Strategy Research Project

Employing U.S. Information Operations Against Hybrid Warfare Threats

by

Colonel Dean A. Burbridge
United States Army

United States Army War College
Class of 2013

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* xx-03-2013	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Employing U.S. Information Operations Against Hybrid Warfare Threats

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Dean A. Burbridge
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. G. Alexander Crowther
Strategic Studies Institute

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 12,133

14. ABSTRACT

U.S. military operations against hybrid threats must integrate IO into their concept of operations to a greater degree than current practice. The whole of the U.S. Government must also work towards more effective dissemination of our narrative. Since hybrid warfare attempts to defeat a nation’s will, a comprehensive information effort is necessary to: generate effects for military operations; attack the hybrid adversaries will; isolate the adversary diplomatically; and maintain international support for the military campaign. Shaping to prevent war must involve coordinating our narrative; enunciating the ramifications of conflict to hybrid threats; establishing information conduits into conflict areas; and collaborating with joint, interagency, intergovernmental, and multi-national partners. Some of the IO techniques may appear tactical; however, the strategic information environment can be significantly altered by or through a single tactical event. Technical enablers such as Electronic Warfare and Cyber activities are also critical to combating hybrid threats, as is controlling how adversaries view our operations through use of Operations Security and Military Deception. In many ways, “the mission is the message.”

15. SUBJECT TERMS
Strategic Communication, Public Diplomacy, Shaping, Media, Irregular Warfare, Targeting, MISO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	68	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Employing U.S. Information Operations Against Hybrid Warfare Threats

by

Colonel Dean A. Burbridge
United States Army

Dr. G. Alexander Crowther
Strategic Studies Institute
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Employing U.S. Information Operations Against Hybrid Warfare Threats
Report Date:	March 2013
Page Count:	68
Word Count:	12,133
Key Terms:	Strategic Communication, Public Diplomacy, Shaping, Media, Irregular Warfare, Targeting, MISO
Classification:	Unclassified

U.S. military operations against hybrid threats must integrate IO into their concept of operations to a greater degree than current practice. The whole of the U.S. Government must also work towards more effective dissemination of our narrative. Since hybrid warfare attempts to defeat a nation's will, a comprehensive information effort is necessary to: generate effects for military operations; attack the hybrid adversaries will; isolate the adversary diplomatically; and maintain international support for the military campaign. Shaping to prevent war must involve coordinating our narrative; enunciating the ramifications of conflict to hybrid threats; establishing information conduits into conflict areas; and collaborating with joint, interagency, intergovernmental, and multi-national partners. Some of the IO techniques may appear tactical; however, the strategic information environment can be significantly altered by or through a single tactical event. Technical enablers such as Electronic Warfare and Cyber activities are also critical to combating hybrid threats, as is controlling how adversaries view our operations through use of Operations Security and Military Deception. In many ways, "the mission is the message."

Employing U.S. Information Operations Against Hybrid Warfare Threats

Many authors have written about the concept of Hybrid Warfare in recent years. Many authors continue to write about the broad subject of Information Operations (IO). However, as of this writing, there is no single document that makes a dedicated attempt to conceptualize how IO can or should be applied towards Hybrid Warfare threats. Despite the fact that authors have written about Hybrid Warfare since 2007, the U.S. military's November 2012 Joint Publication on IO makes no specific reference to Hybrid or Irregular Warfare.[1]

"Virtually every action, message, and decision of a force shapes the opinions of an indigenous population."[2] Hybrid Warfare groups exploit this truism. They further their narrative by exploiting their opponent's failings. U.S. military operations against hybrid threats must integrate IO into their concept of operations to a greater degree than current practice. The whole of the U.S. Government must also work towards more effective dissemination of our narrative. Since hybrid warfare attempts to defeat a nation's will, a comprehensive information effort is necessary to: generate effects for military operations; attack the hybrid adversary's will; isolate the adversary diplomatically; and maintain international support for the overall military campaign.

The potential economic and diplomatic costs to the U.S. from a conflict with a hybrid threat could be substantial, and so like other forms of warfare, prevention is preferable. Prevention requires that we shape the environment well in advance of armed conflict. Such shaping must involve coordinating our narrative regarding the likely Hybrid Warfare conflict locations; enunciating the ramifications of conflict to potential hybrid threats; establishing information conduits into potential conflict areas; and collaborating with joint, interagency, intergovernmental, and multi-national partners.

This paper covers both theory and practical application of information capabilities towards Hybrid Warfare threats. Some of the recommendations discussed in this paper may appear tactical in nature; however, just as the strategic information environment can be significantly altered by or through a single tactical event, so too tactical events can be shaped by a strategic narrative. The emphasis of IO against Hybrid Warfare is to get information to select audiences. However, technical information-related enablers such as Electronic Warfare and Cyber activities are also critical to combating hybrid threats, as is controlling how adversaries view our operations through use of Operations Security and Military Deception. In many ways, “the mission is the message.” This paper will provide an overview of IO and information related capabilities, summarize current Hybrid Warfare thought, discuss why we need to apply IO differently to hybrid threats, and provide recommendations for IO integration and application during the various phases of military operations.

Overview of Information Operations and Hybrid Warfare

Traditional IO Capabilities and Issues

There are five traditional core IO capabilities. Those capabilities are: Military Information Support Operations (MISO), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO) or Cyberspace Operations.[3] U.S. Joint and NATO IO efforts are generally organized and executed in consonance with the “core, supporting, and related” information capabilities historically associated with IO application.[4] The Joint Publication for Information Operations now bundles these and other tools together as “information-related capabilities” (IRCs).[5] In January 2011, the U.S. Secretary of Defense published a memorandum that redefined IO to more clearly indicate IO is primarily a verb rather than a noun.[6] That change was made by removing mention of the five capabilities that had been contained in the previous definition. However, within U.S. joint headquarters, the IO form and function remain largely unchanged. The traditional capabilities are discussed below.

The first IRC is Military Information Support Operations (MISO), termed Psychological Operations or PSYOP until 2010.[7] The purpose of MISO is to "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable" to military or national objectives.[8] Unlike other IRCs, MISO provides the capability to directly reach large foreign audiences with messages tailored to resonate culturally. U.S. MISO resources include radio broadcast, loudspeakers, printed materials (such as leaflets and handbills), and limited contracted media dissemination via foreign radio, television, the foreign-language internet, and commercial print media. The ability to directly reach foreign audiences, including adversaries, makes MISO a powerful force-multiplier.[9] In support of combat operations, MISO units are often organized as a Joint MISO Task Force (JMISTF).

While MISO professionals do receive some cultural training, the training does not result in a uniformly high quality of messaging products. Likewise, U.S. national-level messaging guidance from the White House and Department of State does not fully exploit MISO capabilities.[10]

Military Deception is as venerable as war itself, although the practice, resources and seemingly even the desire to conduct it, have atrophied since the end of WWII.[11]

The purpose of MILDEC is to cause adversaries "to behave in a manner advantageous to the friendly mission."[12] Examples include "misallocation of resources, attacking at a time and place advantageous to friendly forces, or avoid taking action at all."[13] In general terms, MILDEC plans employ various feints, demonstrations, and displays.[14] Military deception is to a large degree a function of planning. Within operational and tactical military units MILDEC is often assigned as secondary function to a staff officer who has other primary and competing responsibilities.[15]

Operations Security (OPSEC) is a "process designed to meet operational needs by mitigating risks associated with specific vulnerabilities in order to deny adversaries critical information and observable indicators."[16] In practice, OPSEC involves determining what friendly information exists that if obtained by adversaries, would pose a risk to friendly operations; determining adversaries' ability to obtain that information; and taking measures to protect the information. Often the information OPSEC seeks to protect comes from what can be publicly observed, e.g., staging of military equipment prior to mission execution. This makes OPSEC distinct from the related U.S. military categories of physical security (which prevents unauthorized access) and information security (which primarily pertains to classified information). OPSEC often suffers from the same dilemma as MILDEC, in that staff responsibility is often a secondary function that is not well integrated with overall planning efforts.[17] OPSEC is also increasing challenged by the proliferation of cellular phone cameras and digital media.[18]

Electronic Warfare (EW) is comprised of three distinct functions: (1) electronic attack in the form of jamming and kinetic strikes against adversary radio communications and radars; (2) electronic support that identifies adversary radio and radar emitters to enable subsequent target or intelligence collection; (3) and electronic protection which defends friendly radio and radar systems.[19] In the context of IO, the primary EW tool is electronic attack, and often the term EW is used solely to mean “electronic attack” or “jamming” rather than any or all of the other EW subsets.

Most U.S. electronic attack capabilities reside in Air Force and Navy aircraft. Army electronic attack capabilities are under-resourced apart from those systems that target remote-controlled improvised explosive devices such as those found in Afghanistan and Iraq.[20]

Cyber Operations involve any use of networked computer systems.[21] This paper focuses on offensive and defensive cyber operations, intended to respectively generate effects against an adversary or protect U.S. systems from adversary cyber attack, as those are the most pertinent cyber relationships to IO in Hybrid Warfare.[22] U.S. Cyber Command (USCYBERCOM) has the lead within DoD for cyber operations, although elements of the Intelligence Community, Department of Homeland Security, and Justice Department also have cyber roles and authorities. Cyber attacks causing death or physical damage, such as attacks on a power grid, could be considered an armed attack in accordance with Article 51 of the U.N. Charter.[23] Such an attack might then legally enable a military response under the right of self-defense also found in Article 51.[24]

Cyber warfare is unique in that vulnerabilities that a network target may have could be discovered by software developers who then immediately develop and release a patch eliminating those vulnerabilities without cost to software users. In most cases, software patches update user protection automatically. As a result, cyber weapon effectiveness is transient, and requires continuous cooperation with industry, cyber tool development, and diligence to discover (and thereby enable patching) friendly vulnerabilities.[25]

Additionally, remote access attacks (sending hostile computer code through internet infrastructure in multiple countries en route to the target) have enormous legal ramifications. Even within the U.S. Government these legal issues have had varied interpretation over the last ten years, and they are not uniformly applied among the international community. In some ways, offensive cyber capabilities are analogous to strategic bombing in terms of attacking into a nation's territory from outside, and many of the desirable cyber targets are the same as those historically targeted by strategic bombing.[26] Just as strategic bombing has an uneven history of generating the desired strategic effects, so too it is possible offensive cyber strikes may not have the desired decisive impact against Hybrid Warfare adversaries even if legal concerns are overcome.[27]

Other Information Related Capabilities

There are several capabilities traditionally related to Information Operations. These are Public Affairs, Key Leader Engagement, Civil Military Operations, Combat Camera and Visual Information, physical attack, and money (i.e. rewards).

Public Affairs (PA) includes "public information, command information, and community engagement activities directed toward both the external and internal publics."[28] "In practice, public affairs is about media relations."[29] Unlike MISO, PA relies on media resources (TV, radio, print) to carry information from military sources to audiences. Though PA is a separate function from IO, PA, IO and MISO elements must coordinate their activities to prevent information fratricide.[30]

Use of the media is central to hybrid threat campaigns. Military forces should engage with media at all levels. Interface with international media is an opportunity to demonstrate U.S. and partner nation military professionalism and the legitimacy of our actions. Embedded media can be critical to accurately portray the ground situation and to expose hybrid threat adversary propaganda. Local media is critical to connecting the population to their government and it can increase partner nation credibility, as well as assist in maintaining our freedom of action. Some media members lack professionalism, and the modern 24 hour news cycle causes some media members to transform information from military sources into what could be described as information entertainment.[31] As a result, many U.S. military leaders are wary of the media, yet media are an unavoidable part of operations in a globalized world. Ignoring or actively avoiding media effectively yields a force multiplier to our adversaries. Likewise, antagonizing or deceiving the media have disproportionate negative effects, usually at the strategic level.

Key leader engagement (KLE, now Soldier and Leader Engagement in Army doctrine) is a command responsibility at all levels.[32] Through KLE military leaders may generate effects on the operational environment through discussions with appropriate foreign leaders in the conflict area, or from discussions with representatives from international organizations. KLE efforts may be supported with “talking points” generated by a focused KLE section, or within the IO, PA, Visitors Bureau, or other staff element.[33] KLE is of most value during stability and transition operations. Political restrictions may preclude KLE during decisive combat operations. Another problem with KLE is that during initial combat operations, a U.S. or partner-nation force may simply not know whom to engage, or it may be impractical from a security, logistics, or translation standpoint. The main problem with KLE, however, is that it assumes key leaders can be influenced by discussion, and more importantly entrusts those key leaders to accurately relate U.S. communication to those they lead. If those key leaders' viewpoints are fundamentally at odds with those who engage them, then a KLE event may serve as an opportunity for those key leaders engaged to exercise their duplicity.

Civil Military Operations (CMO) are a powerful tool to generate positive influence effects through humanitarian assistance, medical assistance, public works construction, and other forms of assistance to foreign civilian communities.[34] Additionally, the dissemination of CMO efforts and goals through other IRCs acts as a force multiplier by expanding the impact of CMO efforts beyond the local area where CMO efforts take place. Close coordination between the IO staff and CMO staff is critical for expectation management or CMO-related counterpropaganda. Many local citizens may desire and expect more CMO assistance than can be immediately provided. MISO support to CMO can also help prevent misunderstandings as to rationale and scope of CMO efforts, particularly in areas where military forces may not be entirely welcome in the aftermath of combat operations. An example of expectation management would be dealing with the propaganda line that "if the U.S. can put a man on the moon, but people in the U.S.-controlled area do not have electricity, it must be because the U.S. is punishing the people in that area."[35]

Photographs and full-motion video can be powerful information tools. For that reason, the U.S. military maintains a capability known as Combat Camera (COMCAM) that obtains visual information for multiple truthful purposes.[36] The "visual information" obtained by COMCAM, military aircraft, and anyone in the military with a camera that provides the photos they take for military use, enables PA and MISO efforts to inform audiences.[37] This is in keeping with the concept that "a picture tells a thousand words." With visual information, those "thousand words" are portrayed by their own evidence. During armed conflict, visual information is particularly useful to bolster friendly claims against disinformation, and to document adversary atrocities.[38]

Physical attack, also referred to as kinetic action, is also a form of influence. Kinetic action against hybrid threats may both remove the threat and deter others from adversarial behavior. The same outcome may result from the threat of kinetic action, particularly when a similar action has already occurred during the same conflict. MISO professionals characterize kinetic strikes among the many "Psychological Operations Actions."[39] Kinetic action sends a message, but like words, it must be measured, meaningful, and synchronized. Failing such to meet standards can prove dangerous to coherent messaging efforts, as will be discussed at length later in this paper.

