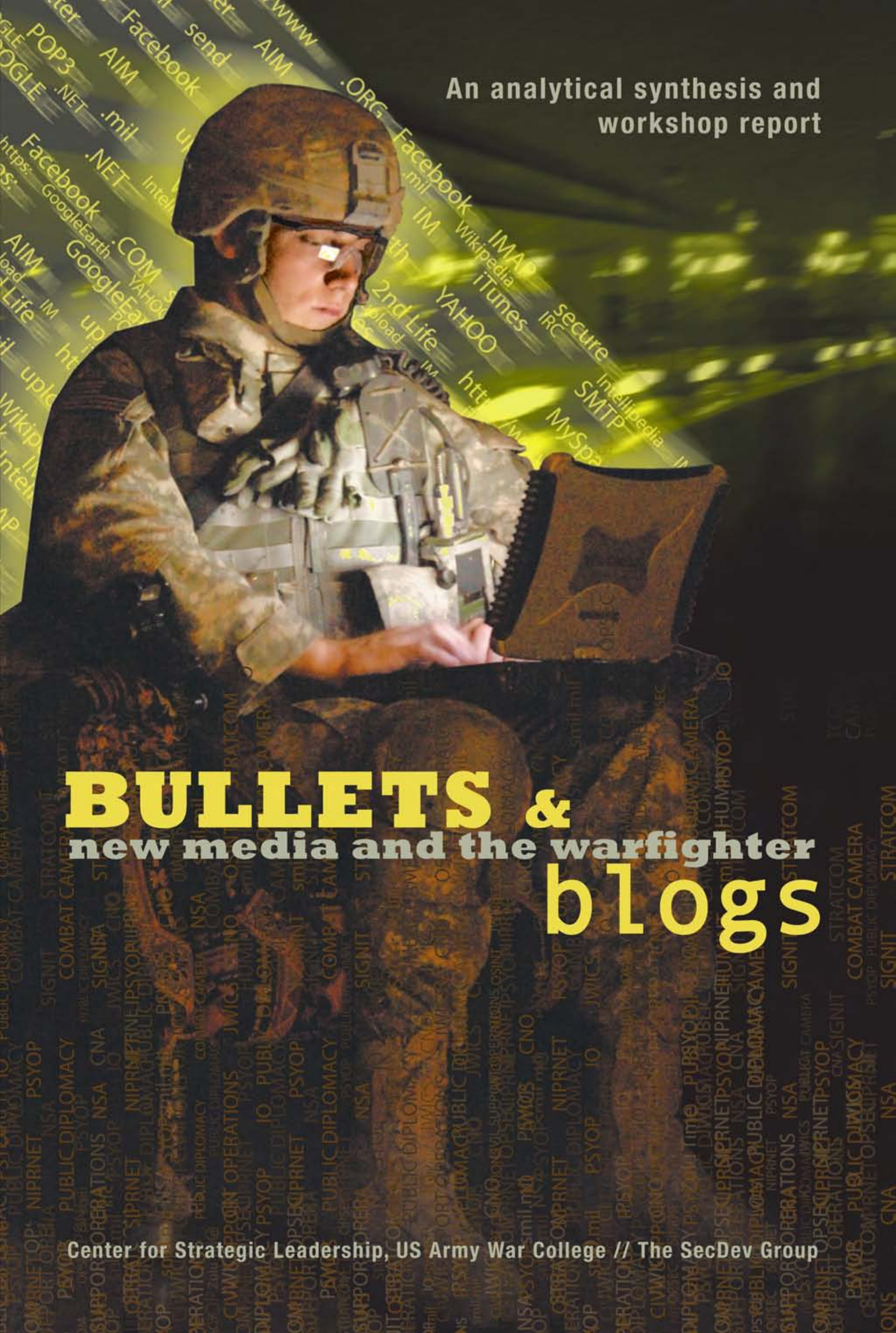
An analytical synthesis and workshop report



BULLETS & blogs

new media and the warfighter

Center for Strategic Leadership, US Army War College // The SecDev Group

About the Workshop

The "New Media and the Warfighter" workshop, held at the U.S. Army War College (USAWC), Carlisle Barracks, Pennsylvania, was a collaboration between the War College's Center for Strategic Leadership (CSL) and The SecDev Group (Canada). It brought together leading practitioners from the Department of Defense, Department of State, Intelligence Community and academia, over a three-day period (January 2008) at CSL's Collins Hall. The workshop used a case study of the 2006 Israeli-Hezbollah War in Lebanon as a jumping off point to examine the role of new media in contemporary warfighting. Focus groups explored the challenges and opportunities for leveraging new media, countering new media, and the implications for operations security. The workshop was an unclassified event, and the Israeli-Hezbollah case studies allowed participants to engage issues without prejudice or risk to ongoing operations.

About this Report

This report was prepared by Deirdre Collings and Rafal Rohozinski of The SecDev Group. Substantive inputs were provided by Dennis Murphy, Cindy Ayers, Harry Phillips, Jerry Johnson and David Smith, all of the USAWC. Special thanks to Jerry Johnson (USAWC) for his support in providing transcripts and Harry Phillips (USAWC) for gathering research material and establishing a web presence for the workshop. Thanks also to Jane Gowan for the report's layout and design work and to Arnav Manchanda and Kim Lawrence (both of SecDev) for editorial support. Finally, a word of thanks to Lieutenant General Bill Caldwell for his invaluable engagement with workshop participants, which enriched the discussions and greatly added to the enthusiasm of the workshop deliberations.

This workshop and report forms the second in a series that looks at the changing operational environment, within which information is now pervasive, and the consequences for the warfighter. The first report in the series — *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations* — can be found on http://www.carlisle.army.mil/dime/documents/ShiftingFire.pdf

Bullets and Blogs

Prudens
Futuri

Bullets and Blogs

New media and the warfighter

An analytical synthesis and workshop report

by

Deirdre Collings and Rafal Rohozinski

Bullets and Blogs

New media and the warfighter

An analytical synthesis and workshop report

Executive agent for the workshop report:
United States Army War College

The views contained in this report are those expressed by workshop participants as captured by the report authors. The contents do not necessarily reflect the views of the authors, or the official policy or position of the United States Army War College, the Department of Defense, or any other Department or Agency within the U.S. Government. This report is cleared for public release; distribution is unlimited.

Cover photography by PFC Michael Hendrickson,
used by permission of the United States Army.

U.S. ARMY WAR COLLEGE

CARLISLE BARRACKS, PENNSYLVANIA 17013

TABLE OF CONTENTS

Prudens Futuri

LIST OF BOXES

Prudens Futuri

Foreword

War is nothing if not a constant process of adaptation. Today, anyone armed with a digital camera and access to the Internet can become an information warrior, potentially reaching global audiences. Twitter, YouTube, Facebook and blogs have become as important to the strategic outcome of military operations as bullets, troops and air power. Appreciating the game-changing properties of new media are as important for today's warfighters as are the skills, training and tradecraft required to maneuver conventional forces.

In the contemporary operational environment, new adversaries have leveraged new media to achieve strategic outcomes. New media are their tactical tools for effective strategies that privilege the informational battlespace as the main effort. In this respect, the Israeli-Hezbollah war of 2006 is instructive. Hezbollah was out-matched by the IDF at all levels, with little hope of prevailing in the conventional military battlespace. And yet, by employing an information-led warfighting strategy that exploited tactical lethal encounters to generate strategic effects, Hezbollah was able to claim a strategic win by denying the IDF the achievement of its principal war aims. This clever use of the information environment, which Hezbollah used to create multiplier effects of its limited conventional military capabilities, essentially outflanked Israel's campaign strategy. By shifting the center of gravity into the information space, Hezbollah was able to generate and sustain the initiative. Hezbollah's warfighting strategy masterfully synchronized conventional and information "fires," creating strategic "information effects" that eventually forced Israel to cease its operations without achieving its stated war aims. The 2006 War provides important insights on the dynamics of the contemporary operational environment and the role of new media, which is why it was selected as the case study to drive workshop discussions.

For the U.S. warfighter one lesson should be clear: the enemy will never fight the war that you prepare for, but rather the one that it thinks it can win. That war will include new media as a warfighting enabler.

The 2006 Department of Defense Quadrennial Defense Review (QDR) posited that future conflict fall into one of four quadrants: traditional challenges; irregular challenges; catastrophic challenges; or, disruptive challenges. It observed that today's military capabilities continue to be focused on traditional warfare even as trends point toward the importance of multiple (or hybrid) threats. The Review confronts today's commanders and senior leaders with several important questions: Are we learning the lessons borne of hard-won experience and adapting our strategic thinking to ensure that we are ready for the next campaign? Is the shift in training and capabilities toward multiple and hybrid threats occurring fast enough? Have we sufficiently acknowledged and prepared for future scenarios in which new media and cyberspace will frame the strategies that our opponents are likely to use?

New media challenges warfighters and senior leaders across several levels. It requires recognition of the complexity of cyberspace as a warfighting domain. It is not just about defending networks or winning the information fight. Rather, it is the degree to which cyberspace exists as a domain in which warfighters will deploy, and the extent to which new media penetrates the warfighting effort in ways that are beyond the commander's ability to control or limit.

For example, today's Soldiers, Sailors, Airmen and Marines come from a generation of "digital natives" who have grown up with, and expect, 24/7 connectivity. They are consumers and users of new media, employing it in ways that are often poorly understood by senior leadership, and which can inadvertently compromise Operations Security. They network relentlessly with peers, colleagues, family, and friends. They learn from this networking. Numerous informal blogs and chat groups among warfighters have reinforced and invigorated a culture of peer learning in this generation. It has also aided morale and allowed warfighters on multiple and continuous deployments to remain close to their families and communities, which is critical for a professional military force.

Yet, DOD's digital natives are led by a generation of senior leaders who are "digital immigrants," many of whom spent their careers planning for conventional combat and possess a deeply ingrained belief that kinetic action is the principal means for achieving strategic outcomes. These leaders are legitimately concerned about the threat to OPSEC that can come from blogging, twittering or use of cell phones by warfighters or those that work alongside them. They are also wary of deploying capabilities for which there is no accepted standard of measure, and legitimately conservative when allocating staff and planning time to creating effects that may extend well beyond their Area of Responsibility (AOR) and which raise difficult legal and policy issues with potentially career-ending repercussions.

