrine Command
TSOC	Theater Special Operations Command
TTP	tactics, techniques, and procedures
UN	United Nations
USA	United States Army
USAID	U.S. Agency for International Development
USSOCOM	United States Special Operations Command
UW	unconventional warfare
UWSTA	Unconventional Warfare Social Theory Academy
VEO	violent extremist organization

Section II
Terms

Counterinsurgency
A comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes (JP 3-24).

Counterterrorism
Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks (JP 3-26).

Counter-unconventional warfare
A strategy encompassing a whole-of-government approach to synchronize the pillars of irregular warfare to integrate joint, interagency, intergovernmental, and multinational partner efforts against adversary unconventional warfare activities.

Foreign internal defense
Participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security (JP 3-22).

Irregular warfare
A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government (JP 1).

Joint intelligence preparation of the operational environment
The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action (JP 2-01.3).

Preparation of the environment
An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations (JP 3-05).

Security Sector Assistance
The security sector is composed of those institutions - to include partner governments and international organizations - that have the authority to use force to protect both the state and its citizens at home or abroad, to maintain international peace and security, and to enforce the law and provide oversight of those organizations and forces. It includes both military and civilian organizations and personnel operating at the international, regional, national, and sub-national

levels. Security sector actors include state security and law enforcement providers, governmental security and justice management and oversight bodies, civil society, institutions responsible for border management, customs and civil emergencies, and non-state justice and security providers (PPD 23 Fact Sheet).

Special warfare
The execution of activities that involve a combination of lethal and nonlethal actions taken by a specially trained and educated force that has a deep understanding of cultures and foreign language, proficiency in small-unit tactics, and the ability to build and fight alongside indigenous combat formations in permissive, uncertain, or hostile environment (ADP 3-05).

Stability operations
Various military missions, tasks, and activities conducted outside the U.S. in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-07).

Surgical strike
The execution of activities in a precise manner that employ special operations forces in hostile, denied, or politically sensitive environments to seize, destroy, capture, exploit, recover or damage designated targets, or influence threats. (ADP 3-05)

Traditional warfare
A violent struggle for domination between nation-states or coalitions and alliances of nation-states. With the increasingly rare case of formally declared war, traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces (SOF) against each other in all physical domains as well as the information environment (which includes cyberspace) (JP 1).

Unconventional warfare
Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area (JP 3-05).

Endnotes

[1] Joint Publication (JP) 3-05 *Special Operations*, April 2011, II-9.

[2] The Islamic State is also known as the Islamic State in Iraq and Syria (ISIS) and Islamic State of Iraq and the Levant (ISIL).

[3] Victoria Nuland, Assistant Secretary, Bureau of European and Eurasian Affairs, Statement Before the Senate Committee on Foreign Relations, *Ukraine: Countering Russian Intervention and Supporting Democratic State*, 113th Cong., 2d sess., May 6, 2014.

[4] John Kerry, Secretary of State, Opening Statement Before the Senate Committee on Foreign Relations, *National Security and Foreign Policy Priorities in the FY 2015 International Affairs Budget*, 113th Cong., 2d sess., April 8, 2014.

[5] See Gen Valery Gerasimov, Chief of Staff of the Russian Federation, “The Value of Science in Prediction,” in *Military-Industrial Kurier*, Feb 27, 2013; cited in “The ‘Gerasimov Doctrine’ and Russian non-Linear War,” accessed Sept 26, 2013: http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

[6] David Maxwell, “Unconventional Warfare and Counter-Unconventional Warfare” (PowerPoint Presentation, United States Special Operations Command, MacDill AFB, Florida, July 9, 2014).

[7] David Maxwell, “Unconventional Warfare and Counter-Unconventional Warfare”.

[8] Traditional warfare is characterized as a violent struggle for domination between nation-states or coalitions and alliances of nation-states. With the increasingly rare case of formally declared war, traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces (SOF) against each other in all physical domains as well as the information environment (which includes cyberspace). JP 1 *Doctrine for the Armed Forces of the United States*, 25 March 2013, x.

[9] U.S. Department of State, Bureau of Political-Military Affairs, *U.S. Government Counterinsurgency Guide* (Washington, D.C.: U.S. Government Printing Office, 2009), accessed May 16, 2014, http://www.state.gov/documents/organization/119629.pdf.