Rewards and other monetary incentives are yet another information tool. Many irregular warfare groups, as well as insurgents, rely on trust relationships to maintain cohesion. Establishing monetary rewards for information or cooperation can attack the trust that irregular combatants rely upon to operate within civilian populations. In some cases, knowing that there is a reward for information on the leaders of an irregular force can cause the leaders to lower their profile, and deprive them of the ability to move freely to coordinate or raise money for their operations. Eventually this leads to a degree of self-marginalization that may discourage others from desiring to follow that irregular leader. Publicizing the rewards is a suitable role for both MISO and PA elements. Indeed, in recent years some U.S. military IO staffs have been responsible for the rewards program in acknowledgement of the role of rewards as an information tool.[40]

How the U.S. Conceptualizes Military Operations

The U.S. arranges military operations in six phases, Phase 0 to Phase V. Phase 0 "Shape," uses military activities and interagency efforts to dissuade potential adversaries and solidify relationship partners. Phase I "Deter," aims to prevent undesirable adversary action by demonstrating the capabilities and resolve of the joint force. Phase II "Seize Initiative," employs joint force capabilities to prevent the adversary from achieving their objectives, and is the first major combat phase. Phase III "Dominate," entails "breaking the enemy's will for organized resistance" and concludes with the termination of major combat operations. Phase IV "Stabilize," restores order in the absence of a functional civil government. Phase V, "Enable Civil Authority," uses military, interagency, and international resources to transition away from U.S. and coalition control of the conflict area.[41] The focus of IO efforts varies during each phase. However, as is the case with counterinsurgency efforts, the military force confronting hybrid threats may conduct elements of each phase simultaneously in different areas. An example is Phase IV Stability operations in areas formerly under hybrid threat control while Phase III Dominate activities are ongoing in areas that remain under hybrid threat control. How the U.S. should prepare and focus their IO efforts during each phase will be discussed later. Throughout this paper specific recommendations are based on the assumption that the U.S. military will be operating as a part of a Combined Joint Task Force (CJTF).

Hybrid Warfare

The U.S. Department of Defense has not defined Hybrid Warfare. However, several writers have developed their own definitions. Russell W. Glenn offered the following definition of hybrid threats, which encapsulates much of what is contained in the Hybrid Warfare literature:

> An adversary that simultaneously and adaptively employs some combination of (1) political, military, economic, social, and information means, and (2) conventional, irregular, catastrophic, terrorism, and disruptive/criminal warfare methods. It may include a combination of state and non-state actors.[42]

Hybrid Warfare is intended to overcome an opponent's conventional military capabilities by arraying a wider set of problems and creating diplomatic, informational, and economic dilemmas outside the military domain.[43] Hybrid Warfare is a '"cocktail mixture"' of terrorist, irregular, and conventional tactics, and may also employ links to transnational criminal elements.[44] Some Hybrid Warfare threats combine the lethality of state or state-like military resources with "the fanatical and protracted fervor of irregular warfare . . . to achieve synergistic effects."[45] Hybrid Warfare entails greater "convergence of the physical and psychological, the kinetic and non-kinetic, and combatants and noncombatants than other forms of warfare.[46] However, the physical combat aspects of warfare are less important than the cognitive impact of the conflict locally and internationally.[47] Rather than focusing on purely military means, Hybrid Warfare takes advantage of the modern information environment to engage in a "battle of narratives."[48] Though hybrid forces can employ sophisticated military capabilities, their primary tools are media reporting, the internet, "and the integration of information operations with strategic communication."[49]

Hybrid military tactics include exploiting terrain and population centers to prevent their opponents from obtaining a decisive military engagement or battle.[50] Hybrid forces intentionally intermingle with civilian populations therefore inviting civilian casualties, which are designed to cause international audiences to perceive their opponent as "brutal, disproportionate, and unnecessary," both locally and internationally.[51] This in turn serves to politically deter further military action, essentially negating any military advantage their opponent may possess.[52] Hybrid forces may use irregular tactics, such as raids and ambushes, assassinations, and terror and/or threat of terror against their opponent's civilian population.[53] Hybrid Warfare forces may also employ advanced technologies such as counter-satellite systems and cyber attack on an opponent's civilian infrastructure and economy. They could even include biological weapons.[54] Hybrid Warfare actors may use cyber attack not only against military and economic targets, but also against civilian infrastructure to create "uncertainty, panic, and physical and social effects" and resulting political pressure.[55]

How Hybrid Warfare Works

The military and terrorist components of Hybrid Warfare are largely intended to generate informational impact. Again, rather than achieve results with purely violent means, Hybrid Warfare exploits the modern information environment to directly attack the political will of opponents.[56] This ability to attack the political will stems from an information environment that now allows even non-state actors to compete with large countries' messaging efforts.[57] The Prussian military theorist Clausewitz wrote at length on focusing efforts against an adversary's "center of gravity" (COG), which is "the hub of all power" for their armed struggle.[58] Whichever side first overcomes their opponent's center of gravity will likely prevail in a conflict.[59] Ultimately, hybrid threats attack the center of gravity of western democracies, which tends to be public opinion and national political leadership.[60]

Why Adversaries Will Use Hybrid Warfare

Desert Storm, operations in former Yugoslavia, as well as Afghanistan and Iraq, demonstrated to potential U.S. (and partner) adversaries that attack in depth through precisions fires and fast-moving well-trained maneuver forces can quickly overcome opposing conventional force formations.[61] Adversaries also learned from Afghanistan and Iraq that counterinsurgency operations eventually favor the U.S. and its partners.[62] For both conventional and counterinsurgency operations, the asymmetric advantages provided by U.S. materiel and financial resources, talent, and ideology, have proven too great for our adversaries. However, there is a truism in warfare that countermeasures are always developed to overcome strengths of an opponent, which is why some state and non-state actors will use Hybrid Warfare, or what writers in the People's Republic of China refer to as "Unrestricted Warfare."[63]

Likely Users of Hybrid Warfare

Potential Hybrid Warfare users are self-resourced groups, state-sponsored organizations, and sovereign states.[64] Countries such as Iran, Venezuela, and North Korea are obviously state candidates to apply a Hybrid Warfare approach. However, the problems Hybrid Warfare poses for adversaries make it attractive to any underdeveloped country or non-state actor that values their survival or other critical objectives more highly than the opinion of the international community.[65] A country such as Iran may choose to employ terrorist and cyber elements of Hybrid Warfare as a form of counter-value "mutual assured destruction" in lieu of a nuclear deterrent.[66] State-sponsored groups with presence throughout the world serve as a low-key deterrent threat to those who may employ traditional military capabilities against their supporting regime.

Hybrid War Example: Hezbollah v. Israeli Incursion into Lebanon in 2006

A major impetus for recent writings on Hybrid Warfare stems from the approaches Hezbollah used during the 2006 Israeli incursion into Lebanon. In addition to use of small-unit tactics, Hezbollah employed a number of sophisticated military technologies, including two different types of unmanned aerial vehicles, anti-ship cruise missiles, advanced anti-tank weapons, and rocket systems directed at Israeli civilians.[67] Hezbollah also reportedly conducted signals intelligence against Israeli Defense Force communications.[68] Through a mixture of conventional, irregular, and terrorist tactics, "Hezbollah inflicted more Israeli casualties per Arab fighter in 2006 than did any of Israel's state opponents in the 1956, 1967, 1973, or 1982 Arab-Israeli interstate wars."[69]

Hezbollah politico-military sophistication surprised Israel, and Hezbollah exploited their military actions and Israeli military errors through the power of information.[70] Hezbollah used the internet and sympathetic international media extensively to expand the impact of their military efforts to audiences regionally and internationally. Further, Hezbollah succeeded in blaming Israeli forces for collateral damage against Lebanese civilians to draw international criticism against the Israeli government.[71] While those in many other countries had thought Israel was justified at the incursion's start, as audiences "saw images of [Lebanese] civilian casualties (both doctored and real) . . . the tide of public opinion turned."[72] Hezbollah's information efforts were compounded by Hezbollah's diplomatic efforts. [73] In the end, "the Israeli local and international media and diplomatic effort was good but totally outclassed."[74]

The result of Hezbollah’s military, informational, and diplomatic efforts was “perceived moral legitimacy of purpose and behavior” in that Hezbollah was seen by many “as the defender of the Lebanese people.”[75] The totality of Hezbollah efforts allowed their narrative to defeat the Israeli narrative. That perceptual victory became reality, allowing Hezbollah to maintain the status quo in spite of the damage they took on the battlefield.[76]

Hybrid War Example: Russia v. the Republic of Georgia in 2008

Another recent variant of Hybrid Warfare occurred during the September-October 2008 armed conflict between Russia and Georgian South Ossetian separatists, and the Republic of Georgia. This conflict resulted from a long history of friction between ethnic Georgians and ethnic Russians in South Ossetia, and from Russian sponsorship of South Ossetian separatists.[77] Russia employed a variety of efforts, including insurgent surrogates in politically-contested South Ossetia, cyber attacks against Georgian military and economic targets, as well as physical attacks on some economic targets.[78] Aware of the potential negative strategic impact of the world seeing Russian tanks attacking Georgian forces, Russia limited its use of conventional military in Georgia beyond South Ossetia.[79] Russia also used Chechen mercenaries that had previously fought against Russia in Chechnya, men who were “brutal fighters, their reputation no doubt instilled fear and intimidation on the populace and thus ensured compliance” of South Ossetians loyal to the Georgian government.[80]

Within Russia, the Russian government used its control over the media to shape public perception over the incursion and even “exploited western military equipment captured from the battlefield” to bolster its narrative that “the Republic of Georgia was a surrogate for the US [sic] to test Russia.”[81] Russia also made use of visual information of humanitarian assistance from Russian soldiers to civilians in South Ossetia.[82] In addition to cyber attack, Russia used electronic warfare jamming against Georgian forces communications, and also used unmanned aerial vehicles to disrupt global positioning system signals.[83] Through use of hybrid techniques of surrogate attacks and propaganda, Russia was successful in cementing the secession of South Ossetia from Republic of Georgian controlled territory.[84]

Why IO Needs to be Applied Differently to Hybrid Warfare

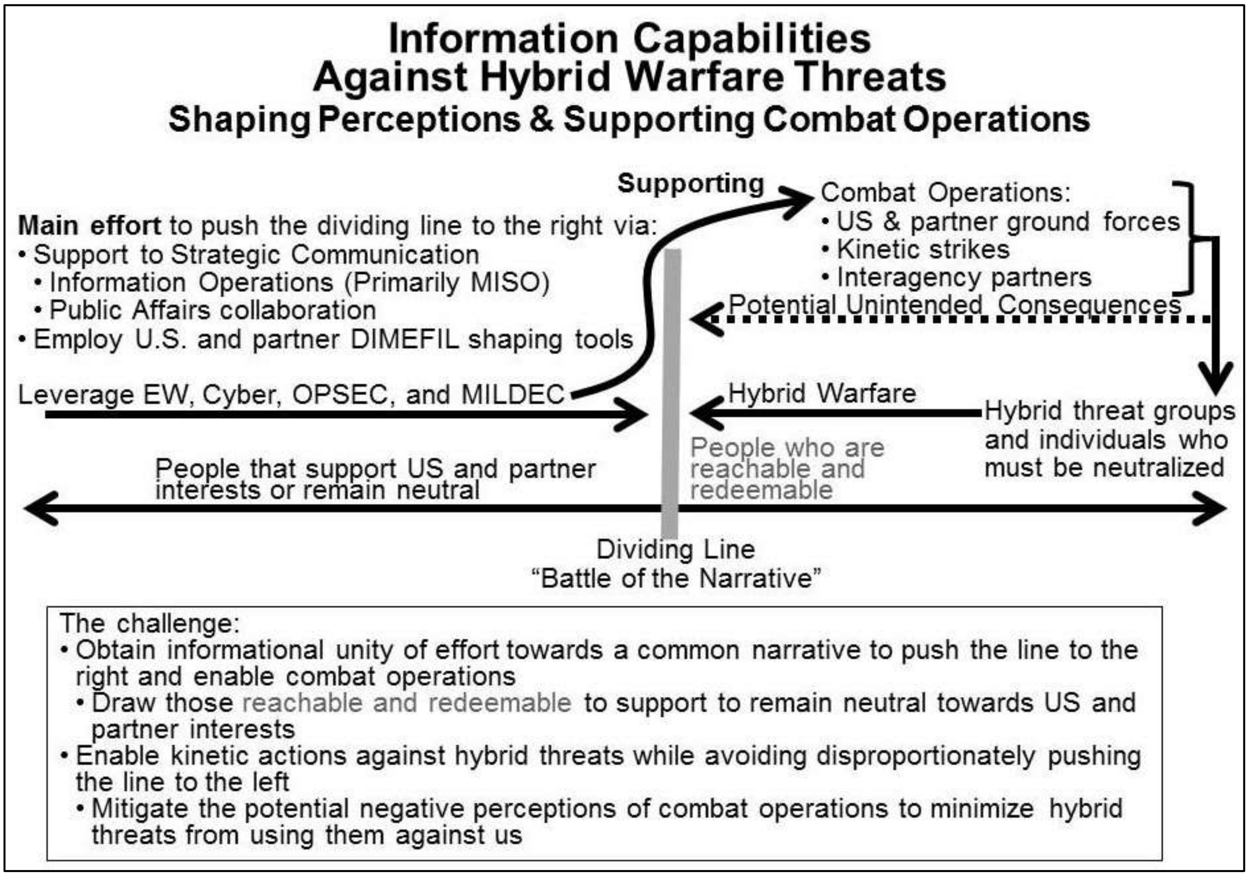
As Sun Tzu counseled, a strategy should "attack the enemy's strategy," and this holds true when either attacking or defending against an adversary.[85] Hybrid Warfare attacks elements of an opponent's national power to convey an informational narrative that serves to defeat the opponent's will to continue military conflict.[86] As Hybrid Warfare threats attempt to use public opinion and political will within democracies, it is imperative to deprive hybrid forces of the opportunity to use information against us. Thus combatting hybrid threats requires extensive U.S. Interagency collaboration and integrated employment of military IRCs.[87]

We must also accurately shape the context of conflict against hybrid threats to expose their sinister methodologies, and degrade the hybrid threat's information capabilities. Since hybrid warfare attempts to defeat a nation's will, a comprehensive information effort is necessary to: generate effects for military operations; attack the hybrid adversary's will; isolate the adversary diplomatically; and maintain international support for the overall military campaign. Although analysts of Hybrid Warfare vary on what it may entail, there is general agreement that the U.S. military (and government as a whole) must adapt to be able to respond to hybrid threats.[88] Given that the focus of Hybrid Warfare is fostering a compelling narrative, combating that narrative requires planning all operations through an IO lens and carefully integrating IRC integration in support of our narrative and combat operations.