Yet, the interconnected Global Information Environment — where information transmission is instantaneous — has introduced a global dimension to even the most limited AOR. The interconnectedness and multimodal nature of cyberspace make it difficult to calculate or contain "information effects" – which can be the result of either actions or words, and which can incur strategic impacts. New media and the cyberspace domain cannot be ignored.

At the same time, new media raise complicated issues. For example, new media operate in and are dependent on civilian infrastructures. The information provider may be located in a different country from where information is being received. Decisions about what to target, how to engage, and with what fires and capabilities invoke complex legal aspects pertaining to the legitimate use of force (including the Geneva Conventions), which are not at all straightforward.

New adversaries have proven that cyberspace can be the main effort in effectual warfighting. And yet, commanders cannot be expected to engage effectively without more explicit guidance and clear rules of engagement. The challenge of engagement, however, raises issues that go beyond DOD's writ alone.

This report is being released at an important historical juncture -- just prior to the release of a major Pentagon report on the use of new media and following the assessment of the war effort in Afghanistan by General Stanley McCrystal, the International Security Assistance Force (ISAF) Commander. The latter report dedicated significant space to the role of strategic communication and new media. We expect that this report -- which reflects an extended conversation among a group of experienced warfighters, practitioners from the intelligence and diplomatic community, and scholars -- will add critical and constructive voices to the policy process as senior leaders shape policy that enables warfighters to fully engage new media as an element of national power.

The title of this report —"*Bullets and Blogs*"— emphasizes the symbiotic relationship between the lethal and nonlethal aspects of contemporary warfighting. The workshop and report are the result of an ongoing and unique international collaboration between the U.S. Army War College (Center for Strategic Leadership) and The SecDev Group (Canada). It demonstrates the vital importance of maintaining open channels between allies and amongst the military, intelligence and academic communities as we collectively assess and address the challenge of collective global security. While perspectives differ and debates are sometimes tough, it is through the spirit of engagement that a greater wisdom can be sought.

Rafal Rohozinski
Principal,
The SecDev Group
Ottawa, Canada

Dennis Murphy
Professor, Information Operations
Center for Strategic Leadership,
U.S. Army War College

Executive summary

Winning in the new media battlespace: Workshop top takeaways

For the U.S. military, new media and the Global Information Environment (GIE) present sustained challenges and opportunities. In recent years, new adversaries — armed with new media capabilities and an information-led warfighting strategy — have proven themselves capable of stopping the most powerful militaries in the world.

The current and future geo-strategic environment requires preparation for a battlespace in which symbolic informational wins may precipitate strategic effects equivalent to, or greater than, lethal operations. It demands a paradigm shift away from an emphasis on information control and towards information engagement. It will require cultural and organizational change within the Department of Defense (DOD) as it adapts to the world of digital natives – its own savvy Soldiers, Sailors, Airmen and Marines and their communicative expectations, proclivities, potential and risk; as well as its current and over-the-horizon opponents. Most of all, it will force the sustained adaptation and transformation of the way the U.S. military thinks and fights.

In recognition of the new media challenge, the U.S. Army War College (USAWC) hosted a workshop in January 2008 entitled "***Bullets and Blogs: New Media and the Warfighter.***" This workshop brought together leading practitioners from the Department of Defense, Department of State, Intelligence Community, and experts from academia. To spark debate, the workshop employed case studies drawn from the 2006 Israel-Hezbollah War in Lebanon. This conflict marked an important milestone for warfare in the information age. The non-state actor Hezbollah proved capable of thwarting Israel's primary war aims and forcing a battlefield stalemate. While Hezbollah stood little chance of prevailing militarily against the Israeli Defense Forces, its strategic victory was achieved by way of an information-led warfighting strategy that leveraged new media to influence the political will of key global audiences (including the Israeli public). The 2006 war previewed the characteristics of hybrid conflict[1] that U.S. forces may encounter in the future.

A synthesis of workshop discussions yielded inter-related takeaways on what is required to "win" in today's operational environment, where cyberspace and new media capabilities are significant components of the battlespace. Participant views clustered around three themes: a) The contemporary operational environment and the need for information engagement; b) New media, irregular and hybrid adversaries and core competencies; and, c) Enduring challenges and priority issues.

[1] According to Hoffman (2009): "Hybrid adversaries employ combinations of capabilities to gain an asymmetric advantage." Hybrid threats may emanate from states, state-sponsored groups, or self-funded actors, who engage in a blended form of warfare that combines modern military capabilities, with the techniques and strategies of protracted insurgencies (such as IEDs etc).

A. Today's operational environment: The information engagement imperative

1. **Cyberspace is an integral component of today's operational environment.** For the warfighter, information is now a critical factor in campaigns and major operations. In some cases it is the main effort. "Effectively employed, information multiplies the effects of friendly successes. Mishandled or ignored, it can lead to devastating reversals."[2] But today's operational environment is not focused solely on the battlefield alone. In the ongoing war of ideas, the U.S. must preemptively use all elements of national power to change negative perceptions and beliefs regarding its values and actions in the world. The warfighter is the frontline in this effort because of ongoing military operations, which are subject to 24-7, global public scrutiny on an unprecedented scale – largely due to the changes wrought by new media.[3]

2. **"Winning" in today's operational environment requires effective "information engagement.**" The win, especially against irregular adversaries, is in the form of political victory. The center of gravity is public opinion – often of multiple audiences.[4] Effectiveness is based on the ability to engage those different publics – in the idioms and through the media that resonate. Increasingly, the expectations and communicative cultures of audiences in the "information age" mean that a distributed presence on multiple and personalized media is becoming more imperative. It is also critical to maintain credibility at all times.[5]

3. **For the U.S. military, "information engagement" represents a paradigm shift.** *"Information superiority is a term we should throw out. You cannot achieve it."*[6] New media assures that no one can control the information available in the GIE.[7] New media also increases the capacity of adversaries to repackage your message, twist it, and use it against you. In this environment, the goals are not "information dissemination" and "message control," which have been DOD's institutional approach. Rather, the goals are effective communication and "message stickiness"[8] with target audiences. This requires a move away from reactive information responses, with centralized control and permissions, toward proactive and ongoing information engagement with decentralized authorities and decentralized execution (rules of engagement), backed up by appropriate training and a clear strategic vision. New media tools can greatly enable this paradigm shift. But it will

[2] Department of the Army (2008).

[3] Specifically, as laid out in the introduction, new media is ubiquitous, enables instantaneous and all pervasive communication and dissemination of narratives and images (via the many media channels) and empowers anyone with a cell phone or Internet connection to become an information warrior or mass communicator.

[4] Audiences can include those in the area of operations and at home, as well as international on-lookers – both sympathetic and antagonistic (some of whom may share the world-view of adversaries in the area of operations, and can be easily incited by what they perceive to be hostile U.S. actions).

[5] The principal strategy for achieving the win is to discredit the adversary in the eyes of the audiences that matter, just as the adversary seeks to discredit the U.S.

[6] This is the first of many participant comments that appear in the text. They are identifiable because they appear in quoted italics and have no additional reference.

[7] Information control is illusory because of the multiple information producers and channels, as well as the viral nature of communication (with messages being picked up and rebroadcast across multiple channels).

[8] Meaning message resonance with the target audiences.

require fundamental cultural and organizational change, as well as a more sophisticated risk calculus (see Points 6 and 12 below).

4. **Ongoing information engagement is a proactive strategy that underpins both the effective *leveraging* of new media, as well as the ability to *counter* the adversary's use of new media.** By being in an ongoing conversation with audiences that matter, you establish trust and credibility. This means that when you need to get your story out, it is likely to be listened to. It also means that adversarial propaganda is less likely to stick (see Point 6 below).

B. New media, irregular adversaries and six core competencies

5. **Irregular and hybrid adversaries — aided and abetted by new media — have demonstrated the capability for rapid and effective maneuver in strategic information engagements**. Adversarial agility is underpinned by three factors: a coherent strategy, synchronized methods, and decentralized organization, all of which leverage new media to their advantage. The strategy is to discredit their more powerful adversaries, (e.g., by showing them as using disproportionate force or harming civilians), while also showing their own capacities to inflict harm (e.g., through IED explosions, etc). The method is to capture (usually by filming) and package tactical lethal events in a way that serves their strategic message. And, they have the teams, equipment and networks in place to capture, produce and push out both imagery and narratives (whether manufactured or not). Insurgent foot-soldiers are empowered and equipped to act instantaneously when they see an opportunity. Overall, new adversaries excel in the six core competencies for agile maneuver in this space (see Point 6 below).

6. **Effective information engagement is underpinned by six core competencies (SAMMMS)**:

   - **Speed.** New adversaries — equipped with new media — have proven capable of generating image-rich propaganda that hits the Internet and airwaves within 45 minutes of U.S. lethal engagements. Speedy and proactive media engagement is essential for countering propaganda, discrediting adversarial actions, and ensuring friendly messages are heard.

   - **Authorities: Need to be powered down.** Insurgent forces get their stories out fast because they all know the story-line, and are non-hierarchical when it comes to message approvals. By contrast, the U.S. military works on a system of hierarchy and permissions, and has lengthy procedures for ensuring Operations Security (OPSEC). This creates time lags that have proven lethal for effective information engagement.

   - **Message: Specific, consistent, persistent, reflexive.** Stickiness requires core messages to be: meaningful to the target audience; consistent across actions, words, departments and operations; and, persistent, requiring a long-term investment and engagement. These prerequisites demand educational investments (in cultural learning), organizational reform (to improve coherence), and a refined capacity for strategic listening (to understand how messages are being perceived, and to feed this information back up the chain for course corrections). New media offers tools that can enhance capabilities across all these fronts.