[10] IW is characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation’s established government. JP 1 *Doctrine for the Armed Forces of the United States*, 25 March 2013, x.; There are principally five activities or operations that are undertaken in sequence, in parallel, or in blended form in a coherent campaign to address irregular threats: counterterrorism (CT), unconventional warfare (UW), foreign internal defense (FID), counterinsurgency (COIN), and stability operations (SO). In addition to these five core activities, there are a host of key related activities including strategic communications, information operations of all kinds, psychological operations, civil-military operations, and support to law enforcement, intelligence, and counterintelligence operations in which the joint force may engage to counter irregular threats. Irregular Warfare: Countering Irregular Threats, Joint Operating Concept, Version 2.0, 17 May 2010, 5.

[11] Field Manual 3-24 *Insurgencies and Countering Insurgencies*, 13 May 2014, 4-11.

[12] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington D.C.: U.S Government Printing Office, December 2012), ii. The Megatrends are individual empowerment, diffusion of power, demographic patterns, and food, water, energy nexus.

[13] Sebastian Gorka, *Army Special Operations Forces Operating Concept Strategic Setting Paper* (Blacksburg, VA: Virginia Tech Applied Research Corporation, September 2013), 7-8.

[14] National Intelligence Council, *Global Trends 2030: Alternative Worlds*, 18.

[15] National Intelligence Council, *Global Trends 2030: Alternative Worlds*, iii.

[16] The key components of a hybrid threat are two or more of the following: military forces, nation-state paramilitary forces (such as internal security forces, police, or border guards), insurgent organizations (movements that primarily rely on subversion and violence to change the status quo), guerrilla units (irregular indigenous forces operating in occupied territory), and criminal organizations (such as gangs, drug cartels, or hackers). Training and Doctrine Command (TRADOC) G-2, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, August 2012, 39.

[17] Training and Doctrine Command (TRADOC) G-2, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, 40.

[18] United States Joint Forces Command, *Joint Operating Environment 2010* (Norfolk, VA: United States Joint Forces Command, 2010), 66.

[19] What has been attempted with less success in the GWOT is to influence the population groups who, through intimidation or affinity, provide the "water", i.e., the support and sanctuary for the terrorist organizations.

[20] A possible model could be the National Response Framework (NRF) and the supporting National Incident Management System (NIMS) used in U.S. disaster response. For more information on the National Response Framework see Federal Emergency Management Agency, “National Response Framework,” U.S. Department of Homeland Security, last modified February 3, 2014, accessed May 15, 2014, http://www.fema.gov/national-response-framework. For more information on the National Incident Management System see Federal Emergency Management Agency, “National Incident Management System,” U.S. Department of Homeland Security, last modified June 4, 2013, accessed May 15, 2014, http://www.fema.gov/national-incident-management-system.

Additionally, the Department of Defense *Strategy for Homeland Defense and Defense Support of Civil Authorities*, February 2013, outlines the missions, objectives, core capabilities and strategic approaches for the Department. A similar strategy should be developed for irregular warfare/counter-UW with a whole-of-government approach.

[21] See “Operating in the Human Domain,” White Paper, Version 0.70, USSOCOM, September 2014.

[22] The President of the United States must approve combat operations as part of FID. JP 3-22 *Foreign Internal Defense*, 12 July 2010, VI-36.

[23] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, “Political Warfare,” Policy Innovation Memorandum No. 33, Council on Foreign Relations, June 2013, accessed May 16, 2014, http://www.cfr.org/wars-and-warfare/political-warfare/p30894.

[24] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, “Political Warfare.”

[25] The White House, Office of the Press Secretary, "Fact Sheet: U.S. Security Sector Assistance Policy," The White House, April 5, 2013, accessed July 3, 2014, http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

[26] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, “Political Warfar.,”

[27] George Kennan, "Policy Planning Memorandum," May 4, 1948, National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, accessed June 9, 2014, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

[28]United States Joint Forces Command, Commander's Handbook for Joint Interagency Coordination Group, 1 March 2007, II-1.

[29] Matthew F. Bogdanos, "Joint Interagency Cooperation: The First Step," *Joint Force Quarterly* 37, (2nd Quarter 2005): 10-18, accessed July 11, 2014, http://www.dtic.mil/doctrine/jfq/jfq-37.pdf. Prior to the development of the JIACG, task forces and working groups were formed in an ad hoc manner to coordinated activities with narrow scopes and authorities. In November 2001, United States Central Command (CENTCOM) established a Joint Interagency Task Force-Counterterrorism (JIATF-CT) in Afghanistan primarily as an intelligence fusion center and to operate the interrogation facility in Bagram —which it did with great success. In 2002, the JIATF-CT evolved into a comprehensive JIACG that changed its focus from the short-term CT fight to the long-term war on terrorism. JIATF-CT comprised 36 U.S. military, 57 non-DOD, and several British and Australian special forces personnel. The interagency team included: Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Diplomatic Security Service (DSS), Customs Service, National Security Agency (NSA), Defense Intelligence Agency (DIA), Defense Human Intelligence Service, New York's Joint Terrorism Task Force, and the Justice, Treasury and State Departments.