Applying IO against Hybrid Warfare

The plan for information-related capabilities must nest with the overall national and strategic military effort to meet long-term policy goals. The military effort should not be focused on short-term policy goals. A theoretical example for an Israeli problem is shaping conditions to motivate Hezbollah to eschew terrorism and rocket attacks against Israel, rather than attempting to destroy Hezbollah's military capabilities at a point in time. Just as enthusiasm is not a substitute for capability, or ideology a substitute for strategy, military capability or corresponding information capability is not a substitute for good policy behind a useful and compelling narrative.

In some cases, information related capabilities (IRCs) are a main effort, such as promoting the U.S. or coalition narrative while combating the Hybrid Warfare adversary narrative. In other cases, IRCs are a supporting effort, such as Electronic Warfare jamming against adversary communications to degrade their tactical coordination; cyber actions against adversary computer networks; or MISO broadcasts to motivate civilians to avoid Hybrid Warfare forces to mitigate the potential for civilian casualties. Therefore, IO planning and execution integration ensures that IRCs support CJTF and national objectives to the maximum extent possible, and minimizes information fratricide. Figure 1 illustrates how the U.S. should employ IRCs against hybrid threats. We should use IRCs to advance our narrative to draw those adversaries who are reachable and redeemable to support our interest or at least become neutral. The figure also describes how IRCs may support combat operations necessary to neutralize hard-core hybrid threats. The ultimate goal is to push to the right the grey line dividing the battle of the narrative to achieve a lasting peace.


Information Capabilities
Against Hybrid Warfare Threats
Shaping Perceptions & Supporting Combat Operations
Supporting
Combat Operations:
• US & partner ground forces
• Kinetic strikes
• Interagency partners
Main effort to push the dividing line to the right via:
• Support to Strategic Communication
• Information Operations (Primarily MISO)
• Public Affairs collaboration
• Employ U.S. and partner DIMEFIL shaping tools
Potential Unintended Consequences
Leverage EW, Cyber, OPSEC, and MILDEC
Hybrid Warfare
Hybrid threat groups and individuals who must be neutralized
People that support US and partner interests or remain neutral
People who are reachable and redeemable
Dividing Line
"Battle of the Narrative"

The challenge:
- Obtain informational unity of effort towards a common narrative to push the line to the right and enable combat operations
  - Draw those reachable and redeemable to support to remain neutral towards US and partner interests
- Enable kinetic actions against hybrid threats while avoiding disproportionately pushing the line to the left
  - Mitigate the potential negative perceptions of combat operations to minimize hybrid threats from using them against us

Figure 1. Information Capabilities Against Hybrid Warfare Threats

Organizing IO for Hybrid Warfare

National-Level Structural Issues Affecting Strategic Communication and IO

The U.S. Department of State (DoS) is responsible for public diplomacy and most strategic communication to foreign audiences.[89] With guidance from the White House and in coordination with the National Security Staff, State sets the tone for U.S. strategic communication to foreign audiences. For decades the U.S Information Agency had the lead for this effort, but Congress passed legislation to disestablish it in 1999 at the behest of the Clinton Administration and its functions were absorbed within the State

Department.[90] In so doing, "the U.S. unilaterally disarmed itself in the area of public diplomacy."[91] Several authors have noted that the problem with the current structure is that "there is no real evidence that the State Department has either the vision or the will to conduct effective public diplomacy."[92] Even if they had the vision and will, the State Department is not manned or funded to conduct extensive public diplomacy, nor is there a solid directive function (beyond the bureaucratic interagency process) within the U.S. National Security Staff to synchronize messaging efforts across the U.S Government towards any audience.[93] As an example, the Broadcast Board of Governors which oversees the content of Voice of America, Radio Free Europe, Radio Free Asia and other U.S.-Government sponsored media broadcasts, although ostensibly a government entity, does not directly respond to U.S Government control.[94] As Stephen Biddle and Jeffrey Friedman write, "major changes in the interagency process would be needed to replace a balkanized, slow-moving decision making system with one agile and integrated enough to compete effectively with politically nimble, media savvy opponents in portraying the results of such [hybrid] warfare persuasively to public audiences."[95] Several authors have developed recommendations to solve this dilemma, though enumerating them is beyond the scope of this paper.

Overall U.S strategic communication efforts have improved over the last ten years; however there is still room for progress in IO and strategic communication coordination.[96] On 28 November 2012, the Assistant Secretary to the Secretary of Defense for PA released a memorandum replacing the term "strategic communication" with "communications synchronization."[97] Subsequent media reporting indicates this memorandum and related policy change was not coordinated with other elements of the

Office of the Secretary of Defense, and it remains to be seen if this change in terminology will last.[98] While the terminology change may be useful in aligning DoD messaging efforts, the fact that DoD did not internally coordinate the name change indicates the difficulty in coordinating the content of strategic communication. Within the uniformed portion of the DoD, successful coordination of IRCs towards disseminating a strategic narrative is largely contingent upon command emphasis and the talent of IO and PA officers.[99] Unfortunately, that talent is uneven.[100] While addressing these issues is also beyond the scope of this paper, multiple authors have written on these topics (as found in the endnotes to this paragraph).

Military IO Organization

Although current U.S. policy no longer includes capabilities within the IO definition, aligning capabilities within a construct makes IO easier to understand, particularly for non-practitioners.[101] IO is integrated within military units through existing staff processes, including IO and Communication Strategy Working Groups. It is useful to group capabilities based on the principal effects they generate.[102] These theoretical categories are Information Activities, Signature Control, and Cyber Electromagnetic Activities. These IRC groupings represent functional collaboration rather than organizational grouping. As will be discussed later, there are many reasons to preserve the traditional separation of some IRC elements.

Information Activities and the support they provide to U.S Government strategic communication are the most critical IO function against the central Hybrid Warfare threat: overcoming the adversary narrative. Information Activities are focused on message content and to a lesser degree the means to disseminate messages. The military IRCs that make up Information Activities are MISO, PA, and to a lesser degree

Key Leader Engagement. Some military Information Activities focus on operational-level effects, such as encouraging civilians to depart the immediate conflict area. However, the overall messaging effort must also support national (U.S. and coalition) objectives and guidance, such that military IRCs should reinforce DoS Public Diplomacy efforts.[103]

Audiences must believe information sources are credible or the information will have little impact, and may even be counterproductive.[104] The credibility of the messenger is essential to make the narrative believable.[105] While neither public law nor policy preclude false message content to foreign audiences, virtually all MISO messages are based on truth so that MISO message content is credible and therefore effective. The mere theoretical possibility that MISO messages could be false degrades their effectiveness with some audiences.[106] The erroneous assumption that MISO and other IO efforts are inherently deceptive generates suspicion among journalists and the general public, and results in tension between the military PA, IO integration, and MISO communities, both within the United States and internationally.[107]

Public Affairs personnel must be trusted to be effective and association with MISO or IO personnel tend to taint PA in the eyes of journalists.[108] Despite the problems over perception of PA affiliation with IO and MISO personnel, over the last ten years there have been instances where the staffs were combined.[109] Integrating PA, IO, and MISO functions into a single staff section, intended to both inform and influence, makes sense from an effectiveness standpoint but combining IO and PA functions damaged the credibility of PA and has drawn criticism.[110] Collaboration is absolutely essential; however, the criticism drawn by combining IO and PA staffs is distracting, ultimately counterproductive, and perhaps even institutionally dangerous.[111] Likewise, using IO personnel as spokespeople to journalists has also resulted in negative consequences.[112] The credibility of the U.S. military is already handicapped in some parts of the world because of distrust of the U.S., distrust of any militaries, or both. Further degrading that trust through contentious organizational structure is therefore a bad approach that is easily avoided by keeping the PA staff separate from the IO (and MISO) staff. It is imperative that PA maintains the public trust. Media engagement facilitated by PA is critical to inform U.S. and partner country audiences, and thereby protect the friendly center of gravity when confronting hybrid threat propaganda.

There have been efforts within the Army towards making the IO staff solely responsible for Key Leader Engagement. Employing the IO staff to orchestrate Key Leader Engagement with U.S. Government officials is unwise, as it may appear the military is directing its influence capability towards the legislative branch, which could be interpreted as a violation of the U.S. Smith-Mundt Act of 1948.[113] Even if interpreted within the U.S. government as legal, it may still be seen by many as inappropriate. This results in the same dilemma as that of combining the PA and IO functions, and can be avoided by not using IO personnel for KLE efforts to U.S. and partner-nation leaders.[114]

The second IRC category is Signature Control, which encompasses OPSEC and MILDEC, and involves shaping the observable and otherwise detectable (e.g., radio) signatures of CJTF elements. Through close collaboration between the OPSEC and MILDEC, the aspects of each become mutually supporting, and facilitate their integration during planning and execution. As a mental model, the concept of Signature Control focuses efforts to shape adversary leaders' and fighters' perceptions of our force capabilities and potential actions to our advantage. The purpose of Signature

Control is not to mislead U.S. or partner publics, and does not directly support the battle of the narrative. However, the positive effects from Signature Control directly support combat operations, and therefore indirectly strengthen our narrative.

The third IRC category is what the U.S. Army now describes as “cyber electromagnetic activities” (CEMA), which is a combination of Cyber and Electronic Warfare.[115] However, the relationship between cyber and EW must be carefully considered. Cyber capabilities and EW are “different physically, doctrinally and technologically, yet simultaneously interdependent.”[116] That said, both are planned and synchronized primarily during the joint targeting process. Both rely on technical data provided by intelligence sources, and an understanding of the interrelationships between the nodes in the system in which they operate, to produce targeting recommendations. Both are also capable of generating effects by themselves, as well as serving as a delivery means for MISO. The focus of CEMA may be as much to support combat operations rather than directly enable the narrative, though like Signature Control, their value to the overall operation indirectly enhances the narrative. Regardless of how the IRCs are organized, they must be fully integrated during all phases of military operations. Figure 2 displays a way to conceptualize the IRCs.

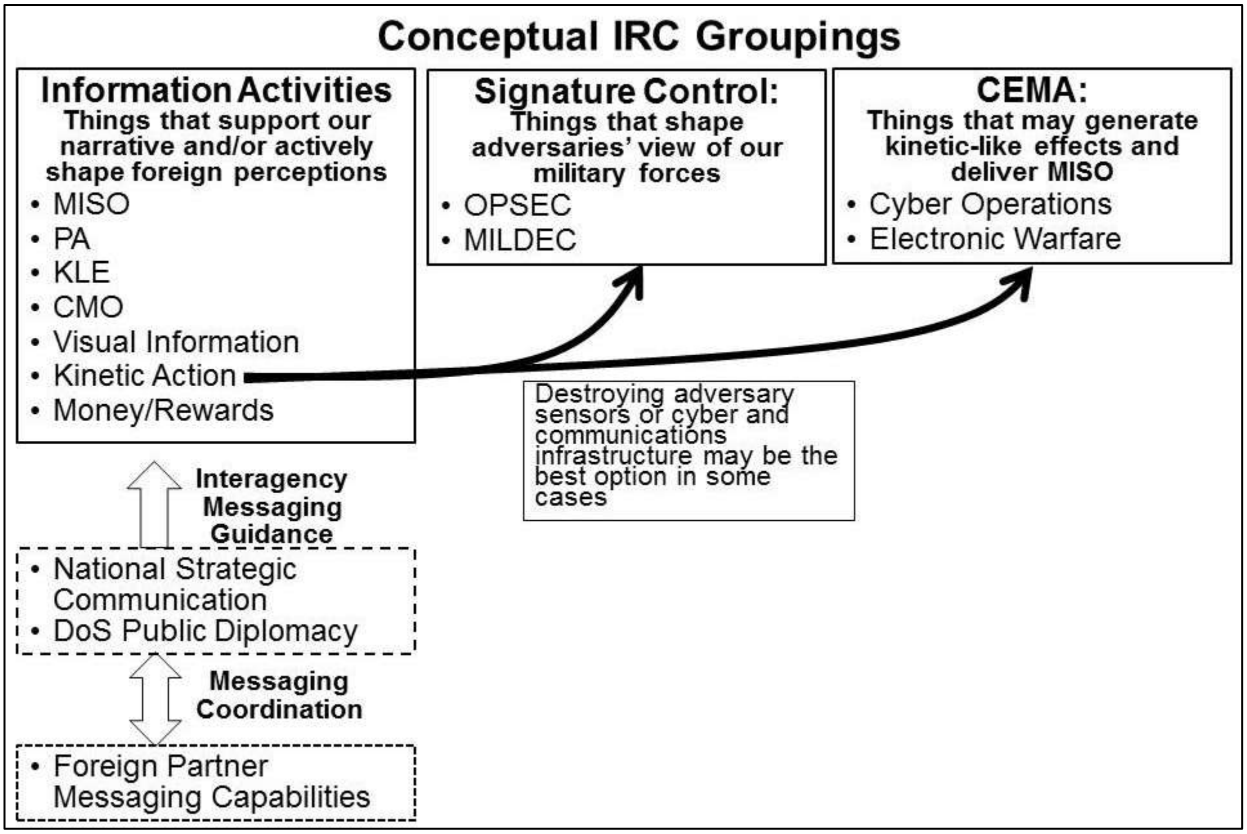

Conceptual IRC Groupings
Information Activities
Things that support our narrative and/or actively shape foreign perceptions
• MISO
• PA
• KLE
• CMO
• Visual Information
• Kinetic Action
• Money/Rewards
Signature Control:
Things that shape adversaries' view of our military forces
• OPSEC
• MILDEC
CEMA:
Things that may generate kinetic-like effects and deliver MISO
• Cyber Operations
• Electronic Warfare
Destroying adversary sensors or cyber and communications infrastructure may be the best option in some cases
Interagency Messaging Guidance
• National Strategic Communication
• DoS Public Diplomacy
Messaging Coordination
• Foreign Partner Messaging Capabilities

Figure 2. Conceptual IRC Groupings

Shaping and Deterrence (Phase 0 and Phase I)

The Chinese military theorist Sun Tzu coined the maxim that "[t]o subdue the enemy without fighting is the acme of skill."[117] Army Doctrinal Publication 1 discusses "[s]haping the strategic security environment".[118] Those concepts are combined in the notion of shaping the adversary and shaping the operating environment where conflict is likely to occur.[119] The purpose of shaping the thoughts of the adversary and the environment is to create conditions where military victory is essentially assured prior to the onset of hostilities.[120] Shaping is always important, but it is particularly critical in deterring and setting conditions for success against Hybrid Warfare threats. Some specific aspects of shaping, particularly as it might apply to hybrid threats, comes in the form of “preparation of the environment.”[121] Since Hybrid Warfare threats use their narrative as a strategic weapon, the U.S. must promulgate its narrative and combat any given hybrid threat narrative. The U.S. diplomatic and military presence across the globe provides an asymmetric advantage to reach foreign audiences. U.S. Geographic Combatant Commands (GCCs) use their Theater Campaign Plans to orchestrate shaping activities, and theoretically set the theater to enable effective contingency plans and operations. This system of GCC planning can be useful to orchestrate IO and IRCs to deter potential hybrid threats, and set conditions to defeat them if necessary. In so doing, the military can support overall U.S. Government efforts to align messages and disseminate them in a synchronized fashion, using the most comprehensive and appropriate means, to the correct audiences, to maximize the impact of our narrative efforts.[122]

The key IO-related components of shaping are: (1) building and coordinating the U.S. narrative regarding the likely Hybrid Warfare conflict areas; (2) clearly enunciating the ramifications of irregular, terrorist, and cyber attacks against the U.S. and its interests; (3) establishing comprehensive information conduits into potential conflict areas; (4) collaborating with joint, interagency, intergovernmental, and multi-national partners; (5) shaping the context of unforeseen events and; (6) the cyber role of cyber shaping. Each is discussed below.