- **Media: If you aren't in *their* space, you are no place.** *"To insert yourself into the conversation, you have to engage the medium that people are tuned in to. Otherwise they will never hear you."* This means engagement across the spectrum of new and old media, both friendly and adversarial.
- **Messengers: Trusted by audience.** Within the information blizzard of the GIE, appropriate and credible messengers can grab the attention of target audiences and help make messages stick. American Soldiers and mil-bloggers can directly and effectively inform the home front by simply telling their stories. For other audiences — including potentially hostile ones — third party validators[9] can be "force multipliers" that enhance the stickiness of U.S. strategic communication and propaganda-countering efforts.
- **Synchronicity.** Synchronicity enables organizational speed and agility by empowering actors at all levels to act appropriately. Synchronicity is achieved when different actors and actions, messages and messengers all reflect a shared narrative and strategy. This does not mean a coordinated and controlled response. Rather, it means that a clear strategic message sets the left and right parameters within which all agencies and levels "nest." Combatant Commands on the ground then have the *"flexibility to tailor their messages in a way that is consistent with the strategic intent, but responds to particular local circumstances and is congruent with their operational activities, not just their informational activities."*[10]

7. **Countering the adversary's "big lie" requires a streamlined, rapid reaction capability that prioritizes documenting, disseminating and speaking the truth.** This necessitates: filming all operations; using existing regulations and policy to determine what information can be unclassified up front; a capacity for rapid declassification of evidence post-action; improved video forensics; speedy, all-of-government investigations; and the authorities to declassify/speak at the right levels (see also Point 6 above). It also requires DOD and the U.S. Government to engage bad news stories honestly and forthrightly. Credibility demands it.

8. **Countering the adversary's narrative by lethally targeting the message delivery system – taking down websites or knocking satellite television or radio stations off the air – is no longer effective. The future is not to remove the message, but to respond to the message.** New media is self-healing — you take it down here, and it pops up there. New media communications are also viral: "*Once the information has gone out on the net, it is already mirrored to the extent that there is nothing you can do about it.*" There are also other potential 2nd and 3rd order effects (e.g., legal and proportionality repercussions).

9. **However, the capacity to inflict temporary disruptions remains a critical warfighting capability, and the palate of options for sophisticated non-lethal network attacks is underappreciated by senior leaders.**

[9] Meaning messengers who are trusted by their home audiences, independent of the U.S. military, but generally supportive of U.S. positions and policies.

[10] Participant comment. Synchronicity also enhances credibility, when the message is nested both horizontally and vertically from the President to the Soldier immersed in native populations.

C. Enduring Challenges and Priority Issues

10. **Military commanders have much less ability to completely control OPSEC.** The contemporary operational environment is awash in new challenges for preserving OPSEC. The potential for rapid and global dissemination of sensitive information has never been greater. At the same time, new adversaries gather most of their intelligence from open sources and from leveraging new media capabilities to gather and aggregate different bits of information into a more strategic whole. Examples of new challenges include:

    - More people are inside – contractors, coalition partners, Non-Governmental Organizations (NGOs), foreign and domestic media, adversaries and local indigenous civilians – and most are carrying new media devices such as video-enabled cell-phones;

    - Today's Soldiers are "digital natives"- expecting a 24/7-communication capability, using any number of digital communications platforms, and culturally conditioned for communicative openness. Constant communication back home, text messaging, participation in social networking sites and mil-blogging all have the potential to increase OPSEC risks. This challenge is compounded by the fact that most senior staff are "digital immigrants" who do not understand the range, scope and potential exposure of new media platforms;

    - DOD's efforts to enhance its strategic communication capacities also open up OPSEC vulnerabilities (for example, enhancing the speed of communication and declassification to explain events, pre-empt propaganda, and get the accurate facts out; or, letting Soldiers tell their stories).

11. **While increased OPSEC vulnerabilities are unavoidable in the age of "radical transparency," the path forward is more comprehensive planning that is fully informed on new media issues, backed up by red-teaming, training and constant vigilance.** There is also a need to better define critical information, and to adopt a more sophisticated risk calculus.

12. **New media can also enhance OPSEC by reducing footprints, aiding Open Source Intelligence (OSINT) and enabling deception**, although the latter strategy has the potential for blowback given the lack of control over information once it gets out into the GIE.

In summary, to achieve strategic agility in the information age, DOD should consider the following priority issues:

- Recognize that the winning strategy is "information engagement," not "information control;"

- Embrace new media as a significant enabler of "*that element of combat power called information*;"

- Prioritize research and development, and organizational change, to exploit new media as a warfighting capability;

- Educate digital immigrants to begin the process of cultural change;

- Exploit digital natives – encourage, educate, empower, and equip;
- Enhance DOD's capacity for commanding the attention and trust of key audiences through improved capacities for appropriate messaging, achieving a distributed global presence on relevant media, and finding and leveraging suitable messengers (third-party validators);
- Prioritize agility in the information environment, by:
    - » Enhancing speed of communication through: proactive information engagement; more refined classification efforts; in-field declassification authorities and capabilities; and, the removal of barriers to inter-agency and inter-service declassification;
    - » Moving towards decentralized authority and decentralized execution by setting the information rules of engagement;
    - » Identifying and mitigating risk, through a more sophisticated risk assessment process;
    - » Ensuring commanders have non-lethal options commensurate with traditional lethal options;
    - » Requiring commanders to define the desired information endstate;
    - » Exploiting new media for better measures of effectiveness;
- Streamline DOD policies and guidance;
- Synchronize, synchronize, synchronize — across all-of-government;
- Pursue a holistic approach;
- Engage the legal debate.

Introduction

For the U.S. military, managing the media and "information effects" has become a hallmark of the contemporary operational environment.[11] In today's geo-strategic environment, within which information is pervasive, much of the conflict may play out in the battlefield of the media. And new adversaries — armed with new media capabilities and an "information-led" warfighting strategy — have proven themselves capable of stymieing and even stopping the most powerful militaries in the world.[12]

The current and future geo-strategic environment requires preparation for a battlespace in which symbolic informational wins may precipitate strategic effects equivalent to, or greater than, lethal operations. It demands a paradigm shift away from an emphasis on information control and toward information engagement. It will require cultural and organizational change within the Department of Defense (DOD) as it adapts to the world of digital natives – both its own savvy Soldiers, Sailors, Airmen and Marines and their communicative expectations, proclivities, potential and risk; as well as its current and over-the-horizon opponents. Most of all, it will force the sustained adaptation and transformation of the way the U.S. military thinks and fights.

In recognition of the new media challenge, the U.S. Army War College (USAWC) hosted a workshop in January 2008 entitled ***"Bullets and Blogs: New Media and the Warfighter."***

Broadly defined, *new media are those consumer level digital devices and the forms of instantaneous, interactive communication they make possible because of their integration with global communications networks* (see Box 1). Since their emergence over the last 10 years, new media — which currently include the Internet, cell phones and digital cameras, blogs, social network sites, instant messengers, on-line websites, SMS and cell phone-based messaging and video-recording — have introduced a significant game-changing disruptive effect, by enabling:

- *individual-centric* reporting and *crowd sourcing*[13] of facts that threaten to displace traditional mass media and official spokespersons as the popular authoritative source of information, reporting and even truth. Anyone can now become a key influencer;
- *instantaneous communication*, which for the warfighter is critical, given that real-time information is emanating from military theaters of operation, first stories out tend to stick (whether true or not), and response times (to propaganda and rumors) must now be measured in minutes, not days or weeks;
- the *viral* spread of information (true or not), as *digital multi-modality* enables content put

[11] The term "information effects" refers to how information – derived from people's interpretation of events, information, or communications — shapes the perceptions, attitudes or beliefs of key audiences and which can influence their political will to the point of altering strategic outcomes. A strategy that prioritizes the creation of "information effects" uses communication campaigns (often involving careful media packaging of tactical lethal encounters) to shape the perceptions and attitudes of key audiences, to thereby influence their political will. Kinetic and tactical operations are often used to support this information-led warfighting strategy. For more discussion, see the previous workshop report in this series – *Shifting Fire* (Collings and Rohozinski, 2006).

[12] Examples can be found in Boxes 2, 3 and 5 of this report. See also Collings and Rohozinski (2006), and Kreps (2007).

[13] http://en.wikipedia.org/wiki/Crowdsourcing

out in one form to be rapidly edited, repackaged and transmitted across other forms;

- *a breach of the "iron wall,"* as audiences can no longer be separated or messages contained; a single communication uttered in a town hall or an isolated prison can potentially reach any audience, anywhere;
- *an explosion of media channels and platforms*, as well as *narrow-casting* to particular audiences, which allows audiences to tune out "big" media, and makes it difficult to reach all the audiences that matter on the media that they trust;
- *deception and propaganda*, as home-made videos rival professional news reporting, and official releases can be tampered with (which at the very least can create doubt and undermine credibility). Image-based propaganda is an especially powerful tool for adversaries;
- *open source intelligence — catapulting it to primary place for new adversaries*, and increasingly for the U.S. military — and also rapid organizational learning and assembly of capabilities;
- *strategic listening* – based on new media's interactive capabilities (for gathering direct feedback), and enhanced surveillance potential;
- *greater Operations Security (OPSEC) vulnerabilities*, as more folks are inside the wire with their digital cameras, cell phones and computers and while platforms like Google Earth create radical transparency.

Overall, new media have leveled the playing field between state and non-state actors and made it possible for anyone with a minimal access to basic infrastructure — individuals, social movements, criminals and corporations — to operate globally, and often outmaneuver and outpace states and international institutions.

Of core and future concern are hybrid[14] and other irregular hostile actors (e.g., terrorists, militant groups, national liberation movements, mafia structures, drug cartels and armed gangs) who are adeptly leveraging new media capabilities. They employ *open source* and *crowd source* methods to enable rapid learning and establish platforms for global command and control networks. They leverage the transparency and global reach of new media to: recruit followers; gather intelligence; organize, finance and implement operations; conduct *Cyop*[15]; and, amplify the strategic impact of their battlefield tactics.[16]

Significantly, the growth and penetration of new media technologies is fastest in countries and regions at risk of instability, violence, militancy, crime and insecurity. These are also the environments in which future U.S. deployments and engagement are likely to occur. At present, the top 27 countries with Internet penetration rates of over 10% are subject to *armed*

[14] For a definition of "hybrid" adversaries, see footnote 1 in the Executive Summary.

[15] Thomas (2007) defines Cyop (pronounced "PSYOP") as "cyber psychological operations that aim to directly attack and influence the attitudes and behaviors of Soldiers and the general population." http://leav-www.army.mil/fmso/documents/new-psyop.pdf

[16] New adversaries use new media as a central component of an information-led war-fighting strategy. See Boxes 2, 3, and 5 in this report.

violence risk factors[17] such as the youth bulge, unbridled urbanization, poverty and unemployment, and resource scarcity. These countries include many of those found in the greater Middle East "crescent of crisis" as well as crime and conflict affected states in Latin America and Africa. In addition, the top 55 countries experiencing exponential Internet growth rates include 90% of Low Income Countries Under Stress (LICUS), which are characterized by weak policies, institutions and governance and in this sense considered fragile and at risk of violence.[18] This means that over the next decade countries under stress from crime and conflict, along with those embodying armed violence risk factors, will possess the largest number of digital natives entering the global information environment.