[30] U.S. Pacific Command, "Joint Interagency Task Force West," U.S. Pacific Command, accessed July 10, 2014, http://www.pacom.mil/Contact/Directory/JointIntegragencyTaskForceWest.aspx.; The JIATF West Strategy is built on the premise of interagency cooperation. JIATF West partners with U.S. and foreign law enforcement agencies through regional U.S. Embassies and their respective country teams. We also partner with regional law enforcement agencies, such as New Zealand Police, Australian Federal Police, and Australian Customs Service, who coordinate complementary capabilities in the region. We bring military and law enforcement capabilities together to combat and reduce transnational crime in the Asia-Pacific.

[31] Michael Knights, “The Evolution of Iran’s Special Groups in Iraq,” Combating Terrorism Center at West Point, November 1, 2010, accessed May 22, 2014, https://www.ctc.usma.edu/posts/the-evolution-of-iran%e2%80%99s-special-groups-in-iraq.

[32] James M. Bright (LtCol, USMC), “Operational Seam: The Command and Control of Conventional and Special Operations Forces” (Newport, RI: Naval War College, 2007), 2, accessed May 15, 2014, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA476433.

[33] An example is the 1st Special Forces Command (Provisional) (1st SFC (P)) can deploy command elements up to a two-star general-commanded SOJTF, as the basis for a hybrid command.

[34] A possible example is where a resistance organization may have a structure to establish safe areas for the guerrilla forces. The C-UW organization would determine if they had the capabilities to identify and disrupt safe area operations. If not, the organization would organize to address the capability gaps.

[35] These include Joint Operation Planning and Execution System (JOPES), Joint Operation Planning Process (JOPP), and Military Decision Making Process (MDMP).

[36] Such as the 1st SFC (P) (SWC).

[37] ARSOF 2022, 21.

[38] ARSOF 2022, 21

[39] ARSOF 2022, 21.

[40] The White House, Office of the Press Secretary, "Fact Sheet: U.S. Security Sector Assistance Policy," The White House, April 5, 2013, accessed July 3, 2014, http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

[41] Joint Concept for Sustained Land Operations, Draft, 10 July 2014, 8.

[42] See “Joint Capability Areas Tier 1 and Supporting Tier 2 Lexicon, Post 24 August 2006 JROC,” accessed Sept 25, 2014: http://www.mors.org/UserFiles/file/meetings/06bar/luke.pdf.

[43] The Joint Intelligence Preparation of the Operational Environment (JIPOE) is an example for intelligence aspects. See Joint Publication 2-01.3: *Joint Intelligence Preparation of the Battlefield, 16 June 2009.*

[44] The Counter Terrorist intelligence fusion process could serve as a model in this regard.

[45] Field Manual 3-24 *Insurgencies and Countering Insurgencies*, 13 May 2014, 7-14. Remote area operations was removed from current FID doctrine. Remote area operations had a section in Appendix A Insurgency and Counterinsurgency, sub section Military Operations in Counterinsurgency in FM 3-05.202 *Foreign Internal Defense*, 2 February 2007, A-9, A-10.

[46] Field Manual 3-24 *Insurgencies and Countering Insurgencies*, 13 May 2014, 7-15.

[47] David Maxwell, “Unconventional Warfare and Counter-Unconventional Warfare.”

[48] Joint Publication 3-05 *Special Operations*, April 2011, II-9.

[49] Joint Publication 3-22 *Foreign Internal Defense,* 12 July 2010, ix.

[50] FID tools include: indirect support including security cooperation, security assistance, multinational/joint exercises, and exchange exercises; direct support including civil-military operations, military information support operations, military training support, logistic support, intelligence, and communications sharing; and combat operations with presidential approval. FM 3-05.2 *Foreign Internal Defense*, 1 September 2011, 1-4; See also JP 3-22 *Foreign Internal Defense*, 12 July 2010, I-8, I-11.

[51] Joint Publication 3-24 *Counterinsurgency*, 22 November 2013, ix.