Coordinate the U.S. Narrative Regarding Hybrid Warfare

State Department policy developers and public diplomacy specialists have developed issue papers that supply strategic narratives. These documents are available on the unclassified State InfoCentral internet portal.[123] DoD and DoS collaborate on messaging towards select regional flashpoints to prevent armed conflict (hybrid or otherwise). We need to expand the catalog of narratives as well as improve interagency coordination on disseminating the narratives. U.S. Special Operations Command (SOCOM) undertook coordination to develop strategic communication material in support of the DoD Global War on Terrorism plans developed by SOCOM in the mid-2000s.[124] Additionally, SOCOM-funded Military Information Support Teams are assigned to multiple U.S. Embassies.[125] “Synchronized with embassy goals and objectives and with Country Team oversight, the teams help to articulate USG messages by informing, clarifying and persuading foreign audiences.”[126] These teams could provide critical assistance in disseminating a strategic narrative regarding Hybrid Warfare threats as part of both shaping efforts and during an armed conflict against adversaries.

Clearly Enunciating the Ramifications of Irregular, Terrorist, and Cyber Attacks

The U.S. Government should clearly enunciate the ramifications of irregular and cyber attacks against the U.S. and its interests, just as it has made unambiguous statements regarding threats to national security from terrorism and nuclear, chemical, and biological attack.[127] As part of overall shaping activities to combat future hybrid warfare, U.S Government strategic messaging efforts should proactively denigrate and delegitimize irregular and terrorist aspects of hybrid warfare as well as its practitioners. Such statements are required as a separate narrative with the intent to deter and dissuade hybrid threat actors, and explain likely U.S. responses to hybrid attacks.[128] Such shaping may have little impact on those intending to engage in irregular or terrorist tactics, even if we explicitly state what adversary strategic assets we hold at risk. However, proactive messaging sets the context for the U.S. response to Hybrid Warfare, as well as the consequences for those who choose to engage in it (e.g., being labeled and liable as a war-criminal, or becoming subject to capture or kill operations).

Attacks through terrorism, cyber, or other means against solely civilian infrastructure are generally regarded as outside of the scope of the internationally recognized laws of armed conflict (LOAC). The internal political calculus of hybrid warfare users may discount the penalty from being perceived as a LOAC violator. Evidence of this comes from the thought process of those who employ terrorism, sometimes successfully. As conflicts often begin with miscalculation, the U.S. narrative should caution potential adversaries that Hybrid Warfare attacks affecting U.S. civilians may be counter-productive, inciting the type of national fervor for retribution (regardless of cost) that followed the attacks of December 7, 1941, and September 11, 2001.

Establish Information Conduits

Throughout much of the world, people increasingly receive information from multiple sources.[129] It is necessary to employ all conceivable forms of communication to reach audiences in the conflict area and to permeate the information environment. This includes radio, television, print media, billboards, internet (webpages, weblogs, & emails), telephone messages (robot calling using equipment identical to that used in U.S. and foreign political campaigns), as well as DVD and CD formats, and where possible, face-to-face (KLE) communication with influential members of the local population. Developing these conduits requires extensive IO preparation of the environment to determine what conduits are most effective for various audiences. This preparation must include establishing the commercial contracts to obtain the necessary talent for product development and dissemination (in addition to what can be disseminated by organic MISO resources).

Collaboration to Shape the Information Environment

Effectiveness against hybrid threats requires all instruments of national power.[130] As previously mentioned, these instruments are Diplomatic, Informational, Military, Economic, Financial, Intelligence, and Law-enforcement (DIMEFIL).[131] Employing them successfully requires collaboration among Joint, Interagency, Intergovernmental, and Multinational (aka JIIM) partners. No single element of the U.S Government (other than the President) has the legal authority to orchestrate all of these DIMEFIL elements, and as is the case with counter-terrorism efforts, countering against hybrid threats requires multinational resources.[132] However, the military is the only governmental entity with a large number of fully dedicated planners and strategists. To maximize chances for future success, military IO and other planners must coordinate with other elements of government to fully employ DIMEFIL elements towards hybrid threats.

Well in advance of military actions, the U.S. and other countries typically employ non-military elements of national power against adversary countries and non-state actors. These methods include diplomatic and economic actions intended to curb behavior threatening international stability, such as trade or financial sanctions. Potential hybrid adversaries misinform their populations as to why these diplomatic and economic actions have been imposed. The military can and should support public diplomacy efforts to accurately shape the context of U.S. action before and during a conflict. Our messaging should explain the potential future diplomatic and economic ramifications for states and supporters of non-state actors that violate the LOAC during the conduct of Hybrid Warfare. The purpose is less to prevent states or non-state groups from employing Hybrid Warfare as to shape the narrative context of the conflict and its aftermath. Successful historical examples include messaging to the citizens of Germany and Japan following WWII that resulted in significant changes to those countries' world view. Populations within the area of conflict, as well as internationally, must be made to understand that those in the conflict area will be sanctioned by diplomatic and economic means because of their tacit or active support of Hybrid Warfare. The intended result of that understanding is disuse of Hybrid Warfare and a willingness to accept terms the U.S. (or coalition) may offer to resolve the conflict.

Given the media sophistication of hybrid threats, shaping the information environment to deter and combat those threats requires a concomitant high degree of messaging sophistication. MISO products and other forms of support to strategic communication should include long-form video and audio products for dissemination via the information conduits discussed previously. Some potential hybrid threats could employ pseudo-legal rationale for their actions, requiring the U.S. to incorporate sound legal reference as part of our narrative. Culturally astute tailored messaging is expensive but essential, which in an austere budget environment should motivate collaboration between DoD, DoS, and other interagency partners, as well as foreign partners where practical.

Another important aspect of shaping is the development of partner-nation IRCs. Partner-nation messaging is often perceived as more credible by those in the conflict area (as opposed to a U.S. MISO effort). A potential result of that credibility is superior effectiveness of partner-nation messaging efforts. Partner-nation messaging efforts are also generally cheaper to produce. Therefore, it can be both more effective and cost-effective to develop and support IO and PA training for partner government and security officials. This will enable them to combat a given hybrid threat narrative locally. Other resourcing assistance could include facilitating partner-nation IRCs (such as radio stations or internet-access points to locations where the population has limited access to information). These efforts are particularly appropriate during Phases 0, I, and IV of military operations. Care must be taken to develop a set of IRCs tailored to the partner country's needs as opposed to cloning U.S. IRCs, as this would degrade the advantage that native IRCs possess.

Shaping the Context of Unforeseen Events

Unplanned events result from nearly every planned military action. IO staffs at all levels should anticipate and plan for events that must be mitigated or could be exploited. The U.S. does not deliberately target civilian or other non-combatants, but some degree of collateral damage is inevitable in any armed conflict. Continuous touting of our precision strike capabilities sets a very high expectation that no collateral damage will occur. Despite all of our efforts, collateral damage will occur due to weapon failure, target misidentification, target coordinate error, or because Hybrid Warfare actors intentionally co-locate with civilians with intent to either shield themselves or increase likelihood of civilian casualties in support of their narrative.

As part of their overall "battle of the narratives" strategy, Hybrid Warfare adversaries exploit civilian collateral damage and other unintended consequences of CJTF military action. To combat that strategy, proactive messaging plans must be prepared by, and coordinated between, IO and PA staffs in advance of military action. IO practitioners should work to set collateral damage and other negative unplanned events in the context of conditions precipitated by Hybrid Warfare users. Some tactical-level events may have international strategic significance and must be coordinated with troop-contributing nation command elements for action or awareness by the U.S. and partner-nation governments. The CJTF IO staff should also exploit actions by hybrid threat forces against civilians and other actions that violate international norms. For example, the IO staff should demonstrate the hypocrisy of, and therefore delegitimize, the narrative used by Hybrid Warfare forces.

Events requiring mitigation or exploitation include: Collateral damage against civilians and/or civilian infrastructure; acts of terrorism in areas held by CJTF; significant combat losses, or lost vessels, aircraft, or other key assets; missing service members presumed captured by irregular forces; friendly forces fratricide incidents; localized humanitarian challenges that receive international media attention; major combat successes such as capture or destruction of adversary units, assets, or leaders; and any other single event that captures regional or international media attention.[133]

Although this type of planning often occurs at the operational and tactical level, the results of the planning support must be consonant with strategic messaging guidance. While all contingencies cannot be foreseen, most events fall into one of the above specific categories, such that the CJTF IO staff (in conjunction with MISO and PA elements) should prepare general “talking points” to accurately shape the context of how such an event occurred, and the way ahead in its aftermath. An example would be explaining how a hybrid force’s use of hostages resulted in civilian casualties. Failing to adequately plan for the aftermath of events can result in severe strategic consequences. Figure 3 displays how an IO staff can work with PA and MISO elements to develop talking points for incorporation into planned operations and in reaction to un-planned (but almost inevitable) events.

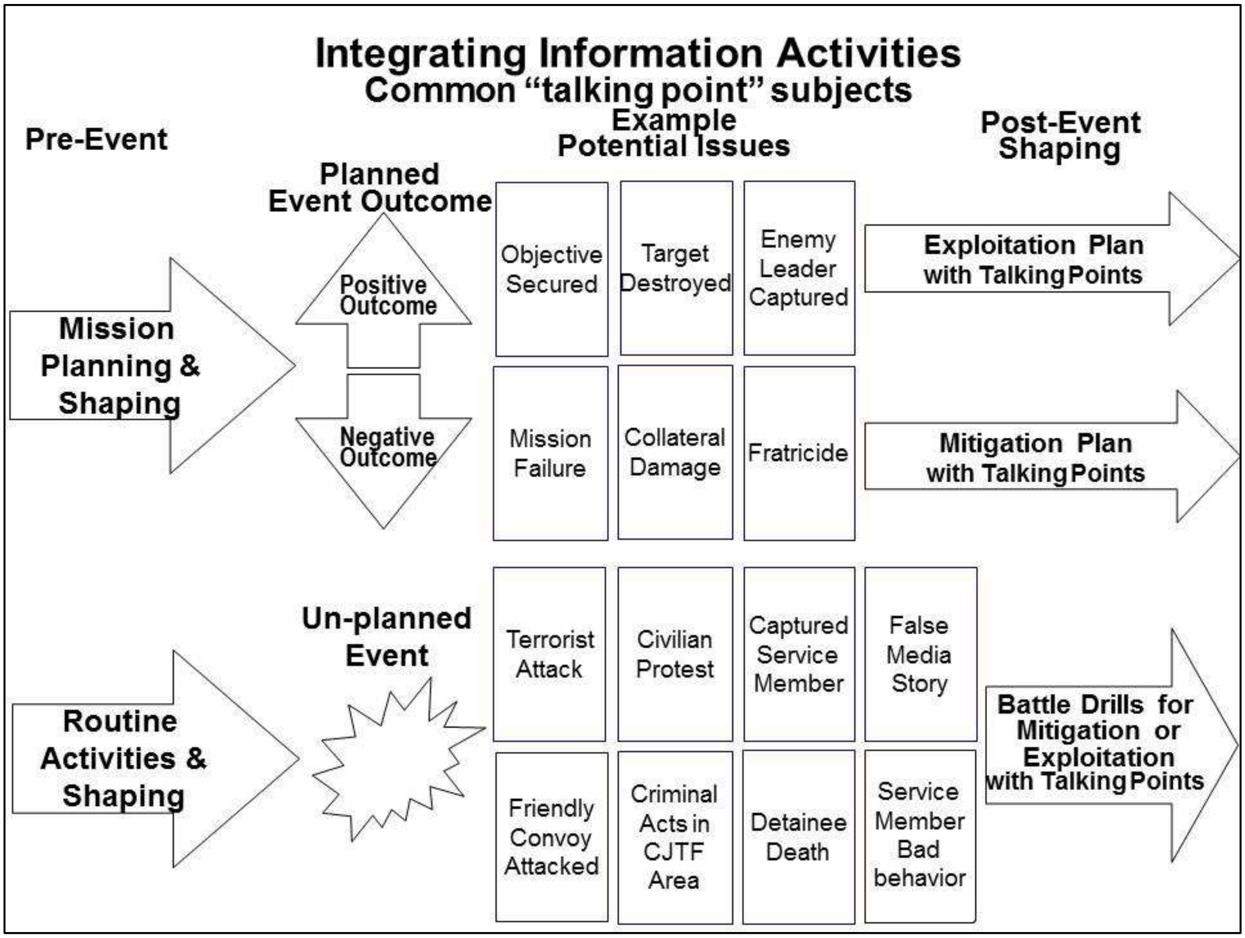


Figure 3. Integrating Information Activities and Common Talking Point Subjects

During subsequent phases of an operation, significant event mitigation or exploitation must be executed as a well-rehearsed process, or "battle drill,"[134] closely coordinated by the IO, PA, Staff Judge Advocate, and current operations staffs, in conjunction with counterparts in component units. An example would be in inadvertent civilian casualties resulting from a precision-guided weapon malfunction, requiring explanation to multiple audiences and outreach to the affected community. Another example would be a false media report of CJTF-caused civilian casualties, requiring the CJTF to transport media members to site to prove the event did not occur. The facts that form the basis of the talking points come from tactical units subordinate to the

CJTF, but the truthful facts must be standardized in talking points, as uncoordinated messaging on the same event may result in perceived contradictions and thus the truth may appear false.[135] Leaders at all levels should use the same talking points to discuss the events with appropriate audiences through “key leader engagement,” as well as to assist development of MISO products regarding the event. The PA staff will also likely develop a media release or response to query that contains the same facts as those in the talking points. Synchronizing dissemination of facts regarding significant events and anchoring those events in the context of the overall operation fosters messaging harmony, aids credibility, and minimizes the likelihood of harmful miscommunication regarding the event. Depending on the significance of the event, the talking points may be developed by the CJTF IO staff, or in the components’ headquarters, or result from directive guidance from troop contributing nation command elements. Figure 4 illustrates how raw tactical reporting of an event, such as an incident that created collateral damage, can be transformed into messaging aligned for dissemination by multiple means to local, regional, and global audiences.