Box 1.

Six characteristics of new media

Pervasive. There are over 1.5 billion Internet users worldwide, with over two-thirds located outside of North America and Europe. At present, Asia alone accounts for 42% of the global Internet population.[19] According to the International Telecommunications Union (ITU), 4.1 billion people — or over 60% of the global population — now use cell phones.[20] In both cases the figures likely underestimate actual usage numbers as in poorer countries Internet connections and cell phones are often shared.

Ubiquitous. Smart phones, Internet-enabled iPods, GPS devices, and other consumer appliances are increasing the number of network-attached devices through which new media content can be accessed. During the disputed elections in Iran (2009), videos were recorded on cell phones and digital cameras, uploaded to Twitter, YouTube, and posted to blogs, before being played back by satellite television channels.[21]

Instantaneous. New media is real-time. Blogs, instant messengers, Twitter, YouTube and SMS messages can spread almost instantly around the globe. New media forms report faster than old media, and reach a larger audience. They have been used to organize protests and resistance movements, and spread propaganda. Both the Internet and cell phones were used to organize the successful Orange Revolution in Ukraine (2005).

Interactive. New media enables interactive communication on an unprecedented scale. This is not just about instant messengers, email and cell phones. It is also about the "comment" function on blogs, websites and social networking platforms that enable interactive conversations and reader feedback, which in turn can promote mutual learning and fact correction, or further consolidation of extreme views.

Social and specific. New media leverage social connections between people based on language, shared interests, family, schooling etc. Recent figures show that over two-thirds of the 1.1 billion people aged over 15 have access to the Internet, and of these, 734 million (two-thirds of the total) accessed at least one social network site in May 2009.[22]

[17] See: Organization for Economic Cooperation and Development (OECD), 2009.

[18] Many LICUS countries are also experiencing conflict or are in a fragile post-conflict phase. For more information see: http://www.worldbank.org/ieg/licus/licus05_map.html

[19] Internet World Stats, (2009). http://www.internetworldstats.com/stats.htm

[20] Tryhorn (2009). http://www.guardian.co.uk/technology/2009/mar/03/mobile-phones1

[21] Alarilla (2009). http://asia.cnet.com/blogs/babelmachine/post.htm?id=63011506

[22] comScore, (2009). http://www.comscore.com/Press_Events/Press_Releases/2009/7/Russia_has_World_s_Most_Engaged_Social_Networking_Audience

"Sticky." Taken together, new media's pervasiveness, speed, interactivity, and social specificity means that its information and messages tend to be more trusted and *sticky* than those delivered by old media sources. Consumers become participants in the information-making process, following or participating in stories as they develop, which contributes to a positive sense of *crowd sourcing* and seemingly avoids the perceived bias of *old media* (where information is thought to be filtered).

Why this workshop?

How are new media and the Global Information Environment changing the geo-strategic calculus for warfighting? How are new adversaries leveraging new media for strategic wins? How are they out-maneuvering state military actors in this domain? Are we fully exploiting our rank-and-file "digital natives" or is organizational culture holding us back? Can we maximize the benefits of mil-blogging and other Soldier–centric communication while minimizing its liabilities? What does this age of "radical transparency" mean for OPSEC? What will the next campaign look like? Does the shift of capabilities to address multiple and hybrid threats take sufficient account of the need to fundamentally transform our informational capabilities and approach?

These were some of the questions raised during the USAWC's 2008 workshop, which brought together an international group of military, national security community and intelligence community leaders, as well as experts from academia. To spark debate, the workshop employed case studies drawn from the 2006 Israel-Hezbollah War in Lebanon. This conflict marked an important milestone for warfare in the information age, and previewed the characteristics of hybrid conflict that U.S. forces may encounter in the future.

During the 2006 war, Hezbollah, a non-state actor, was able to thwart Israel's primary war aims and force a battlefield stalemate. This was achieved through a strategy that synchronized well-planned and coordinated tactical military actions with a sophisticated communication strategy that ranged from the rapid exploitation of information gathered through Signals Intelligence (SIGINT), through to multichannel and multimedia delivery of well-designed strategic communication targeting the international community, Israeli population, its own domestic following, as well as sympathetic on-lookers (potential recruits) both at home and abroad. Militarily, Hezbollah stood little chance of prevailing against a sustained Israeli Defense Forces (IDF) campaign. Its success hinged upon correctly identifying the *information environment* and the political will of the Israeli population and key international audiences, as the center of gravity for its main effort during the campaign. Hezbollah's war strategy was therefore premised on *achieving decisive information effects in the cyberspace domain.*

Workshop discussions were facilitated by three illustrative case studies drawn from the 2006 war, which looked at how Hezbollah and Israel sought to leverage new media, and counter their adversaries' use of new media, as well as the repercussions on OPSEC. (See Boxes 2 and 3 below). These served to catalyze a broader exploration of current and future issues facing U.S. operational policy and practice.

Workshop discussions were limited by their unclassified nature. As such, the overall focus centered on new media's impacts within the strategic communication piece of winning current and future wars. Discussions of new media as a potential tool for lethal engagement were mostly avoided due to their classified nature.

The workshop was held under the "Chatham House Rule." As such, this report does not attribute individual or institutional comments made at the workshop.[23] However participant quotations are used liberally throughout to give a flavor of the exchanges and perspectives. Participant quotations are enclosed in quotation marks *and* italicized, but have no further identifying references.[24]

Box 2.

New media and the 2006 Israeli-Hezbollah War: Three key takeaways**

1. When lethal and informational efforts are synchronized, cyberspace can be a domain for decisive outcomes — equal in importance to the effort on land, air, sea or space.

- Hezbollah's military effort was designed to support its primary effort, which was in the information environment and cyberspace domain. At a tactical level, Hezbollah's military actions were insufficient to inflict a military defeat on the IDF. However, Hezbollah packaged tactical events (filmed, narrated and disseminated) – both its own successes and Israel's destructive efforts – in a way that serviced a well-formulated and multichannel cyber-strategy encompassing offensive and defense elements to generate a strategic political effect. Thus, militarily, Hezbollah sought to inflict maximum IDF casualties and to maintain resistance for as long as possible even in areas overrun or occupied by the IDF. (By the war's end Hezbollah positions were still occupied within 500 meters of the Israeli border.) The objective was both to demoralize the Israelis, while inspiring support among its followers, sympathetic onlookers and potential new recruits. Unguided Katyusha rockets were used to generate strategic effects through the fear and insecurity they caused among the Israeli population (despite their limited military utility).

- On a strategic level, Hezbollah used Israel's tactical successes to collapse support for Israel's effort, by capturing and disseminating the destruction of Lebanon and the attacks on civilians by the IDF. Hezbollah's fighters were among (and of) the population. Its military leaders and weapons were hidden in civilian buildings. Israel's attacks on Hezbollah caused sustained damage to civilian and religious infrastructure as well as civilian casualties. Hezbollah filmed, packaged and disseminated scenes of this destruction, which had the effect of: intensifying support for its resistance ideology and recruitment; dampening anti-Hezbollah opposition from neighboring states, while ensuring supply of weapons, fighters and funding; and, eroding domestic support for Israel, both within Israel and the United States.

- Hezbollah successfully leveraged cyberspace to effect a political victory over a militarily superior opponent, by publically denying the IDF and Israeli political leadership accomplishment of its principal war aims. Despite military superiority on land, air, sea and space, the IDF was unable to reverse the perception that they could not achieve the three principal war aims within an acceptable timeframe (and cost): return of captured Israeli

[23] See, http://www.chathamhouse.org.uk/about/chathamhouserule/

[24] Participant quotations were taken from the transcripts made from the recorded workshop sessions. In some cases, the spoken quotation has been modified to suit a print format.

Soldiers, ending Hezbollah missile strikes on northern Israel, and the military destruction of Hezbollah as a threat to Israel. By denying these aims — (which were clearly negated by the Hezbollah leader Nasrallah's ongoing media presence, as well as the ground-swell of support for its resistance across the region) — Hezbollah was able to claim a strategic victory despite the absence of any clear military victory, the suffering and wide scale damage to its military and civil infrastructure, and the significant loss of life among the Lebanese civilian population.

2. New media can service the adversary's warfighting aims and expose OPSEC vulnerabilities. In this, the opponent's creativity is more important than the sophistication of equipment or methods.

- Hezbollah correctly targeted weaknesses in Israeli OPSEC as a significant force multiplier. Hezbollah successfully monitored (unauthorized) cell phone usage by Israeli Soldiers in Lebanon. IDF movements were tracked, and reports of casualties were quickly transformed into strategic communication and Psychological Operations (PSYOP) products. Throughout the war, Hezbollah's reporting of tactical operations was consistently faster and more accurate than that of IDF spokespersons, leading to a significant "credibility gap" for the Israelis.

- Hezbollah reverted to relatively low-tech means to ensure the integrity of its command and control. Hezbollah anticipated that its command and control network would be targeted and consequently relied on distributed mission orders for much of the campaign (minimizing the need for direct contact between field units and headquarters). Core communications were secured by buried fiber-optic links, most of which survived the duration of the war, and were not disrupted or compromised by IDF SIGINT.

- Hezbollah built and hardened a redundant capacity for strategic communication, recognizing it as a critical warfighting asset. In this, it fully exploited the interconnectivity of the GIE. Despite apparent attempts by the IDF to hack and disrupt Al-Manar TV and Hezbollah's Internet infrastructure, neither was affected throughout the duration of the war. Hezbollah TV remained on the air despite the destruction of its primary broadcast facilities in south Beirut. Satellite communications and distribution remained operational throughout the conflict (despite a 12 minute interception and takeover by the IDF early in the conflict), and Hezbollah's Internet reach and presence was not at any time disrupted or degraded. Hezbollah did this by dispersing and embedding its infrastructure across the globe, including servers in the U.S. as well as in Russia, making it difficult and legally problematic for the IDF to take it down.