[52] Joint Publication 3-07 *Stability Operations*, 29 September 2011, vii.

[53] Ibid., I-1.

[54] Joint Publication 3-26 *Counterterrorism*, 17 November 2009, vi.

[55] Surgical strike is the execution of activities in a precise manner that employ special operations forces in hostile, denied, or politically sensitive environments to seize, destroy, capture, exploit, recover or damage designated targets, or influence threats. ADP 3-05 *Special Operations*, 31 August 2012, 9.

[56] Max Boot, "Appendix: The Invisible Armies Database," in *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (New York: Liveright Publishing Company, 2013), 569-589.

[57] Charles L. Smith, “Soviet Maskirovko,” *Airpower Journal* 2, no. 1 (Spring 1988): accessed July 30, 2014, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj88/spr88/smith.html.

[58] Janis Berzins, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” Policy Paper 2, Center for Security and Strategic Research, National Defence Academy of Lativa, April 2014, 5.

[59] “The Military Doctrine of the Russian Federation,” Text of report by Russian presidential website 5 February 2010, approved by Russian Federation presidential edict on 5 February 2010, Carnegie Endowment for Peace, accessed July 30, 2014, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

[60] Tchekinov and Bogdanov quoted in Janis Berzins, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” Policy Paper 2, Center for Security and Strategic Research, National Defence Academy of Lativa, April 2014, 6.

[61] Stratfor, “Putting Russia’s Crimean Intervention in Context,” Stratfor, April 12, 2014, accessed July 21, 2014, http://www.stratfor.com.

[62] Stratfor, “Putting Russia’s Crimean Intervention in Context,” Stratfor, April 12, 2014, accessed July 21, 2014, http://www.stratfor.com.

[63] Richard Clarke and Robert Knake, *Cyber War: The Next Threat To National Security and What To Do About It* (New York, NY: HarperCollins Publishers, 2010), 13.

[64] Ibid., 13-15.

[65] Ibid., 18-19.

[66] Ibid., 19.

[67] Ibid., 19.

[68] Ibid., 20.

[69] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, trans. Foreign Broadcast Information Service. (Beijing: PLA Literature and Arts Publishing House, 1999) 2.

[70] Bill Gertz, *The China Threat: How the People's Republic Targets America* (Washington, D.C.: Regnery Publishing, 2000), 16.

[71] Department of Defense, Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," August 2011, 26, accessed August 1, 2014, http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf.

[72] Department of Defense China Report May 2013 quoted in Bill Gertz, "Warfare Three Ways: China Waging 'Three Warfares' against United States in Asia, Pentagon Says," *The Washington Free Beacon*, March 26, 2014, accessed July 31, 2014, http://freebeacon.com/national-security/warfare-three-ways/.

[73] Timothy A. Walton, "China's Three Warfares," Special Report 3, Delex Systems, January 18, 2012, 5, accessed July 30, 2014, http://www.delex.com/data/files/Three%20Warfares.pdf.

[74] Department of Defense China Report May 2013 quoted in Bill Gertz, "Warfare Three Ways: China Waging 'Three Warfares' against United States in Asia, Pentagon Says."

[75] Ibid.

[76] Timothy A. Walton, "China's Three Warfares," Special Report 3, Delex Systems, January 18, 2012, accessed July 30, 2014, http://www.delex.com/data/files/Three%20Warfares.pdf, 5.

[77] Department of Defense, Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," August 2011, www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf (accessed August 1, 2014) 26.

[78] Bill Gertz, "Warfare Three Ways: China Waging 'Three Warfares' against United States in Asia, Pentagon Says.

[79] Timothy A. Walton, "China's Three Warfares."

[80] Department of Defense, Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," August 2011, 26, accessed August 1, 2014, http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf.

[81] Timothy A. Walton, "China's Three Warfares."

[82] Richard Clarke and Robert Knake, *Cyber War: The Next Threat To National Security and What To Do About It*, 57-58.

[83] Department of Defense, Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," May 2012, iv, 9, accessed August 1, 2014, http://www.defense.gov/pubs/pdfs/2012_cmpr_final.pdf.

[84] Department of Defense, Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," May 2012, 10, accessed August 1, 2014, http://www.defense.gov/pubs/pdfs/2012_cmpr_final.pdf.

[85] Shane Harris, "China's Cyber-Militia," *National Journal*, Updated January 31, 2011, accessed August 5, 2014, http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531?print=true.

[86] Ibid.

[87] Ibid.