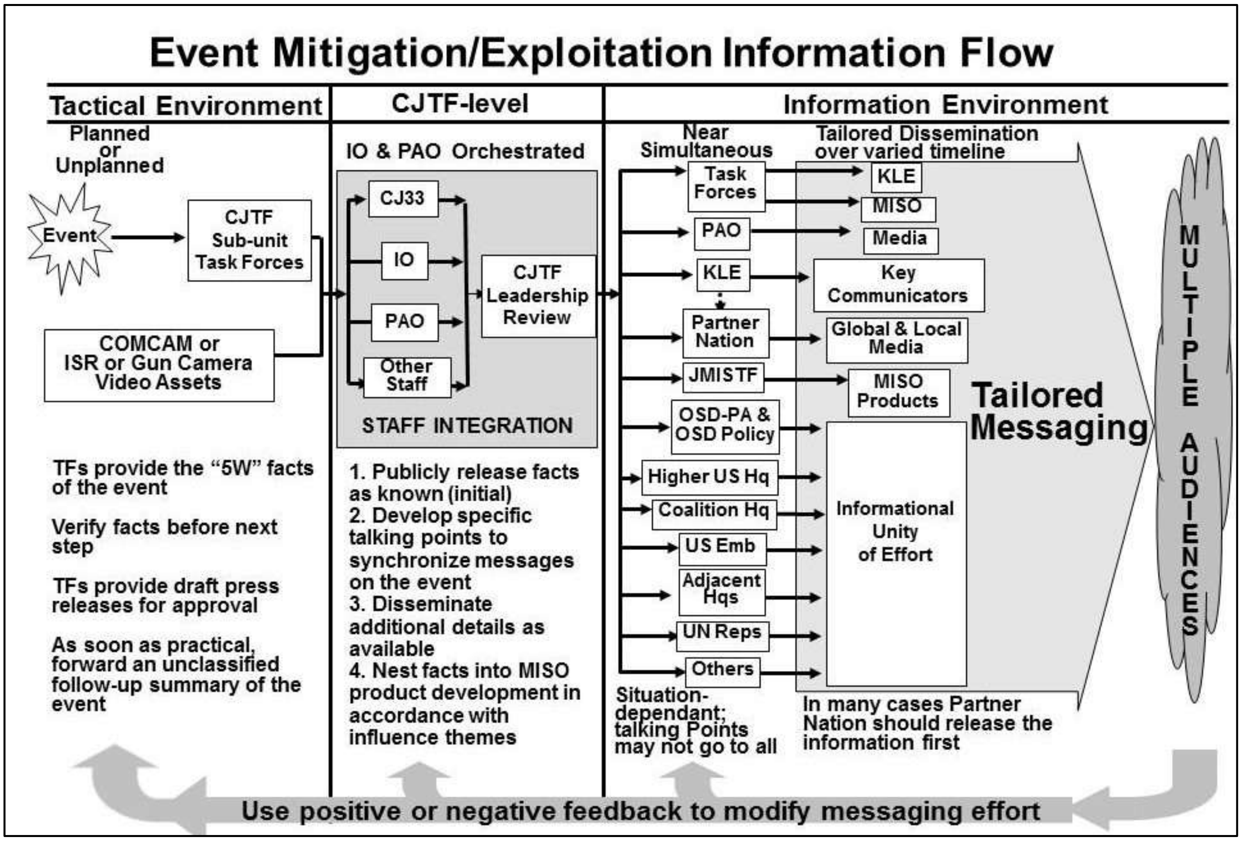

Event Mitigation/Exploitation Information Flow
Tactical Environment
CJTF-level
Information Environment
Planned or Unplanned
Event
CJTF Sub-unit Task Forces
COMCAM or ISR or Gun Camera Video Assets
TFs provide the "5W" facts of the event
Verify facts before next step
TFs provide draft press releases for approval
As soon as practical, forward an unclassified follow-up summary of the event
IO & PAO Orchestrated
CJ33
IO
PAO
Other Staff
CJTF Leadership Review
STAFF INTEGRATION
1. Publicly release facts as known (initial)
2. Develop specific talking points to synchronize messages on the event
3. Disseminate additional details as available
4. Nest facts into MISO product development in accordance with influence themes
Near Simultaneous
Task Forces
PAO
KLE
Partner Nation
JMISTF
OSD-PA & OSD Policy
Higher US Hq
Coalition Hq
US Emb
Adjacent Hqs
UN Reps
Others
Situation-dependant; talking Points may not go to all
Tailored Dissemination over varied timeline
KLE
MISO
Media
Key Communicators
Global & Local Media
MISO Products
Informational Unity of Effort
Tailored Messaging
In many cases Partner Nation should release the information first
MULTIPLE AUDIENCES
Use positive or negative feedback to modify messaging effort

Figure 4. Event Mitigation/Exploitation Information Flow[136]

Hybrid Warfare actors will use our emphasis precision fires against us when collateral damage does occur through the line that “since the U.S fires are precise, civilian casualties must be intentional.” Therefore, to minimize the appearance of a gap between what we are saying and what we are doing, military leaders and spokesmen should focus public discussion on our deliberate procedures to prevent harm to civilians, and juxtapose that fact with a hybrid threat’s deliberate targeting of civilians.

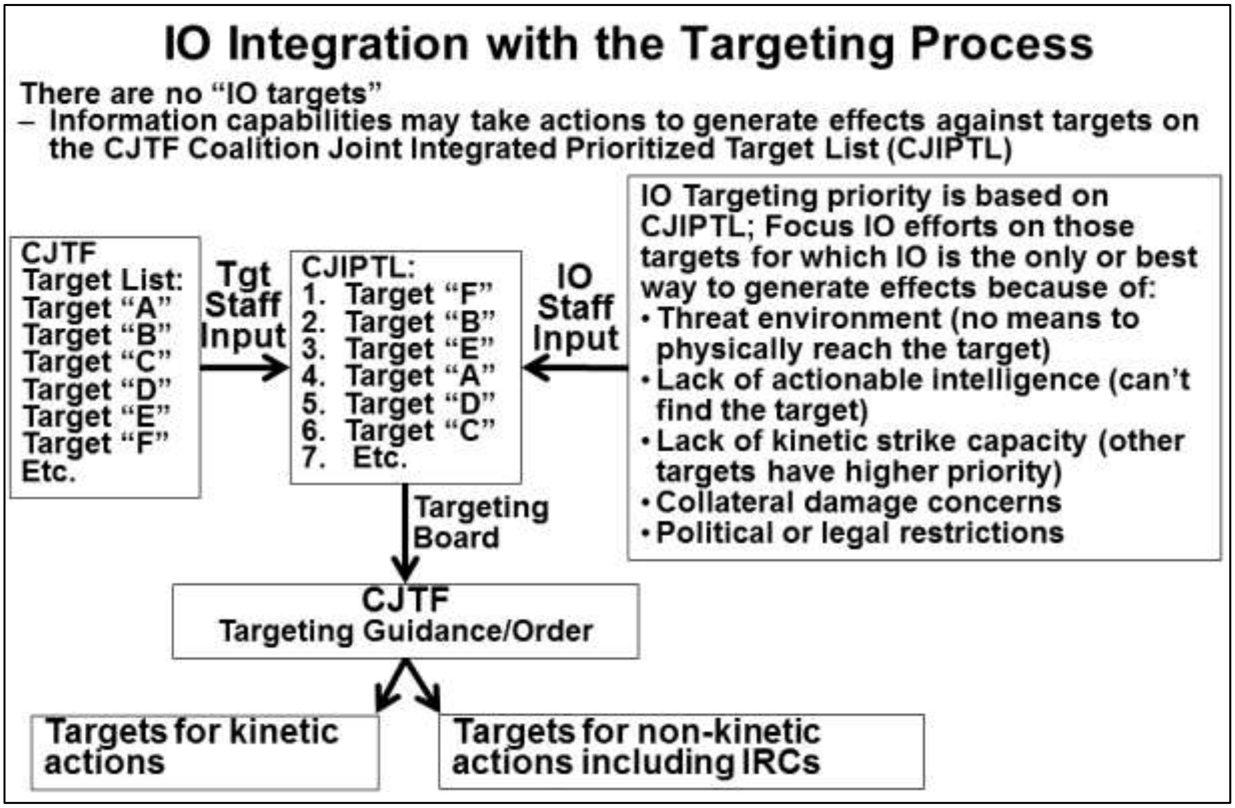
Cyber and Shaping

Most of the discussion of offensive cyber capabilities revolves around its application by a strategic force, which is offensive cyber capabilities employed via the internet from U.S. sanctuary, even when applied to operational or tactical objectives.

However, it is quite possible that this option will not be available when confronting hybrid adversaries. Many countries, including Iran and to a lesser degree China and Russia, maintain digital cocoons around their populations.[137] These countries limit the degree to which outside information can enter. Additionally, as occurred during the civil wars in Libya and Syria, internet access was effectively terminated.[138] Though in both instances it is unclear who was responsible for the disruption, the effect was the same. Not only were the people in those countries cut off from information via the internet but hypothetical access to networked targets was denied (if reliant solely on international internet gateways). There may also be potentially lucrative targets for U.S. cyber operations residing on networks that are inaccessible from the internet.[139] Therefore, generating cyber effects against networks disconnected from the internet requires capabilities to bypass international internet gateways and access closed network systems. Accessing either types of network requires a capability that is employed from within the conflict area (akin to close air support in keeping with the cyber and air-power analogy). Additionally, it may be useful to provide internet access, and thereby access to external information, to populations whose routine access has been cut off by hybrid threats. A CJTF could provide that access via deployable Wi-Fi hotspots, aerostats, or unmanned aerial platforms connected to commercial satellite internet infrastructure. However, the equipment necessary for such deployable public internet capability is not currently in military inventories.

IO Integration During Phase II and III

A key element of how the U.S. conducts combat operations is through the joint targeting process. Some U.S. military officers believe that there are “IO targets” that are somehow separate and distinct from the Joint process.[140] In truth, there are no “IO targets," but instead targets that may be more suitable for action via IRCs.[141] Information capabilities serve as a potential "weaponeering solution" to generate effects against targets.[142] IO staffs at all level should develop and nominate targets for action by IO capabilities in coordination with the Intelligence and Targeting staffs and component or subordinate units. Placing the IO staff within the J3 (Operations) staff facilitates that integration, and empowers the IO staff to task CJTF IRCs, and request IRC support from higher headquarters, under the CJTF Commander's delegated authority (as with other elements of the J3 staff (e.g. J3-Air, J3-Fires, etc.)). CJTFs should employ IRCs to generate effects against targets in accordance with overall targeting priorities. Emphasis for IO capabilities should be to generate effects when kinetic strikes against a high-priority target is constrained (such as targets with high collateral damage potential or where precise target location is unknown) such that the best targeting method may be EW, MISO, or Cyber. Figure 5 displays how IO inputs to the CJTF target list result in a Combined Joint Integrated Prioritized Target List (CJIPTL)[143] that most appropriately applies IRCs to achieve overall CJTF objectives.


IO Integration with the Targeting Process

There are no "IO targets"

– Information capabilities may take actions to generate effects against targets on the CJTF Coalition Joint Integrated Prioritized Target List (CJIPTL)

CJTF Target List:
Target "A"
Target "B"
Target "C"
Target "D"
Target "E"
Target "F"
Etc.

Tgt Staff Input

CJIPTL:
1. Target "F"
2. Target "B"
3. Target "E"
4. Target "A"
5. Target "D"
6. Target "C"
7. Etc.

IO Staff Input

IO Targeting priority is based on CJIPTL; Focus IO efforts on those targets for which IO is the only or best way to generate effects because of:
- Threat environment (no means to physically reach the target)
- Lack of actionable intelligence (can't find the target)
- Lack of kinetic strike capacity (other targets have higher priority)
- Collateral damage concerns
- Political or legal restrictions

Targeting Board

CJTF
Targeting Guidance/Order

Targets for kinetic actions

Targets for non-kinetic actions including IRCs

Figure 5. Integrating IO with the Targeting Process

Although the diagram differentiates between kinetic and non-kinetic actions, it is important to note that kinetic actions can have non-lethal effects, just as non-kinetic actions can have lethal effects. Examples include the U.S. detonating a large and potentially very lethal conventional bomb (such as a BLU-82 or GBU-43 "MOAB")[144] in an unpopulated area for purely informational impact, or an adversary conducting cyber attack that shuts down U.S. electrical systems resulting in the death of hospital patients on life support systems. Additional ways to support CJTF efforts include integrating information activities with kinetic targeting, neutralizing non-state actor's narrative apparatus, cyber integration, as well as protecting ourselves through cyber and communications systems security

Integrating Information Activities with Kinetic Targeting

When the U.S. (or our partners) conducts deliberate strike targeting, we do so with the intent to destroy a known structure or mobile armed force unit for a specific reason that supports the overall operational plan. The same is true for a ground forces raid against a fixed site. When these strikes occur, Hybrid Warfare actors will attempt to cast them in a context that supports their narrative against the U.S. through misinformation provided to journalists or directly disseminated via the internet.[145] Since a CJTF knows why, where, and when it will conduct a deliberate strike or raid, it is possible (and often operationally imperative) to build a completely truthful unclassified information package about the planned event for PA, MISO, and KLE purposes. This information package should be prepared during planning prior to the operation and released immediately after the strike or raid takes place. Announcing the event and why it occurred degrades a Hybrid Warfare adversary's ability to falsely claim that the target was civilian or otherwise illegitimate. This technique should be employed for all targets with high collateral damage estimates, and in some cases it might be strategically prudent to actually announce the event in advance as a warning to civilians in the area. Should there be collateral damage, announcing the strike or raid sets the narrative context of the event, and mitigates claims that it was a random attack (intended to terrorize civilians). Depending on whatever strike or raid damage assessment ultimately occurs, the CJTF should use photos or other visual information to further demonstrate the effects of the event and mitigate adversary disinformation efforts. Figure 6 displays a process of how visual information could flow from where an event takes places to dissemination to audiences.