3. Strategic communication is effective when it targets the right audience, with the right message.

- Hezbollah focused its effort on influencing the political will of the Israeli population and wider international audiences, correctly identifying these as key centers of gravity. Hezbollah's significant new media machine, which included radio, television, RSS newsfeeds, videos, etc, communicated events occurring on the ground with speed and accuracy, in Arabic, Hebrew and English. Initially, "most of the international community agreed that, in principle, retaliation against Hezbollah for capturing two Israeli Soldiers was justified." But as the conflict continued, and the physical destruction of Lebanon mounted, Hezbollah's strategic communication campaign, with compelling imagery that called into question the proportionality of Israel's response – proved effective: "The Israeli government later acknowledged that the images of IDF raids in Beirut and the resulting civilian damage eroded its international support over the course of the conflict." The result was pressure on Israel to end its prosecution of the war before it had achieved its stated war aims. (Both quotes in this paragraph from Kreps, 2007: 80-81).

- By contrast, Israeli strategic communication focused on U.S. and European audiences. The narratives, which highlighted Hezbollah as a terrorist organization and Israel's moral right to a military response, had limited relevance and resonance among Arab audiences, and were eventually subverted in the eyes of Western onlookers. As just noted, Israeli claims became subverted by the compelling video reporting of damage and casualties to civilians in south Lebanon, which eventually eroded their international support. Israeli video footage showing precision strikes and Hezbollah weapons placed near civilian objects by contrast had limited effect. Hezbollah was not seen by Arab audiences as being a conventional military force, and therefore was not expected to act as one.

** For more detailed discussion of many of the above points see: Kreps (2007).

A reader's guide to this report

This report synthesizes the key themes and observations from across the workshop sessions. It is organized in five parts, with one appendix.

Part One, From information control to engagement, elaborates participants' views on DOD's need for a paradigm shift – from information control to information engagement.

Part Two, Leveraging and countering new media: Six requirements, summarizes participants' views on the core capabilities required for effective information engagement in the age of new media and irregular adversaries. This section synthesizes observations from both the "leveraging" and "countering" workshop sessions, as participants realized that ongoing information engagement is the proactive strategy for both efforts.

Part Three, Countering new media: Special considerations, further elaborates participants' views on what is required to effectively respond to the "big lie" (specific adversarial propaganda). It also considers how new media has compromised the effectiveness of lethal attacks aimed at shutting down the media (delivery system) itself.

Part Four, OPSEC in the age of radical transparency considers the multiple vulnerabilities that new media, and its exploitation, introduces;

Part Five, Seizing the new media offensive: Priority issues, summarizes participant recommendations on priority issues – including cultural, bureaucratic and legal impediments that need to be addressed to improve DOD's warfighting agility in the new media age.

The **Appendix** contains the **case study materials** based on the 2006 Israeli-Hezbollah War in Lebanon that formed the backdrop to workshop discussions.

Box 3.

Strategic information wins. Hezbollah’s attack on the Israeli Naval Ship *Hanit*

During the 2006 Israeli-Hezbollah War, Hezbollah successfully leveraged new media to package and disseminate tactical military actions so as to generate strategic political effects. A compelling example is found in Hezbollah’s attack on the Israeli Naval Ship (INS) *Hanit*.

On the evening of 12 July, with cameras rolling, Hezbollah launched two Chinese C-802 anti-shipping missiles at the INS *Hanit*. One of the missiles struck the Saar-5 corvette in the stern killing four crew members, and creating a spectacular explosion. Hezbollah broadcast the entire operation — live — on its television station Al-Manar, which has terrestrial and satellite broadcasting.

Within 15 minutes, the Al-Manar footage was carried by Al-Jazeera. By coincidence, the incident occurred at exactly the same time that the Israeli Chief of Staff, Lt General Dan Halutz was completing a televised press conference in which he emphasized the degree to which the IDF was in command of the situation in Lebanon (60 hours into the operation, in which airpower was used extensively, and with devastating effect). The footage of the attack on the *Hanit* was broadcast immediately after the interview with General Halutz, and was voiced over by a live phone-in interview with Hezbollah leader Hassan Nasrallah. During the interview, Nasrallah informed viewers that Hezbollah had struck an Israeli ship while it was attacking Beirut. He said the ship was burning and would sink. He emphasized that Hezbollah had more surprises for the IDF and that they would pay dearly for their adventure in Lebanon.

Within 24 hours, Al-Manar’s new media unit combined footage of the devastation caused by the IDF’s shock and awe bombing campaign against targets in south Lebanon, with footage of the attack on the *Hanit*. The videos were edited against a soundtrack of patriotic music and Nasrallah’s stirring narration, and then broadcast repeatedly on Al-Manar, and redistributed throughout the Arab region and globally as PowerPoint presentations, video clips, and circulated by e-mail and on regional video sharing sites.

The attack on the *Hanit* quickly took on symbolic meaning, and the story took on a narrative of its own. False photographs and accounts of the *Hanit* exploding and sinking appeared across blogs and in clearly doctored photographs and videos. The fact that the damage to the *Hanit* was relatively minor, and the loss of life limited to four sailors, became irrelevant. Hezbollah had discredited the Israeli Chief of Staff, undermined IDF claims of military superiority and claimed an important symbolic victory as the *Hanit* incident served to rally domestic and wider Arab/Muslim support behind Hezbollah, while demoralizing the Israeli public.

Part 1.

From information control to engagement: Winning in the new media battlespace

> *"We all know that you win a war on the offensive. The defensive is not where you want to be."*
>
> *"Information superiority is a term that we should throw out. You cannot achieve it."*
>
> —Workshop participants

Today's operational battlespace requires a paradigm shift: away from *information control* and toward *information engagement*. This was a central takeaway that echoed across all workshop sessions.

Participants stressed that for warfighters, the informational terrain is an integral component of today's operational environment – not something apart. A number of participants complained that some folks seemed to be "*trying to carve out informational activities separate from operational activities. This is wrong. They are part and parcel of the same thing. The moment that we try to simplify it by divorcing them, we complicate the issue and we complicate the effort.*" There needs to be a shift in thinking so that the information effort is seen as a capability that must be seamlessly integrated with the rest — so that warfighters plan for and "*use all means at their disposal to achieve the desired effect... whether that is firing a tank round, or pushing a button and [delivering] the 'blue screen of death.'*"

> “
>
> *Informational activities and operational activities are part and parcel of the same thing.... They need to be seamlessly integrated.*

Participants concurred that it is no longer sufficient to consider the "information piece" as a before-or-after adjunct to lethal engagement. Rather, information can be as important as lethal action in determining the outcome of campaigns and major operations. When effectively employed, information can augment friendly successes. When mismanaged, it can turn tactical success into strategic failure.[25]

While the informational dimension of the fight has become increasingly obvious, so has the complexity of the GIE. New media — with its multiplicity of information producers and channels and its "viral" nature[26] — have eviscerated the capacity of any actor, including the U.S. military, to control the information available in the GIE.[27] This is especially so when it comes to

[25] See also Collings and Rohozinski (2006).

[26] See Introduction and the Takeaways 1-3 of Executive Summary.

[27] Participants concurred that despite the technological superiority of the U.S. military, achieving control over the informational environment is only possible within a localized operational space, for a very limited time.

longer-term operational engagement and the broader terrain of the "war of ideas." No actor can prevent an adversary from putting a message out there, nor from having that message heard. And although "*you can control what you say, ...you can't control what people hear or what other people say*." As a participant observed:

> *"I think we make a mistake when we focus narrowly on trying to control the adversary's information that is out there. Rather what we have is a wide range of comments that are positive, negative, some organized, some not; some are ours, some are theirs. Some are finely crafted comments. Other times it is a Solider saying: 'What the hell...' All of that is out there. We have an information environment that is full of static. We create some of that, academics create some of that, others add to it. Our job is not to suppress that static so that we can get out our finely crafted message. Rather our job is to analyze that static, find messages that are in our interest, and figure out how to increase their 'volume.'"*

> ***Today's information environment is like the weather: A condition of the battlefield that can fundamentally affect your operation. But you can't control it.***
>
> ***If I can discredit my adversary, then I don't have to kill him.***

And as another participant noted: "*Often we speak as if information is controllable. But today's 'information environment' is much more like the weather... It is a condition of the battlefield that can fundamentally affect your operation. But you can't control it... Rather, the senior leader must be continually updated on the state of the weather. He must consider: 'Given the weather, what we can hope to accomplish? How might it change my ongoing operation? How can we adapt?' ... We need a constant probe and check to see what is going on out there with how messages are being perceived and reacted to.*"

Overall, the effect of new media is to "*create more information than the entire human race can consume. Therefore attention is what matters.*" And attention is best captured by effective "information engagement."

1.1 What "information engagement" means

> *Effectiveness is based on ability to engage the public debate...which in turn is dependent upon credibility, authority, and the ability to engage (Holt, 2008).*

Information engagement means using all elements of national power to influence the perceptions and will of key audiences. It means becoming an integral presence in the ongoing public conversation out there, in all the forums where critical audiences dwell. It is a move away from a reactive stance — popping in and out of the public debate to explain a specific operation or intention, or to counter an adversary's communication — towards proactive engagement. Proactive engagement means that you don't have to join a conversation, because you're already in it.

The goal, participants agreed, is to "*establish credibility and productive relations with key audiences and communicators, so that people come to **us** and say: 'What do you think really happened?' We need to position ourselves so that when we say, 'This is how we see it,'* *the audiences that matter will actually consider it."*

As one participant observed, proactive engagement can set the conditions so that "*propaganda and violent extremist propaganda don't have a place to go... If I can discredit my adversary, then I don't have to kill him. I've achieved my objective by eliminating him as a threat of influence over a broad population by making him laughable. I've emasculated him in the eyes of his target audience. So now they are no longer going to pay attention to him. They are going to pay attention to me. And I have won. It is low fatality, pinpoint accurate, and I have no blowback."*

> “
>
> ***New media tools give us the capability to remain in the conversation and to also get feedback while we're at it.***

Another participant related how effective engagement worked to limit adversarial influence with the Western media in Afghanistan:

> *"We had a real problem in Afghanistan because of bad reports every time a bomb was dropped. [They would often cite the local Taliban spokesman] and report that there were 100 casualties and make it look a lot worse than it really was. So, we started declassifying reports and showing the truth. We went to the reporters and said: 'Look, this is what is being said. But this is what we believe happened, and here is the local data to support this.' And we just kept hammering and hammering this. And now if you look at an article from Afghanistan it will stay the local Taliban spokespeople have been known to exaggerate the facts. And that is a huge victory because we went from — 'look at this, a whole village has been wiped out' — to putting the actual facts into perspective. We let them know that there is no moral equivalency between the local Taliban spokesman and the U.S. Army spokesman."*

New media complicates the task of proactive engagement because: i) many audiences (both hostile and friendly) need to be addressed; ii) those audiences now receive their information from a multiplicity of platforms (with some more trusted than others); and, iii) a conversation with one audience can be heard by others.