[88] FoxNews, "Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals," *FoxNews.com*, March 1, 2012, accessed August 1, 2014, http://www.foxnews.com/scitech/2012/03/01/chinese-hackers-nasa-jpl-lab/?intcmp=features#ixzz1o4lu0Zfq.

[89] Thomas Pierre and Olivia Katrandjian, "Chinese Hack Into US Chamber of Commerce, Authorities Say," ABC News, December 21, 2011, accessed August 2, 2014, http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642.

[90] Demetri Sevastopulo, "Chinese hacked into Pentagon," *Financial Times*, September 3, 2007, accessed August 1, 2014, http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html#axzz1ub4uQxx1.

[91] Alireza Nader, "The Iran Primer, Part I: How Would Iran Fight Back? United States Institute for Peace, October 1, 2012, accessed August 11, 2014, http://iranprimer.usip.org/blog/2012/oct/01/part-i-how-would-iran-fight-back?

[92] Department of Defense, "Annual Report on Military Power of Iran," Executive Summary, January 2014, accessed August 11, 2014, http://freebeacon.com/wp-content/uploads/2014/07/Iranmilitary.pdf.

[93] Ahmed S. Hashim, “The Evolution of Iran’s Military Doctrine,” Center for Strategic & International Studies, January 9, 2013, accessed August 11, 2014, http://csis.org/files/attachments/130109_Summary_Hashim.pdf.

[94] Department of Defense, “Annual Report on Military Power of Iran,” Executive Summary, January 2014, accessed August 11, 2014, http://freebeacon.com/wp-content/uploads/2014/07/Iranmilitary.pdf

[95] Michael Cummings and Eric Cummings, The Cost of War with Iran: An Intelligence Preparation of the Battlefield," *Small Wars Journal*, August 31 2012, accessed August 20, 2014, http://smallwarsjournal.com/jrnl/art/the-costs-of-war-with-iran-an-intelligence-preparation-of-the-battlefield.

[96] Barbara Starr, "Official: U.S. Vessels Harassed by High-Speed Iranian Boats," CNN, January 13, 2012, accessed August 20, 2014, http://www.cnn.com/2012/01/13/us/iran-boats-tensions/.

[97] Barbara Starr, “Official: U.S. Vessels Harassed by High-Speed Iranian Boats.”

[98] Michael Rubin, “U.S. Response to Iran’s Use of Unconventional Warfare” (PowerPoint presentation at USASOC Irregular Warfare Seminar, Fort Bragg, NC, August 28, 2014). Mr. Rubin also highlighted the IRGC’s involvement in the Iranian electronics industries such as computers, telephones, scanners, and SIM cards; the IRGC has signed $50 billion worth of contracts with the Oil Ministry under President Ahmadinejad; the IRGC operates the cargo airport Payam International Airport; and has 25 gates outside customs control at the Imam Khomeini International Airport.

[99] Department of Defense, “Annual Report on Military Power of Iran,” Executive Summary, April 2012, accessed August 11, 2014, http://fas.org/man/eprint/dod-iran.pdf.

[100] Matthew Levitt, "Hizballah and the Qods Force in Iran's Shadow War with the West," Policy Focus 123, Washington Institute For Near East Policy, January 2013, 1.

[101] Matthew Levitt, "Hizballah and the Qods Force in Iran's Shadow War with the West,",1.

[102] Ahmed S. Hashim, “The Evolution of Iran’s Military Doctrine,” Center for Strategic & International Studies, January 9, 2013, accessed August 11, 2014, http://csis.org/files/attachments/130109_Summary_Hashim.pdf.

[103] Gabi Siboni and Sami Kronenfeld, “Developments in Iranian Cyber Warfare, 2013-2014,” INSS Insight No. 536, April 3 2014, accessed August 20, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=6809.

[104] Gabi Siboni and Sami Kronenfeld, “Developments in Iranian Cyber Warfare, 2013-2014.”

[105] Shane Harris, “Forget China: Iran’s Hackers Are America’s Newest Cyber Threat,” Foreign Policy, February 18, 2014, accessed August 20, 2014, http://complex.foreignpolicy.com/posts/2014/02/18/forget_china_iran_s_hackers_are_america_s_newest_cyber_threat.

[106]Shane Harris, Ibid..

[107] Gabi Siboni and Sami Kronenfeld, “Developments in Iranian Cyber Warfare, 2013-2014.”

[108] James Clapper quoted in Shane Harris, “Forget China: Iran’s Hackers Are America’s Newest Cyber Threat.”