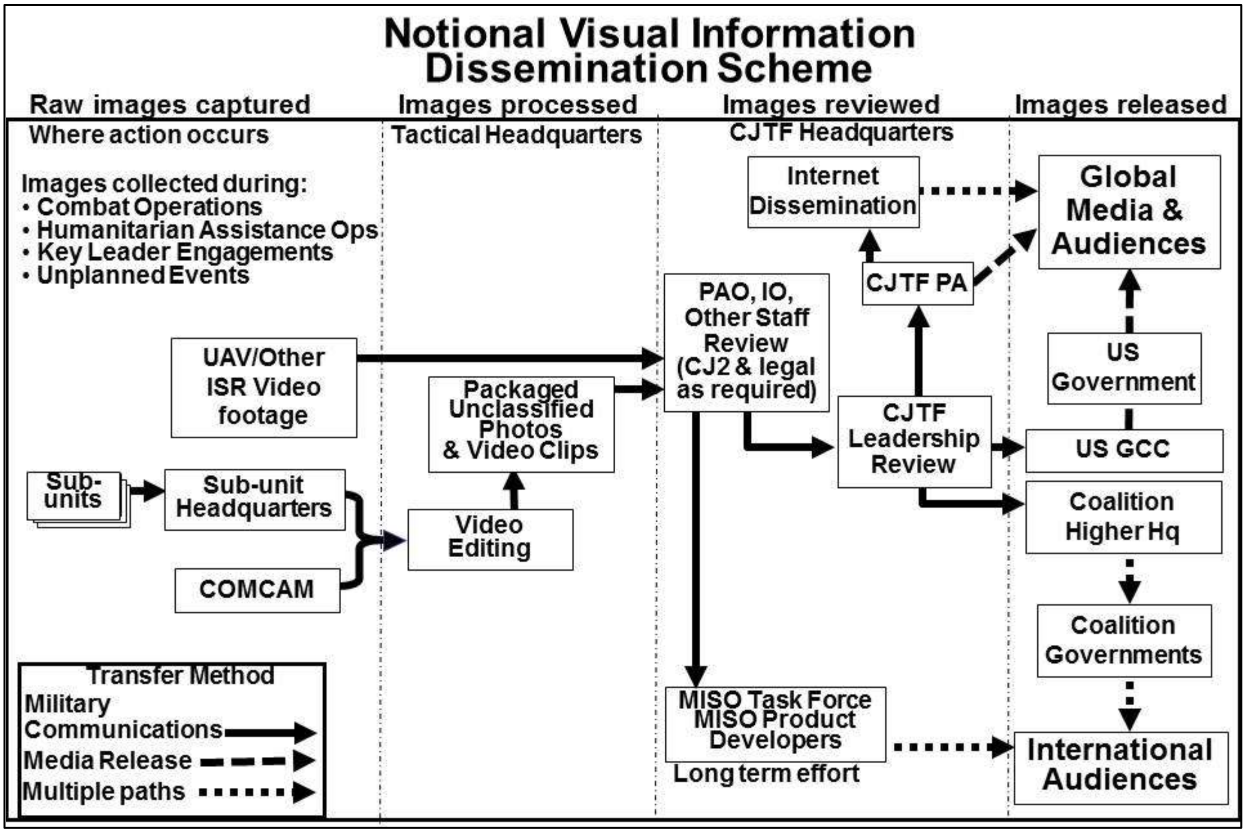


Figure 6. Notional Visual Information Dissemination Scheme

Sometimes the military utility of striking a target or conducting a raid is less significant strategically than the possible negative impact from collateral damage. That reality may not be apparent at the tactical or operational level. Historical examples of U.S. Presidential review of individual military targeting nomination illustrate that the negative impact of collateral damage is clearly understood at the national level. All targets with the potential for high collateral damage should be reviewed through a strategic rather than operational lens to avoid incidents that support the narrative of a Hybrid Warfare force and degrade the legitimacy of the CJTF and the overall U.S. (and coalition) effort.

Hybrid threats will attempt to cast U.S./coalition military actions in a context that supports the overall hybrid threat narrative. Therefore, there are three key themes that will be almost universally necessary at the outset of any military conflict with hybrid threats. The first theme is “why we are involved/.” We must explain the reason for the U.S./coalition military action and/or why there are U.S. ground forces in the conflict area. The second theme is “what we are doing.” We must explain the general U.S./coalition military objectives (e.g. return to status quo ante, security of weapons of mass destruction, humanitarian relief, etc.). The third theme is “when are we leaving.” We must explain the general conditions under which the U.S./coalition will terminate the conflict and/or withdraw ground forces. We need to integrate these three themes into the overall strategic communication and public diplomacy effort, as well disseminated via MISO resources to those in the conflict area and possibly adjacent territory. Failing to clearly enunciate these themes will cede the information initiative to the hybrid threat, generate problems from civilians in the conflict area, likely prolong the conflict, and slow post-conflict transition.

When possible and advantageous to the overall mission, the CJTF should integrate EW disruption of adversary radio communications with MISO messaging to generate both EW and MISO effects on those nodes. Selected disruption of critical adversary communications nodes with MISO broadcasts will assist in isolating adversary conventional forces and surrogates as well as support MISO objectives. As adversary forces are among those that must be targeted by MISO, an effective technique employed in Afghanistan, Iraq, and elsewhere is infusing adversary radio communication networks with MISO messages via electronic warfare systems. An example of MISO messages would be information on how to turn-in particular hybrid threat leaders for monetary rewards, via broadcasts that override hybrid threat tactical radio communications. The technique serves multiple purposes: it directly targets adversary fighters (regardless of what hybrid form they take), and least temporary, it disrupts the adversary's communications. The U.S. Army's Field Manual (FM) 3-36, Electronic Warfare, dated November 2012, makes only two references to MISO, and in both cases briefly mentions deconfliction rather than collaboration.[146] The same is true for the Army's MISO FM.[147] Fortunately, the Joint Publication for MISO discusses the technique in some depth.[148]

Neutralizing Non-State Actor's Narrative Apparatus

When dealing with non-state actors, additional options are available to neutralize their narrative. Promulgation an adversary narrative is composed of three elements, the narrative itself, the means by which it is disseminated, and those who are responsible for its content and dissemination. Thus the U.S. and partner nations must use three lines of effort to neutralize a non-state hybrid threat's narrative. First, we confront their narrative with our own. Second, we must deny or disrupt their dissemination means physically, technologically, or through diplomatic and legal action. While a non-state actor may develop their narrative in ungoverned areas, a large portion of the technical infrastructure on which they rely, such as internet hosting, may be resident in the U.S. or U.S.-partner country. Such infrastructure is potentially subject to legal action or cooperative agreement with commercial enterprises to terminate hosting hybrid threat content, assuming such action is in consonance with the laws of those countries. Third, if possible, we must neutralize through military or law-enforcement means those responsible for developing the hybrid threat narrative, as well as those who orchestrate its dissemination

While the primary method to combat hybrid threat narratives is our messaging, disrupting adversary narrative dissemination may severely degrade their messaging effectiveness and therefore reduce the scope of conflict to a primarily military realm where we have no peer. Failing to address a non-state actor's narrative management and dissemination allows hybrid threat's narrative to perpetuate indefinitely, thereby continuing to foster the threat's pernicious agenda.

This model of attacking all three elements of a non-state hybrid threat's narrative apparatus is generally not fully applicable when confronting a sovereign-state adversary. Attacking a government or commercial information infrastructure within the hybrid threat country may be counterproductive towards our efforts to use that same technology to disseminate our messages to that country's population. Though targeting portions of a hybrid threat's television and radio broadcast equipment might be useful in some areas. Targeting a sovereign nation's propagandists would likely appear disproportional under international law, and the option to use legal means against them, such as the International Court of Justice, is unlikely to have an immediate impact, if any.

Cyber Targeting Integration

The CJTF staff must integrate cyber with kinetic strikes. Targeting staffs identify effects that cyberspace operations could potentially achieve, and integrate offensive cyber capabilities into the CJTF targeting plan. The CJTF staff should both provide its high priority CJIPTL targets through U.S. channels to USCYBERCOM, as well as query

CYBERCOM as to what effects (if any) they can generate in the CJTF area of operation.

There is a predisposition by some cyber subject matter experts to focus solely on symmetrical countermeasures against adversaries (e.g., only employing cyber operations towards cyber attackers). Like many other forms of symmetrical conflict, the result can be unsatisfying. Once a hybrid adversary has obtained cyber attack tools they may launch those attacks from anywhere in the world where there is access to the internet. Therefore, attacking adversary cyber infrastructure may not preclude future attacks. The critical vulnerability of cyber attackers is the humans that conduct the attacks, and so the most effective way to counter cyber attacks is to dissuade or destroy the cyber attackers themselves. This type of asymmetry is converse to using cyber attacks against military weapons systems, and represents a targeting philosophy described by one IO professional as “bomb the hackers, and hack the bombers.”[149]

The U.S. Department of Justice (DoJ) now intends to indict those responsible for cyber attacks.[150] This is a useful “asymmetric” step against hackers, likely intended as much to deter attacks as to result in successful prosecutions. Similarly, the DoD should announce that those foreign civilians responsible for cyber attacks against certain U.S. targets are unlawful combatants, and therefore potentially subject to physical attack by U.S. forces during military operations.[151] Civilian cyber attackers would come to know they lose their status as protected individuals if they disrupt U.S. infrastructure or commerce, or if they significantly degrade military operations. Even more so than a legal indictment, designating foreign civilian cyber attackers as unlawful combatants is likely to deter some of them, as well as shape the context for military strikes against them during future conflict. For those whose personalities draw them to cyber warfare rather than physical combat, a future subject to air strikes or ground-forces raids would likely be a powerful deterrent.

Some in the U.S. intelligence community argue that the effect of using potential U.S. cyber capabilities against adversary cyber attackers or adversary websites will be short, as adversaries can quickly shift to using other cyber infrastructure (a “hydra” effect). Members of the intelligence community have likened such effort to the children’s game of “Wack-A-Mole,” whereby a player attempts to strike the head of a mechanical mole only to find the head immediately pop up elsewhere in the game machine. Regardless, repeatedly suppressing the adversary cyber “moles” can have a cumulative effect, and it is certainly better than ceding the information environment to adversaries, particularly if they cannot be neutralized via kinetic means.

Cyber and Communication System Security

The U.S. military has for several years undergone a process of consolidating all of its internet-connected data centers. The primary reasons are cost and efficiency.[152] Unfortunately, consolidating this infrastructure is akin to the proverbial notion of “putting all of one’s eggs in one basket.” As consolidation continues, facilities and the network connections to them are becoming increasingly lucrative targets for Hybrid Warfare actors. In some cases, sending an email or retrieving a computer file from one site in a foreign country to another in the same country requires multiple satellites and/or fiber-optic cable “hops” to and from the U.S. This increases the vulnerability of communications to physical attack by Hybrid Warfare actors against ground-based communication nodes, as well as electronic warfare against communications satellite transponders (or even kinetic or laser attack on the satellite buses that carry them).

Resolving these vulnerabilities requires maintaining data center redundancy, significantly hardening the data centers against attack, and establishing additional redundant communications links, all of which are costly solutions in an era of decreased military resources.[153]

IO Integration During Phase IV-V

Over the last ten years, there have been a myriad of articles and books published on IO integration during stability operations as part of counterinsurgency and to enable transition to legitimate local civilian authorities. Therefore, this paper will not belabor IO during Phase IV. If a CJTF has reached Phase IV, then the hybrid threat they face has lost narrative momentum. However, the recommendations for Phases 0-III also apply to Phases IV-V, particularly shaping and targeting integration.

Assessment of IO and IRC-Generated Effects

Military operations must be continually assessed to ensure the CJTF is doing the right things the right way.[154] As is the case with other aspects of a military operation, IO assessment (like other types of assessment) needs to be built into the overall plan. Assessing IRC effects enable adjustments to improve overall IO effectiveness. The CJTF IO staff should maintain a recurring dialog with the staff effects assessment element (assuming one exists), as well as contribute to effects assessment for issues most closely linked to IO capabilities. However, depending on the operational area and phase, and particularly for EW and influence efforts, obtaining immediate measures of effectiveness may be difficult if not impossible. Rather than readily observable battle damage assessment, the CJTF IO staff and effects assessment element may need to rely on “impact indicators” to evaluate IO and individual IRC effectiveness, and those impact indicators may not clearly relate an effect to its cause.[155] An example of an impact indicator would be a billboard bearing photos of individuals for whom rewards are offered being obviously cut down with a chainsaw, despite the fact the billboard abuts a police station. This action indicated that those on the billboard felt the rewards were a threat (one of the desired impacts of monetary rewards as an IO tool), and additionally indicated they probably had some relationship with those working in the police station.[156] Another classic example would be the comparative number of women and children in public as an indicator of the local perception of safety and security.

The CJTF assessment plan must include metrics or impact indicators (which may be anecdotal evidence), and indicate who is responsible for collecting and assessing data, for incorporation into the overall CJTF intelligence collection plan. Effectiveness assessment is not institutionalized across the military, and assessment of IO-related impact indicators is not taught to most intelligence analysts.[157] Therefore, the CJTF IO staff and IRC subject matter experts will need to be involved in the assessment plan and processes, and develop information requirements for integration into the CJTF intelligence collection plan. Some assessment data will require resources external to the CJTF, such as polling portions of the population in the conflict area.[158]

The IO staff may also have to manage expectations of CJTF leaders to maintain support for continued IO efforts in the face of often ambiguous results, as assessing IO effects is not like assessing destruction of physical targets.[159] Assessing the results of MISO and other influence efforts can be particularly problematic.[160] However, just because data cannot be immediately collected does not mean IRC resources should not be expended.[161] Even when effects are marginal to a tactical fight, the strategic or operational value of that effect often outweighs the resourcing cost. The alternative is to do nothing. Unless impact indicators support a finding of ineffective efforts, it may be necessary to stay the course of IRC efforts for prolonged periods.