At the same time, new media is a boon for improving measures of effectiveness, as its interactive capabilities enable strategic listening, to better understand how messages are being perceived – both your own and those of your adversary. Both sources of information can enable course correctives. As various participants commented:

> *"New media tools give us the capability to remain in the conversation and to also get feedback while we're at it.*[28] *Staying in the conversation...helps with our credibility maintenance and expectation management, and [can help us to] adapt to whatever culture we happen to be working in."*

> *"Being engaged in the conversation all the time allows you to be able to make adjustments, as needed. You can gauge the weather and feel it, because you are*

[28] By feedback, the participant is referring to the interactive capabilities of many new media, such as the "comment" function on blogs – see discussion in Section 2.5.2 below.

walking in it. The weather doesn't matter if you are never outside. You need to be in it… to be attuned to what is out there."

"Engagement is not a one-off thing. It is about shaping perceptions and creating knowledge of what we are doing. It is about gauging the reaction to earlier events and people's understanding of them, and how this shapes their perceptions of the next event."

New media is also creating a global culture where both the speed of communications and their authenticity (meaning speakers close to the source) enhance their "truth value" in the eyes of audiences (see Introduction). For a hierarchical organization like DOD, adapting to these requisites will require fundamental organizational and cultural transformation (see Box 4). Interestingly, a number of participants stressed that — where organizational adaptation is already underway — it is proving its potential:

> *"We hear a lot about Al-Qaeda being able to beat us at the information game. But their tactics in the information war are the same as their tactics on the battlefield. What they cannot afford to do is to stay engaged. Which is exactly what we need to do — in all forms across all platforms — stay engaged. We need leaders at all levels to come forward and say this is exactly what is happening. Our bread and butter at the Blogger's roundtable in OSD[29] is not speaking to a General Lynch. It is speaking to the Colonels, the LTCs, and the guys on the ground — the battalion commanders that are making a difference down there. That's who folks want to hear from, and there's nobody down there telling their story. And by staying engaged at that level, there is a whole new narrative coming out — one that is in synch with what people are actually now starting to see through other media – because there is an ongoing counter to the bad news piece."*

"

Our bread and butter at the Blogger's roundtable is speaking to the … guys on the ground – the battalion commanders that are making a difference down there. That's who folks want to hear from.

[29] Office of the Under Secretary of Defense (OSD).

BOX 4.

DOD and information engagement: Cultural and organizational change

Participants concurred that the move to a culture of engagement will require fundamental organizational and cultural change.

Away from	Toward
Information control and media avoidance	Information and media engagement
Information environment as an afterthought in operational planning (information as a support operation)	Information environment as a core determinant of the operational battlefield, and sometimes the focus for the main effort
Information dissemination	Strategic communication
Uni-directional “Messaging”	Interactive strategic listening and establishing credible relations with key audiences and communicators
Reactive	Proactive
Focus on tactical operational success	Packaging tactical operational success for strategic wins with key audiences
Information hierarchies, centralized control and permissions	Full-spectrum agility, empowerment at the lowest levels, with appropriate rules of engagement
Piecemeal efforts and policies	A holistic and integrated approach
Digital immigrants	Digital natives

Throughout the workshop discussions, participants noted how irregular and hybrid adversaries – aided and abetted by new media – have demonstrated an ability to trump established militaries in strategic information engagement. This advantage is underpinned by three factors: a coherent information led-strategy, synchronized methods, and decentralized organization. The strategy is to discredit their more powerful adversaries, (e.g., by showing them as using disproportionate force or harming civilians), while also showing their own capacities to inflict harm (e.g., through IED explosions, etc). The method is to capture (usually filming) and package tactical lethal events in a way that serves their strategic message. And, they have the teams, equipment and networks in place to capture, produce and push out both imagery and narratives (whether manufactured or not). Insurgent foot-soldiers are empowered and equipped to act instantaneously when they see an opportunity. Overall, irregular adversaries excel in the six core competencies for agile maneuver in this space, a subject to which we now turn.

Part 2.

Leveraging and countering new media: Six requirements (SAMMMS)

Although the workshop devoted separate sessions to "leveraging" and "countering" new media,[30] participants concluded that these seemingly different objectives share a common core. Whether for offense or defense, effective maneuver in today's operational environment requires a refined capability for ongoing information engagement.[31]

Trust and credibility are established by engaging in an ongoing conversation with audiences that matter. This means that when you need to get your story out, it is likely to be listened to. It also means that adversarial propaganda is less likely to stick, as various participants observed: "*What is more important than a tit-for-tat processional countering of propaganda is the maintenance of good credibility at all times. What you need to show is that there is a bad dynamic at work against you out there, and to make that argument media rich;"* and, *"The whole idea of countering is wrong-headed. As we've said, it is about proactive engagement. You need an ongoing conversation. And the U.S. government has to participate in this conversation."*

> "
>
> *Effective maneuver in today's operational environment requires a refined capability for ongoing information engagement.*

Across all workshop sessions, participants highlighted six core requirements that are critical for both leveraging and countering new media, that is, for effective information engagement in today's operational environment: Speed; Authorities; Message; Media; Messengers; Synchronicity (SAMMMS). What follows is a brief look at participant perspectives on these six requirements.

2.1 Speed: First past the post sticks

> *"Even though we have every technological advantage, the adversary has response time on their side. We have to match their capacities to collect, process and disseminate."*
>
> — Workshop participant

Within 45 minutes of a U.S. lethal engagement in Iraq, the *Jaish Al-Mahdi* — equipped with new media – spread compelling, image-rich propaganda of the operation across the Internet and airwaves. The result was the effective benching of a U.S. Special Forces Unit for

[30] That is, countering the adversary's use of new media.

[31] Note that the leveraging-countering convergence focuses on the "soft power," or strategic communication component of new media. The participants also engaged the issue of lethal attacks as a method for disrupting the adversary's messaging/communication capabilities. This discussion is captured in Part 3 (Countering – Special Considerations).

a month (see Box 5). During the 2006 Israeli-Hezbollah War, the speed of Hezbollah's battlefield reporting enhanced the seeming credibility of their information and command of the battlespace. This was especially so given Israeli hesitations and unwillingness to comment (see Box 6, page 25).

Participants concurred that in the current geo-strategic environment "*speed is of the utmost importance.*" The first story out tends to get repeated across multiple platforms[32] and, the longer an adversary's version of events is allowed to go unanswered, the more truthfulness it accrues in the eyes of many audiences. As a senior keynote speaker emphasized: "*A piece of information put out on the public airways — if left by itself — will increase in truthfulness over time in the eyes of the people listening to that story. With no comeback over time, it increases in truthfulness.*"

New media has drastically increased the imperative for speedy engagement and release of information: "*In an era where we are trying to shape perceptions, we have a small window of opportunity to jump in. And if you choose not to jump in, you will lose that window.*" And, as another participant noted: "*New media has driven us to the point that we finally realize that we cannot take weeks, days or even hours to release imagery and information. We have to do it in minutes. In less than minutes. This is our adversary's timeframe. Unless we can keep up, we will continually be behind the curve and be reactive rather than proactive.*"

“

New media has driven us to the point that we finally realize we cannot take weeks, days or even hours to release imagery and information. We have to do it in minutes. In less than minutes. This is our adversary's timeframe.

Box 5.

Operation Valhalla: U.S. Special Forces neutralized for a month by cell phones

In 2006, the *Jaish Al-Mahdi* effectively benched a U.S. Special Forces Unit in Iraq for a month — with cell phone images and a propaganda story that hit the airwaves within 45 minutes of a kinetic engagement. A recent article in the Military Review captures the story:

"*Operation Valhalla* was an engagement between a battalion of U.S. Special Forces Soldiers with the Iraqi Special Forces unit it was training on one side, and a *Jaish Al-Mahdi* (JAM) squad…on the other. The *engagement* was entirely ordinary: the U.S. forces tracked down the JAM fighters responsible for the especially brutal murders of a number of civilians and several Iraqi troops. When U.S. and Iraqi government forces reached the JAM compound, a brief firefight ensued…

"Neither the battalion of the U.S. Army's 10th Special Forces Group (Airborne) under the command of then Lieutenant Colonel Sean Swindell (at the time a part of the Combined Joint Special Operations Task Force, Arabian Peninsula [CJSOTF-AP]) nor the Iraqi government forces

[32] For more extended discussion, see Collings and Rohozinski (2006).

took any casualties during the fighting on 26 March 2006, beyond one Iraqi Soldier with a non-life-threatening injury. Sixteen or 17 JAM were killed, a weapons cache found and destroyed, a badly beaten hostage found and rescued, and approximately 16 other JAM members detained, at which point U.S. and Iraqi government forces left the site.

"However…by the time the SF and Iraqi forces returned to their compound, roughly an hour after leaving the site of the firefight, [explosive Internet propaganda was already on the wires]: Someone had moved the bodies and removed the guns of the JAM fighters back at their compound so that it no longer looked as if they had fallen while firing weapons. They now looked as if they had fallen while at prayer. Someone had photographed the bodies in these new poses and they had been uploaded to the web, along with a press release explaining that American Soldiers had entered a mosque and killed men peacefully at prayer. All this had taken approximately 45 minutes…

"Both the American and Arab media picked up the story almost immediately. The result was an investigation that took roughly a month, during which the unit was, to put it bluntly, benched. Thus, a unit that could never have been bested in actual combat by JAM forces was essentially neutralized for a month by those same forces using a cell phone camera.

"Fortunately, U.S. forces had been accompanied by members of the 'combat camera' units, and had themselves been wearing 'helmet cams' in several cases. Thus 'before' pictures were available to contrast with the 'after' pictures the militia members posted to the web. This made all the difference in the investigation. (Indeed, in an interview with the author, Lieutenant Colonel Swindell noted that he would never again participate in an operation without at least helmet cams if combat camera personnel were unavailable, and in fact doubted he would ever again have an operation approved if he did not build into his planning some means for creating a visual record).

"Although the enemy set an all-time speed record in the case of Valhalla, the U.S. made no particular effort to respond in kind. [It took a full three days for the U.S. response, despite the fact that visual evidence countering the propaganda was packaged and ready within hours]. An operations officer for 10th Group, part of CJSOTP-AP at the time of Valhalla, Major Chris Smith, explained the delays this way:

"'We launched an operation against known insurgents. In this operation, we rescued a hostage who was certain to be killed and showed signs of torture, we found weapons galore... We were shot at by the insurgents, we ended up killing a good amount of them, and arresting about the same amount who were not shooting at us—showing fire discipline as well… We had an opportunity that night to speak to…the Washington Post—we also had an opportunity to get on television and describe what happened. [But]… It took … the Army three days to allow any news to get out. When we did, it came from the Secretary of Defense. And the briefing board that he used there at the Pentagon, the actual briefing board, the graphics that were on there, was our briefing board that had been prepared within hours of the operation. So it sat for almost 70 hours, the same [information] that was briefed three days later, sat for 70 hours. That's our fault.'"

Source: Dauber (2009).

A senior leader emphasized that all U.S. lethal engagements need to be accompanied by rapid and proactive "media engagements," especially those taking place in inhabited areas: "*We keep getting clobbered on airstrikes. But the solution is simple. You have a UAV film the whole thing. Go down, and get close-in pictures… We need live video to show what actually happened on the ground. So if someone tries to spin it some other way, we have the answer… [And those pictures] have to be declassified and out to the press within one hour… As soon as the operation is complete, you should be out conveying to the press exactly what has occurred.*" He also noted, however, that the imperative for proactive media engagement is not yet sufficiently absorbed into the commander's vision and planning cycle: "*But we don't do this well… We don't always think it through this way and plan for it. Instead we focus on the lethal engagement and getting the target. The strategic communication is terrible.*"

> "
>
> *We keep getting clobbered on airstrikes. But the solution is simple. Have a UAV film the whole thing… [And those pictures] need to be declassified and out to the press within one hour.*

Another participant shared an experience from Iraq at the start of the war that further emphasizes the need for cultural focus on the importance of speed. A reporter asked a Public Affairs (PA) Officer for clarification about an explosion where some people were killed: "*The PA officer went to his desk officer and asked what happened, and was told: 'We don't know anything about it.' But then a few days later he discovered there was imagery, and the whole thing was true. We had dropped some JDAMs on people and killed them. That whole report was true. Now roll that scenario three or four times.*" It is this kind of slow response that helps to give adversaries' stories and images — including fabricated ones — more stickiness than they deserve. As a participant noted: "*If you do not have the information, then you have to go and get it fast, so when a bad guy is out there trying to spin a story, you have more authoritative and credible information, be it good or bad.*"

Beyond lack of appropriate planning and awareness, DOD's communicative speed is compromised by its hierarchical organization, need for permissions, OPSEC requirements and still lingering cultural proclivities to control information and avoid media engagement. In the *Valhalla* case,[33] the U.S. commander had gathered the necessary evidence to counter the propaganda. The problem was permission to respond. It took over 70 hours for that key footage to be released. And, when the briefing finally came, it was given in Washington by briefers who were "several thousand miles and several layers of rank away from the events on the ground."[34] This distance, and the inability of the briefers to answer specific questions because "we weren't there, but we'd be glad to get you those answers," served to undermine the credibility and momentum of the military's case.

Participants recognized the inherent tensions between speed of communication and ensuring OPSEC as well as the accuracy of information. Most agreed on two key points. First, the accuracy of information is essential: "*The secret seems to be 100% truthful. Know your facts.*

[33] See Box 5 above.

[34] Dauber (2009).

Report your facts. If you don't know that something is truthful, then don't report it." Second, engage immediately, even if more time is needed to confirm the facts. Drawing on the case-study example — where the Israelis lost credibility with key audiences because they were slow to confirm the successful Hezbollah attack on their naval ship *Hanit* — a participant argued that the Israelis should have "*come forth and said: 'We have a report that one of our warships has been hit. We are investigating and we'll get back to you.' This would have allowed them to seize the media high ground. Media attention would have focused there…as the authoritative source of information that will come out."*

Box 6.

Lesson From Lebanon: Speed matters

Throughout the 2006 Israeli-Hezbollah War in Lebanon, Hezbollah media sources consistently reported the number and location of Israeli casualties faster than IDF sources. This had a negative effect on Israeli public perception, as reports made by Al-Manar were picked up by Israeli media, or disseminated on Hezbollah's Hebrew language service. The slowness of IDF reporting may have been a function of Israeli OPSEC considerations (as an early release could threaten ongoing operations), as well as the need to verify casualties (and their identities) to ensure that families of the deceased were the first to be notified.

A cumulative effect caused by the speed and accuracy of Hezbollah reports, and the slowness of IDF confirmation, was to create a "credibility gap" for the IDF. This was particularly evident following Hezbollah's successful attack on the Israeli Naval Ship *Hanit* (see Box 3 in Introduction). Al-Manar reported the attack in real time, while the IDF took 24 hours to confirm. The IDF delay may have been necessitated by OPSEC, but the result was a major negative "information effect," as the Israeli public felt that the IDF was being needlessly deceitful with their information.

Via Al-Manar and other media outlets, Sheikh Hassan Nasrallah (Hezbollah's supreme leader and chief spokesperson) was viewed by the Israeli public as providing more credible information than the Israeli media outlets.[35] This was also the first war where Israeli citizens were more fully exposed to what was happening in Lebanon, in almost real time, via different media outlets. After the war this led to severe criticism of Israel's own media.

2.2 Authorities powered down: Agility requires it

Insurgent forces get their stories out fast because they are non-hierarchical, at least when it comes to message approvals. Decentralized decision-making is possible because every insurgent understands both the strategy and the message,[36] and is equipped with new media to capture, package and deliver their propaganda payload. When insurgent foot soldiers see an opportunity, they are empowered to act instantaneously.

The U.S. military, by contrast, "is a large hierarchical organization that answers to civilian control. Those creating material have to have it approved by their chain of command before

[35] Dahan (2007).

[36] That is, to discredit their more powerful "enemies," while portraying themselves as heroic underdogs. See Takeaway 5 in the Executive Summary.

they can release it, and the release authority is often several layers above the creator of the material."[37] Participants concurred that a key requisite for improving U.S. agility in this arena was to get the authorities down to the right level:

> *"We have World War II era command and control policies, doctrine, law and culture. And we need to overcome all of it… We need decentralized authority and decentralized execution."*
>
> *"Combat commanders need the authority to operate in this space."*
>
> *"We need to get freedom of action down to the lowest possible level. They need the flexibility to do what they need to do, and to make the decisions they need to make."*
>
> *"Freedom of action at the individual level allows for agility at the command level."*
>
> *"Those with responsibility are not currently given authority."*
>
> *"As a CoCom [Combatant Command], I am always given the capability I ask for, but the problem is time. You don't know five or six days in advance … We have to change all of this if this capability is expected of us. We need decentralized authority to execute and decentralized execution."*

Overall, participants concurred that the U.S. military will never achieve the agility required if "*our spokesperson is sitting six or seven echelons above where the action is and you are trying to drill down for the needed information. There has to be a new paradigm – where a reporter is told to ask one of the guys closer to the action – so he can go head on with the guy doing the action.*"

"

There aren't a lot of Generals who will tell the person charged with dealing with the media: 'You have the authority to declassify whatever you need.'

A senior leader shared his experience around a U.S. proactive "win" in Iraq, which was enabled by appropriate authorities at the field level, including for rapid declassification of materials in theater (see Box 7). He emphasized, however, that "*not a lot of commanders out there will give that kind of power. There aren't a lot of Generals who will tell the person charged with dealing with the media: 'You have the authority to declassify whatever you need in order to support how you tell the American Soldier's Story.'*"

While most participants accepted that there are good reasons for requiring permissions, they also thought current policies and procedures were unnecessarily cautious and restrictive: "Y*ou know, I have to go buck-naked in the freezing rain for extended periods of time just to get the most mundane approvals. Like just to do simple websites. This is a problem.*" Many also commented on the irony of soldiers being trusted to fire weapons, but not to speak to the press: "*We will let a brigade commander's soldiers make the decision to fire a weapon – just like that. But we have got to go up to God-knows-where to get permission to allow our soldiers to say what they need to say…*

[37] Dauber (2009).

[And by the time] it wanders up there, the moment has passed. It is interesting that we've put ourselves in such a situation."

Participants agreed that the front line Soldiers, Marines and Airmen are underexploited strategic assets in the new media wars. They are the digital natives, savvy in the use of new media – the devices, the platforms, the networks and the possibilities. They are also the front line point of contact with adversaries and the foreign populace: *"A Soldier with a cell phone camera can be a powerful informational device... The young infantry PFC (Private First Class) 20-year-old may be the best guy to catch critical images and hand them off to his boss. We all know the rules of engagement: you can't fire on a mosque. We all get that. So the young lieutenant uses his cell phone to take a picture of the AK-47 coming out of the mosque. There is the verification, the documentation, which shows that mosque is no longer protected. We can use this material in support of our offensive operations. It can allow us to get out in front, so the bad news can't get out first."*[38]

> "
>
> *The front line Soldiers, Marines and Airmen are underexploited strategic assets in the new media wars.*

Box 7.

U.S. strategic communication win in Iraq: Decentralized authority made the difference

Muqtada Al-Sadr's supporters announced there would be a "million man march" in support of their leader. A senior American leader realized that if they could show that this event did not attract a million men, it would be an "*incredible opportunity to ensure the press accurately portrayed what happened.*" On the day of the march, a maximum of 10,000 people showed up. The U.S. staff captured it on video-feed. But that is when the challenge started.

"We had to get the video declassified and get it to the press as fast as possible. Timeliness is everything. If we didn't get it out, they would take pictures from low-level perspectives and make it look like there were tens of thousands. I had to assign two full time military officers to work the FDOs[39] — all they did was declassify things. [Normally] the challenge of trying to turn something from classified into unclassified so it could be released to the press would take three to five days. So we assigned two officers, which changed the turn-around time to three hours or so. And then we could start telling the story that we needed to talk about.