There are times when assessing the information environment can serve as its own information distractor, degrading confidence in PA efforts and harming credibility. As with the issue of combining PA and IO efforts, the utility of some forms of information can be outweighed by the criticism they engender. For example, the U.S. military has made use of contracted media analysis to determine what slant a reporter may impart on a new article resulting from exposure to military operations.[162] Elements of the media criticized the assessment effort, and the contract was terminated as the media scrutiny "had become a distraction."[163] This is unfortunate, as lack of analysis hinders PA staffs from being able to identify which reporters intentionally misreport information or divulge classified information that they had agreed to protect in exchange for access to military operations.[164]

Conclusion

Most of the foreseeable future conflicts the in which U.S. or its partners will be involved will likely have Hybrid Warfare components. Even if an adversary does not initially intend to employ hybrid techniques, failure to achieve their goals by conventional military means may result in a shift to application of hybrid techniques out of desperation (particularly irregular warfare or terrorism). It is therefore prudent to plan and train under the assumption that all future military action will occur in an environment of hybrid threats. Hybrid Warfare strategy focuses on advancing a strategic narrative intended to achieve a political outcome favorable to the Hybrid Warfare actor. Evolving to counter that strategy is comparatively inexpensive, and can be integrated comparatively easily with other forms of military modernization and training.

Hybrid threats will undoubtedly bring their “A-game” of sophisticated media-manipulation to further their narrative during future conflicts. Therefore, we need to organize and train to bring our own ”A-game,” such that our efforts towards harmonizing messaging are least equal to the effort we put into other aspects of military preparation and execution. Just as fires, maneuver, and logistics are integrated, so too must the IRCs.

Success against hybrid threats demands extensive application of IO towards foreign audiences, as well as PA efforts to ensure the U.S., coalition, and other partner-country audiences understand the context of why the conflict began and how subsequent events unfold. Shaping the information environment to preclude or prevail in future conflict requires action now to build and coordinate the U.S. narrative regarding the likely Hybrid Warfare conflict areas, as well as establishing information conduits into those areas. The U.S. diplomatic and military presence across the globe provides an asymmetric advantage to reach foreign audiences, but more interagency collaboration is required to make use of that advantage.

U.S. military IRCs, particularly MISO and PA, can support shaping efforts more than they do now, and such shaping efforts should specifically include deterrence of Hybrid Warfare tactics. Doing so will require a greater degree of interagency and multi-national partnership than is the norm today.

We must not overlook the contributions of the IRCs against hybrid threats in support of our combat objectives, since degrading a hybrid threat’s capacity for violence weakens the viability of their narrative. Unlike other aspects of warfare, tactical and operational IRCs often generate strategic effects. Our narrative and our targeting efforts must be mutually supporting, but our doctrine does not yet contain the procedures to ensure that takes place. We also need to do a better job at protecting our own information and information systems and not view cost as the greatest consideration.

Understanding the nature of the Hybrid Warfare threat and applying some of the methods described in this paper are a step towards developing the military information portion of a holistic U.S. Government approach to prevent conflict, and if necessary, win against hybrid threats. Many of the efforts described herein may not in themselves be decisive, but success against hybrid threats could be decided by small margins. This topic deserves more study and elaboration, and this paper is intended as a point of departure for the IO community in particular and the greater national security apparatus in general.

Endnotes

[1] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, (Arlington, VA: The Potomac Institute for Policy Studies, 2007); U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13, (Washington, DC: U.S. Joint Chiefs of Staff).

[2] Christopher Paul, *Information Operations, Doctrine and Practice: a Reference Handbook*, (Westport, CT: Praeger Security International, 2008), 120.

[3] U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13, (Washington, DC: U.S. Joint Chiefs of Staff, February 13, 2006), I-6; James E. Cartwright, Vice Chairmen of the Joint Chiefs of Staff, “Joint Terminology for Cyberspace Operations,” memorandum to the Service Chiefs, Commanders of the Combatant Commands, and Directors of the Joint Staff, November 2010.

[4] U.S. Joint Chiefs of Staff, *Information Operations,* (2006), II-1.

[5] IRCs are “A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.” U.S. Joint Chiefs of Staff, *Information Operations,* (2012), GL-3.

[6] The memorandum defines IO as “The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.” Robert M. Gates, Secretary of Defense “Strategic Communication and Information

Operations in the DoD," Memorandum 12401-10, memorandum to the Service Chiefs, Commanders of the Combatant Commands, and Directors of the Joint Staff, 25 January 2011.

[7] Marc Ambinder, "Original Document: Making PSYOPS Less Sinister," June 30, 2010, *The Atlantic* weblog, http://www.theatlantic.com/politics/archive/2010/06/original-document-making-psyops-less-sinister/58947/ (accessed 22 February, 2013).

[8] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02, (Washington, DC: U.S. Joint Chiefs of Staff, as amended through December 15, 2012), 199. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed December 19, 2012).

[9] Hy S. Rothstein, "Strategy and psychological operations," in John Arquilla and Douglas A. Borer, eds., *Information Strategy and Warfare: a Guide to Theory and Practice* (New York, NY: Routledge, 2007), 167-168.

[10] Ibid., 160.

[11] Though the U.S. employed MILDEC during the Vietnam War, Desert Storm, and to a limited degree in Iraq and Afghanistan, those efforts were miniscule compared to those employed during WWII. Paul, *Information Operations, Doctrine and Practice*, 74.

[12] U.S. Joint Chiefs of Staff, *Information Operations,* (2012), II-10.

[13] Ibid.

[14] Paul, *Information Operations, Doctrine and Practice*, 73; Cairnes Lord, "Reorganizing for public diplomacy," in Arquilla and Borer, *Information Strategy and Warfare*, 124: Barton Whaley, "The one percent solution, The costs and benefits of military deception," in Arquilla and Borer, *Information Strategy and Warfare*, 154.

[15] Paul, *Information Operations, Doctrine and Practice*, 71.

[16] U.S. Joint Chiefs of Staff, *Information Operations*, (2012), II-12.

[17] Dennis M. Murphy, "Operations Security in an Age of Radical Transparency," *IO Sphere* (Winter 2009): 36.

[18] Dennis M. Murphy, "Operations Security in an Age of Radical Transparency," *IO Sphere* (Winter 2009): 36-39; Paul, *Information Operations, Doctrine and Practice*, 79.

[19] U.S. Joint Chiefs of Staff, *Electronic Warfare*, Joint Publication 3-13.1, (Washington, DC: U.S. Joint Chiefs of Staff, January 25, 2007), I-4 – I-6. https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf (accessed January 8, 2013)

[20] Paul, *Information Operations, Doctrine and Practice*, 92; Kris Osborn, "Adaptive Electronic Warfare," *Army AL&T* (January-March 2012): 44.

[21] "Cyberspace operations" are "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace," U.S. Joint Chiefs of Staff,

Joint Operations, Joint Publication 3-0, (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), GL-8.

[22] DoD defines “cyber attack” as “A hostile acting using computer or related networks or systems, and intend to disrupt and/or destroy an adversary’s critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or the data themselves–for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 [command and control] capability.” Cartwright, “Joint Terminology for Cyberspace Operations”; Max Manwaring, *The Complexity of Modern Asymmetric Warfare*, (Norman, OK: Univ. of Oklahoma Press, 2012), 126-129.

[23] Arie J. Schaap, “Cyber Warfare Operations: Development and Use Under International Law,” *Air Force Law Review* 64, (2009): 147-148, 144

[24] Ibid.

[25] Paul, *Information Operations, Doctrine and Practice*, 96.

[26] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Routledge, 2004), 142.

[27] Lonsdale, The Nature of War in the Information Age, 135-136.

[28] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary*, 238. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed December 19, 2012).

[29] Paul, *Information Operations, Doctrine and Practice*, 100.

[30] U.S. Joint Chiefs of Staff, Public Affairs, Joint Publication 3-61, (Washington, DC: U.S. Joint Chiefs of Staff, August 25, 2010), I-8 – I-9, II-9. “Information fratricide is the result of employing information-related capabilities in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces.” U.S. Department of the Army, *Inform and Influence Activities,* Field Manual 3-13, (Washington, DC, U.S. Department of the Army, January 25, 2013) 1-1.

[31] Paul, *Information Operations, Doctrine and Practice*, 109.

[32] U.S. Department of the Army, *Inform and Influence Activities*, Field Manual FM 3-13, (Washington, DC: U.S. Department of the Army, January 25, 2013), 8-1.

[33] The organization of KLE is dependent on the unit the desires of its commander or chief of staff; several models have been used in Iraq and Afghanistan with success or failure dependent primarily on the personal involved.

[34] Paul, *Information Operations, Doctrine and Practice*, 111; Richard Dunbar, *Achieving Irreversible Momentum, IO sphere*, (Winter 2009), 13.

[35] Complaints such as this were common during U.S. stabilization operations in Iraq.

[36] U.S. Joint Chiefs of Staff, *Public Affairs*, 50; U.S. Department of the Army, *Inform and Influence Activities,* Field Manual 3-13, (Washington, DC, U.S. Department of the Army, January 25, 2013), 3-3; "visual information — Various visual media with or without sound. Generally, visual information includes still and motion photography, audio video recording, graphic arts, visual aids, models, display, and visual presentations." U.S. Joint Chiefs of Staff, *Department of Defense Dictionary*, 328. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed December 22, 2012).

[37] U.S. Joint Chiefs of Staff, *Public Affairs*, 50; U.S. Department of the Army, *Inform and Influence Activities*, 3-3.

[38] Richard Dunbar, "*Achieving Irreversible Momentum", IO sphere, (*Winter 2009), 15.

[39] U.S. Department of the Army, *Psychological Operations Process Tactics, Techniques, and Procedures*, Field Manual FM 3-05.301, (Washington, DC: U.S. Department of the Army, August 30, 2007), 2-29.

[40] Historically, based on the author's experience, the IO staff in U.S. operational-level headquarters in Afghanistan orchestrates the DoD Small Rewards Program on behalf of the commander.

[41] U.S. Joint Chiefs of Staff, *Joint Operational Planning*, Joint Publication 5-0, (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-39 – III-43.

[42] Russell W. Glenn "Thoughts on 'Hybrid' Conflict," *Small Wars Journal*, (March 2, 2009), http://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict (accessed December 23, 2012).

[43] Thomas X. Hammes, "Fourth Generation Warfare Evolves, Fifth Emerges." *Military Review* (May-June 2007): 14. http://www.army.mil/professionalWriting/volumes/volume5/july_2007/7_07_1.html (accessed December 19, 2012)

[44] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 120; Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle PA; U.S. Army Strategic Studies Institute, 2008), 9; Frank G. Hoffman, *Hybrid Warfare and Challenges, Small Wars Journal*, no. 52, (1st Quarter 2009): 35.

[45] Hoffman, "Hybrid Warfare and Challenges," 37, 36.

[46] Ibid., 34.

[47] David Sadowski & Jeff Becker, "Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare," *smallwarsjournal.com*, (Jan 2010): 5, http://smallwarsjournal.com/jrnl/art/beyond-the-hybrid-threat-asserting-the-essential-unity-of-warfare (accessed December 22, 2012).

[48] U.S. Joint Forces Command, *The Joint Operating Environment 2010*, (Norfolk, VA: U.S. Joint Forces Command, February 18, 2010), 58, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf (accessed November 30, 2012).

[49] Steven C. Williamson, *From Fourth Generation Warfare To Hybrid War*, Strategic Research Project, (Carlisle Barracks, PA: March 26, 2009), 15.

[50] Brian P. Fleming, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, School of Advanced Military Studies Monograph (Ft Leavenworth, KS: U.S. Army Command and General Staff College, May 2011), 36-37.

[51] Lonsdale, The Nature of War in the Information Age, 84; Manwaring, *The Complexity of Modern Asymmetric Warfare*, 147.

[52] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 147.

[53] Hoffman, “Hybrid Warfare and Challenges,” 37.

[54] Ibid.; Dorothy E. Denning, “Assessing the computer network operations threat of foreign countries,” in Arquilla and Borer, *Information Strategy and Warfare*, 187; Paul, *Information Operations, Doctrine and Practice*, 119; Manwaring, *The Complexity of Modern Asymmetric Warfare*, 126-127.

[55] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 129.

[56] Paul, *Information Operations, Doctrine and Practice*, 119; Glen E. Robinson, “Jihadi information strategy,” in Arquilla and Borer, *Information Strategy and Warfare*, 111.

[57] Ibid.

[58] Michael Howard, *Clausewitz: A Very Short Introduction*, (New York: Oxford University Press, 2002), 40-41; Clausewitz, Carl von, Michael Howard, Peter Paret, and Bernard Brodie, *On War,* (Princeton, N.J.: Princeton University Press, 1984), 595.

[59] Howard, *Clausewitz: A Very Short Introduction*, 40-41.

[60] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 139.

[61] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 125; Brian P. Fleming, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, 38-39.

[62] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 125-126; Fleming, *The Hybrid Threat Concept*, 38-39.

[63] Lonsdale, *The Nature of War in the Information Age*, 194; Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999), 6.

[64] Hoffman, *Hybrid Warfare and Challenges,* 37.

[65] Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, School of Advanced Military Studies Monograph (Ft Leavenworth, KS: U.S. Army Command and General Staff College, April 2009), 2.

[66] Thomas C. Schelling, “The Diplomacy of Violence,” in *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 1-34.

[67] Hoffman, “Hybrid Warfare and Challenges,” 37.

[68] Ibid.

[69] Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle PA; U.S. Army Strategic Studies Institute, 2008), xv.

[70] Hoffman, *Conflict in the 21st Century*, 38.

[71] Biddle and Friedman, *The 2006 Lebanon Campaign and the Future of Warfare*, 4.

[72] Tom Nelson, *The Second Lebanon War: Three Perspectives, Joint Center for Operational Analysis Journal*, (Spring 2009): 3.

[73] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 146.

[74] Ibid., 147.

[75] Ibid., 146.

[76] Ibid., 147-148.

[77] Peter Shearmana and Matthew Sussex, “The roots of Russian conduct,” *Small Wars & Insurgencies* 20, no. 2, (June 2009): 251–275 257, 254

[78] Asymmetric Warfare Group, “Russian-Republic of Georgia Conflict,” *Joint Center for Operational Analysis Journal*, (Spring 2009): 12.

[79] Ibid.

[80] Ibid.

[81] Ibid.

[82] Ibid.

[83] Ibid., 9.

[84] Ibid.

[85] Sun Tzu, *The Art of War*, translated by Samuel B. Griffith, (Oxford, U.K., Oxford University Press, 1963), 77.

[86] The instruments are Diplomatic, Informational, Military, Economic, Financial, Intelligence, and Law-enforcement (DIMEFIL). Timothy T. Tenne, “Why the military can’t do it all,” *Armed Forces Journal Online,* http://www.armedforcesjournal.com/2007/04/2575499/ (accessed September 23, 2012); Manwaring, *The Complexity of Modern Asymmetric Warfare*, 133.

[87] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 152. Biddle and Friedman, *The 2006 Lebanon Campaign and the Future of Warfare*, 6.

[88] John J. McCuen, "Hybrid Wars," *Military review*, (March-April 2008), 113; Hoffman, *Conflict in the 21st Century*, 46.

[89] Lord, "Reorganizing for public diplomacy," in Arquilla and Borer, *Information Strategy and Warfare*, 114; U.S. Public Diplomacy "includes communications with international audiences, cultural programming, academic grants, educational exchanges, international visitor programs, and U.S. Government efforts to confront ideological support for terrorism." U.S. Department of State, "Under Secretary for Public Diplomacy and Public Affairs," http://www.state.gov/r/ (accessed February 24, 2013).

[90] Lord, "Reorganizing for public diplomacy," in Arquilla and Borer, *Information Strategy and Warfare*, 116; Juliana Geran Pilon and Nicholas J. Cull, "The Crisis in U.S. Public Diplomacy: The Demise of USIA," *Project on National Security Reform Online*, http://old.pnsr.org/web/page/914/sectionid/579/pagelevel/3/parentid/590/interior.asp (accessed March 5, 2013)..

[91] Borer, "Conclusion: Why is information strategy so difficult?," in Arquilla and Borer, *Information Strategy and Warfare*, 237.

[92] Lord, "Reorganizing for public diplomacy," in Arquilla and Borer, *Information Strategy and Warfare*, 117.

[93] Ibid., 117-118.

[94] Ibid., 117.

[95] Biddle and Friedman, The 2006 Lebanon Campaign and the Future of Warfare, xi-xii, 6.

[96] Rosa Brooks, "Confessions of a Strategic Communicator," *ForeignPolicy.com*, December 6, 2012, http://www.foreignpolicy.com/articles/2012/12/06/confessions_of_a_strategic_communicator (accessed December 27, 2012).

[97] Assistant Secretary to the Secretary of Defense for Public Affairs George E. Little, "Communication Synchronization – A Local Coordination Process," Memorandum for Commanders of the Combatant Commands, Washington, DC, November 28, 2012. http://www.foreignpolicy.com/files/fp_uploaded_documents/121206_brooksmemo.pdf.pdf (accessed December 20, 2012).

[98] Rosa Brooks, "Confessions of a Strategic Communicator," *ForeignPolicy.com*, December 6, 2012, http://www.foreignpolicy.com/articles/2012/12/06/confessions_of_a_strategic_communicator (accessed December 27, 2012).

[99] Paul, *Information Operations, Doctrine and Practice*, 35.

[100] Rumi Nielson-Green, “Fighting the Information War but Losing Credibility – What Can We Do?,” *Military Review* 91, no. 4 (July-August 2011), 9, 13; Author’s personal observation and comments made by fellow officers during the course of 11 years as an Information Operations officer.

[101] Paul, *Information Operations, Doctrine and Practice*, 50.

[102] Joint Publication 3-13*, Information Operations,* 27 November 2012, II-4 - II-7; GEN(R) Gary Luck, *Insights on Joint Operations: The Art and Science, Best Practices, The Move toward Coherently Integrated Joint, Interagency, and Multinational Operations*, U.S. Joint Forces Command Joint Warfighting Center, September 2006, 31.

[103] Paul, *Information Operations, Doctrine and Practice*, 119.

[104] Anthony R. Pratkanis, “Winning Hearts and Minds, A social influence analysis,” in Arquilla and Borer, *Information Strategy and Warfare*, 63

[105] Ibid.

[106] Paul, *Information Operations, Doctrine and Practice*, 41.

[107] Paul, *Information Operations, Doctrine and Practice*, 41; Nielson-Green, “Fighting the Information War but Losing Credibility,” 2-3.

[108] Nielson-Green, “Fighting the Information War but Losing Credibility, 5; Paul, *Information Operations, Doctrine and Practice*, 106.

[109] Nielson-Green, “Fighting the Information War but Losing Credibility,” 5-6.

[110] Michael Hastings, “Another Runaway General: Army Deploys Psy-Ops on U.S. Senators,” *Rolling Stone,* February 23, 2011, http://www.rollingstone.com/politics/news/another-runaway-general-army-deploys-psy-ops-on-u-s-senators-20110223 (accessed December 4, 2012); Michael J. Dominique, *Information Operations: The Military’s Role In Gaining Information Superiority*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, March 17, 2009), 5; Dennis M. Murphy and James F. White, “Propaganda: Can a Word Decide a War?,” *Parameters* 37, no. 3, (Autumn 2007), 15; Nielson-Green, “Fighting the Information War but Losing Credibility,” 2-3.

[111] Nielson-Green, “Fighting the Information War but Losing Credibility,” 5-6.

[112] Paul, *Information Operations, Doctrine and Practice*, 106.

[113] Hastings, “Another Runaway General.”

[114] Ibid.

[115] U.S. Department of the Army, *Inform and Influence Activities,* Field Manual 3-13, (Washington, DC, U.S. Department of the Army, January 25, 2013) 1-1.

[116] Laurie M. Buckhout, “Electronic Warfare and Cyberspace Operations: Where is the Convergence?,” *IO Journal* 2, no. 2, (May 2010), 35.

[117] Clausewitz, *On War*, 97; Sun Tzu, *The Art of War*, 77.

[118] U.S. Department of the Army, *The Army,* Army Doctrinal Publication 1, (Washington, DC, U.S. Department of the Army, September 17, 2012) 1-5. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp1.pdf (accessed December 27, 2012.)

[119] Sun Tzu, *The Art of War*, 42.

[120] Ibid., 41.

[121] For discourse on this topic, see USSOCOM Directive 525-16, *Preparation of the Environment*.

[122] Beau Hendricks, Randall Wenner, and Warren Weaver “DIME is for Integration: Strategic Communications as an Integrator of National Power,” *IO Journal* 2, no. 2 (May 2010), 36.

[123] Information from the U.S. Department of State InfoCentral web portal is available at https://infocentral.state.gov/ (accessed December 18, 2012).

[124] Michael G. Vickers, “SOCOM’S Missions And Roles,” *Congressional Record*, (June 29, 2006). H060629 http://www.globalsecurity.org/military/library/congress/2006_hr/060629-vickers.pdf (accessed December 27, 2012).

[125] U.S. Africa Command, “Military Information Support Team,” Fact Sheet, Stuttgart, Germany, July 2010, www.africom.mil/file.asp?pdfID=20100719122755 (accessed December 27, 2012).

[126] Ibid.

[127] Harry W. Conley, “Not with Impunity Assessing US Policy for Retaliating to a Chemical or Biological Attack,” *Air & Space Power Journal*, (Spring 2003), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj03/spr03/conley.html (accessed February 26, 2013).

[128] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 130-131

[129] Ben Sherwood, President of ABC News, discussion with author, New York, NY, November 15, 2012.

[130] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 152.

[131] Tenne, “Why the military can’t do it all.”

[132] Ibid.; Manwaring, *The Complexity of Modern Asymmetric Warfare*, 152.

[133] Based on the author’s experience during several deployments to Afghanistan and Iraq.

[134] A “Battle Drill” is “A collective action rapidly executed without applying a deliberate decision-making process.” U.S. Department of the Army, *Infantry Platoon and Squad,* Field Manual 7-8, (Washington, DC: U.S. Department of the Army, April 22, 1992), vii.

[135] Paul, *Information Operations, Doctrine and Practice*, 44-45.

[136] The original PowerPoint slide on which this figure is based was painstakingly translated from the author’s hand-drawing by MAJ Al Ramirez, U.S. Army.

[137] James Kinniburgh and Dorothy E. Denning, “Blogs and military information strategy,” in Arquilla and Borer, *Information Strategy and Warfare*, 224.

[138] Alexia Tsotsis, “Libya Finds New Way To Cut Off Internet,” *TechCrunch Online*, (March 4, 2011), http://techcrunch.com/2011/03/04/libya/ (accessed November 29, 2012); “Internet services down across Syria,” *Al Jazeera English Online*, (November 29, 2012), http://www.aljazeera.com/news/middleeast/2012/11/20121129185299277773.html (accessed November 29, 2012).

[139] Zachary Fryer-Biggs*, “*Cyber’s Next Chapter: Penetrating Sealed Networks,” *Defense News online*, December 16, 2012: http://www.defensenews.com/article/20121216/DEFREG02/312160002/Cyber-8217-s-Next-Chapter-Penetrating-Sealed-Networks (accessed December 21, 2012).

[140] Statement made by an unknown Army War College student during a guest lecture on Information Operations and Public Affairs, U.S. Army War College, Carlisle Barracks, PA, January 4, 2013; Discussion between the author and a U.S. Navy officer on the International Security Assistance Force Headquarters IO staff in Kabul, Afghanistan, in the Fall of 2008.

[141] The primary DoD definition of a “target” is “An entity or object that performs a function for the adversary considered for possible engagement or other action.” U.S. Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60, (Washington, DC: U.S. Joint Chiefs of Staff, January 31, 2013), GL-8.

[142] Weaponeering is “The process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapons characteristics and effects, and delivery parameters.” U.S. Joint Chiefs of Staff, *Department of Defense Dictionary,* 332. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed December 22, 2012).

[143] A “joint integrated prioritized target list” is a “prioritized list of targets approved and maintained by the joint force commander.” U.S. Joint Chiefs of Staff, *Joint Targeting*, GL-6.

[144] The BLU-82, colloquially as the “Daisy Cutter,” was replaced by the GBU-43, referred to as the “MOAB” (officially Massive Ordnance Air Blast, unofficially “Mother of all bombs”). Patrick Nichols, “Duke Field Airmen drop last 15,000-pound bomb,” *U.S. Air Force News Online*, (July 21, 2008), http://www.af.mil/news/story.asp?id=123107470 (accessed March 5, 2013); Stacia Zachary, “Five years later, it's still known as 'Mother of all bombs',” *U.S. Air Force News Online*, (March 13, 2008), http://www.af.mil/news/story.asp?id=123089967 (accessed March 5, 2013).

[145] William J. Nemeth , *Future War And Chechnya: A Case For Hybrid Warfare,* (Monterey CA: Naval Postgraduate School, June 2002), 74.

[146] U.S. Department of the Army, *Electronic Warfare*, Field Manual 3-36, (Washington, DC: U.S. Department of the Army, November 9, 2012), 4-15, 5-4.

[147] U.S. Department of the Army, *Psychological Operations Process Tactics, Techniques, and Procedures*, Field Manual FM 3-05.301, (Washington, DC: U.S. Department of the Army, August 30, 2007), 3-17.

[148] U.S. Joint Chiefs of Staff, *Military Information Support Operations*, Joint Publication 3-13.2, (Washington, DC: U.S. Joint Chiefs of Staff, August 25, 2010), January 7, 2010, xi, II-11.

[149] LCDR Heather Beal, U.S. Navy, U.S. Pacific Fleet N39 staff, discussions with author, Pearl Harbor, HI, May 2011. Used with permission.

[150] Aram Roston, "DOJ Plans to Indict State-Sponsored Cyber Attackers," *DefenseNews.Com,* December 18, 2012, http://www.defensenews.com/article/20121218/C4ISR01/312180009/DOJ-Plans-Indict-State-Sponsored-Cyber-Attackers (accessed 21 December 2012).

[151] Schaap, "Cyber Warfare Operations:" 147-148, 144. This does not include espionage via cyber methods, which does not meet the DoD definition of cyber attack.

[152] Robert K. Ackerman, "Army Streamlining Information Facilities," *Signal Online*, (November 3, 2010), http://www.afcea.org/content/?q=2010/11/03/9162 (accessed February 24, 2013); Paul A. Strassmann, "Defense Board Computing Recommendations Lack Strength," *Signal Online*, (November 1, 2012), http://www.afcea.org/content/?q=node/10269 (accessed February 24, 2013).

[153] Manwaring, *The Complexity of Modern Asymmetric Warfare*, 132.

[154] Gary Luck*, Insights on Joint Operations*, 21.

[155] Lonsdale, *The Nature of War in the Information Age*, 158.

[156] This event occurred in Colombia in the mid-2000s, the author saw the before and after photographs of the billboard.

[157] Rothstein, "Strategy and psychological operations," in Arquilla and Borer, *Information Strategy and Warfare*, 166.

[158] Robinson, "Jihadi information strategy," in Arquilla and Borer, *Information Strategy and Warfare*, 98.

[159] Lonsdale, *The Nature of War in the Information Age*, 157

[160] Paul, *Information Operations, Doctrine and Practice*, 70.

[161] During the summer of 2006, the U.S. Joint Forces Command, Joint IO Planners Course taught that actions should not be conducted if they cannot be assessed; Reports from subsequent students indicate this facile philosophy is no longer taught.

[162] Charlie Reed, "Journalists' recent work examined before embeds," *Stars and Stripes,* August 24, 2009, http://www.stripes.com/news/journalists-recent-work-examined-before-embeds-1.94239 (accessed December 19, 2012); "Files prove Pentagon is profiling reporters," *Stars and Stripes*, August 27, 2009, http://www.stripes.com/news/files-prove-pentagon-is-profiling-reporters-1.94248, (accessed December 19, 2012); Leo Shane III, "Army used profiles to reject reporters," *Stars and Stripes*, August 29, 2009, http://www.stripes.com/news/army-used-profiles-to-reject-reporters-1.94340 (accessed December 19, 2012).

[163] Kevin Baron, "Military terminates Rendon contract," *Stars and Stripes*, August 31, 2009, http://www.stripes.com/news/military-terminates-rendon-contract-1.94400 (December 19 ,2012).

[164] Leo Shane III, "Army used profiles to reject reporters*", Stars and Stripes*, August 29, 2009, http://www.stripes.com/news/army-used-profiles-to-reject-reporters-1.94340 (accessed December 19, 2012).