"Not only were we able to show that there were only around 10,000 people at this 'million man march.' We were also able to take that UAV and hone down and show that most people were not carrying pictures of Sadr, but pictures of the Iraqi flag. So then we could let the press draw their own conclusions. But we just gave them our best assessment of the numbers and what folks were actually doing by giving them those live video feeds. And it was done within hours of the march taking place."

Source: Workshop participant

[38] See also Part 2.5 below on allowing soldiers to tell their stories, and Part 4 on the challenges and risks.

[39] Feature Data Objects (FDOs) – "a spatial data access and manipulation abstraction layer, allowing you to easily access and perform common spatial operations on many different data formats." Source: http://n2.nabble.com/Feature-Data-Objects-FDO-f2048583.html

“

Filming an attack has become an integral part of the attack itself.

A workshop consensus: DOD should move from a process of permissions towards rules of engagement for both leaders and soldiers, backed up by the proper training: “*We need to establish rules of engagement like we do for other things. Proliferate that down; make it required training. We need to allow the young Lieutenant to be able to answer questions within the standing rules of engagement that he has with him today: when can he strike, when can he call in assistance.... There are certain methodologies we practice in the military all the time. Why don't we set them up within that same paradigm?*”

We return to the discussion of digital natives, authorities and rules of engagement in Part 5.

2.3 Message: Specific, consistent, persistent

New media has exponentially increased the cacophony of information “noise.” More than ever before, the capacity to influence key audiences requires that your message is listened to and sticks. Participants discussed three aspects of message “stickiness”: specificity, consistency, and persistence over time.[40]

Specific and appropriate

The core message has to be meaningful to the target audience – it needs to be conveyed in the language, imagery and cultural narratives or idioms that resonate. Ultimately, it doesn't matter what *you* think you are saying. What matters is what *they* think you are saying and why. Perception is reality. “*Sure you can have your message, but how is it being perceived? You need to understand this for your own correctives. You need to continuously adjust your messaging to the ongoing conversation, and to how your message is being perceived.*”

A number of participants noted that “*adversaries often seem to know us better than we know them.*” In Iraq, for example, insurgent messaging and propaganda events often target U.S. Soldier morale, as well as U.S. and international public opinion. Many observers have suggested that insurgent kinetic strikes in the age of new media — IED attacks on convoys, suicide bombings, execution of hostages – are undertaken specifically for filming and propaganda purposes: “Filming an attack has become an integral part of the attack itself.”[41] Compelling examples came from the workshop case study (the 2006 Israeli-Hezbollah War in Lebanon), where Hezbollah effectively targeted the public opinion of both international and Israeli domestic audiences, as well as the morale of IDF soldiers.[42]

New media also enables insurgents to assess the effectiveness of their efforts to influence foreign audiences. For starters, insurgents are aware that the Western press monitors their websites, and that

[40] Stickiness is also enhanced by appropriate messengers (see Part 2.5), the credibility that comes with synchronicity (see Part 2.6) and speed (see Part 2.1).

[41] Quote is from Glaser and Coll (2007) of The Washington Post, as quoted in Dauber (2009). See latter for more extended discussion.

[42] See Boxes 2 and 3 in the Introduction. Insurgents also know their own audiences far better than outsiders – what images and narratives resonate, (regardless of their relationship to the truth), although certain groups have been known to overstep the mark. Thus, whereas Hezbollah's resistance narratives generate widespread support amongst various constituencies both inside and outside Lebanon, other campaigns – like Zarqawi's attacks against Arab and Islamic targets – are thought to have alienated popular support.

their information and "stories" reach Western audiences via that route. At the same time, because the insurgents can access most newspapers and television coverage via the Internet, they are also able to gauge how their informational campaigns are playing out in the Western media.[43]

Participants concurred that the U.S. is behind the curve when it comes to understanding their foreign target audiences sufficiently to disseminate messages that are packaged in ways that resonate: "*Culturally appropriate content is the hardest part of effectively engaging, whether that is countering an adversary's message, trying to engage the adversary himself, or trying to engage a wider, non-committed foreign audience. The culturally appropriate content is the hardest part to do.*"

> "
>
> *There are usually objective reasons why ideologies become motivating factors for people on the ground. The less you understand that…the less effective you will be at shaping a narrative that is going to resonate with any of them.*

Another participant reflected on this gap in Iraq: "*This is one area where we could have done better. We had 24/7 monitoring of Internet channels. We looked for when inaccuracies occurred. We had people that would help us work up an appropriate response in Arabic — Iraqis who were working for us. They would help us write it so it was accurate, so we could send it to the particular news media, TV station or whatever to correct factual information. But the area that we didn't have was looking at it more culturally from their perspective. We just wrote it, and had them translate it. But that whole cultural context piece needs to be taken into consideration more, so that things are put into a cultural context that they understand.*"

Participants concurred that much effort was still needed to develop the requisite depth of cultural expertise and target knowledge, and that "*this language, regional and cultural development is not something we can solve overnight. We all know these are long-term investments in people and in bringing in academia…But without this capability, we are just putting out noise.*"[44] They also noted the vital importance of finding and leveraging "third party validators" – culturally appropriate key influencers who support the friendly message. We return to this discussion in Part 2.5 (on messengers).

On a related point, one participant stressed that an important part of growing cultural capability is to be able to get beyond labels of good and evil. Even if the enemy uses terror tactics, analysts need to understand his mindset and why his message (actions and words) resonates with various audiences (potential recruits, supporters, fence-sitters): "*I think one of the worst things that has happened in the last seven years is a tendency for blanket-labeling of adversaries as 'terrorists.' Because the moment you call someone a terrorist, you separate the actor and his actions from the context. [You eliminate the need to understand] why they are doing what they are doing, and why they capture popular support. There are usually objective reasons why ideologies become motivating factors for people on the ground. The less you understand your adversary and the*

[43] See also, Dauber (2009).

[44] A number of participants noted that, during the Cold War, it took some 30 years for the United States Information Agency (USIA) to grow effective expertise that produced effective cultural narratives.

objective conditions under which the foreign population lives, the less effective you will be at shaping a narrative that is going to resonate with any of them."

"

What you are doing is so loud, I cannot hear what you are saying.

Consistent: Actions and words

New media and the GIE have changed the pathways to influence. An actor no longer needs to be physically present in a population in order to influence it. He can also influence by way of *virtual* presence, provided his messages have resonance.

At the same time, U.S. joint operations occur amongst populations. This places a premium on ensuring that both the U.S. physical and virtual presence are coherent. To build confidence and trust with target audiences, actions must reinforce words; words must reinforce actions. Actions send the loudest message. Words and images provide the context to the action — to provide a holistic, accurate message. Consequently, words are a necessary, but not sufficient part of a message: "*Symbolic communication is much stronger than anything you say: 'What you are doing is so loud, I cannot hear what you are saying... Messages should amplify the actions on the ground; action should underwrite the credibility of the message.'*"

When actions do not match words, it creates a "say-do" gap that undermines moral credibility and provides rich fodder for adversarial propaganda.[45] This gap can also be picked up and amplified by journalists, academics, politicians and other commentators in ways that negatively shape perceptions of U.S. intent and credibility with various audiences.

The challenge for the warfighter is that tactical lethal action can no longer be planned from a conventional battlefield perspective. Rather, every lethal action needs to be considered on the broader canvas of how this action will play out in the perceptions of critical audiences, and with an awareness that everything you do may be captured, uploaded and deployed to global audiences: "*In today's age, you can't restrict [yourself to a conventional battlefield perspective]. If you destroy a Shiite mosque you may have attained a tactical victory — you've killed adversary target number one — but you've incurred a very strategic loss, because of the implications on a much wider battlefield. We always need to look at the tactical and operational level from a strategic standpoint.*"[46]

Recognizing that the adversary's strategy is heavily dependent on packaging lethal events to create propaganda effects, participants stressed the need to avoid being baited by adversary action that seeks to provoke a heavy-handed response. A participant shared his experience when stationed with the Israelis: "*The Division Commander in charge of the terrain where missiles were falling (before the war) knew that the way to counter Hezbollah was not to react. His strategy was to send the front commander to the office of the Chief of Staff, and tell them not to react.*" The Division Commander knew that Hezbollah was standing by with reporters and camera crews ready to film the IDF fighter jets. So he chose not to react. Instead, he engaged three weeks later.

[45] For more discussion, see Collings and Rohozinski (2006); Wass de Czege (2008).

[46] As already noted, attacking a mosque requires solid photographic evidence and a sustained communication campaign to clearly justify the decision to attack.

Participants acknowledged that in warfighting, mistakes happen. This places a premium on planning for unintended consequences: "*When you say you are not going to cause damage and you do, you automatically draw the ire of everyone. In Afghanistan we're out there, and we are trying to take out the bad guys. But then we end up with collateral damage. We have to tell people what we're trying to do, but if it goes wrong, we need to tell them about that too.*" Participants concurred that bad news stories need to be proactively and honestly engaged. Ignoring or downplaying bad news undermines hard-won credibility, and cedes the terrain to your adversary.

Overall, ensuring the consistency of actions and words means having the information practitioners present at the very start of the planning process: "*They need to be glued at the hip of your … operations person from the beginning, so that they are constantly suggesting what needs to be done. Right now, this tends to be an afterthought rather than a forethought. We're not being proactive. We can no longer exclude the communications folks. They need to be seen as a critical member of staff at the early stages of the planning process.*"

An enduring challenge, however, is the new media induced transparency of the GIE and the multiple audiences — with different interests and perspectives — that can now "overhear" messages intended for others.[47]

Persistent, but reflexive

Participants agreed: "*Effective messaging requires long-term investment and engagement.*" As noted, no one can control the information available in the GIE. No one can control the negative stories circulated by adversaries, the media or even fellow Americans. No one can control how his message is perceived by different target audiences. No one can control the evolution of a message. As one participant observed: "*I may put out that this thing is iced tea but by the time it bounces around the information environment – it may end up being Coca-Cola.*"

The only viable strategy, then, is for constant, iterative engagement to ensure your message gets out, and is heard in the way you intend it. The latter also requires a capability for strategic listening. As one participant summarized: "*We need to establish ways to do strategic listening that we currently do not have. And this needs to link back into policy. What it really boils down to is this: our messages must align with our actions. This is what gives us credibility. But we've had a break (on this front) in Iraq. So we need the ability to create linkages back from our strategic listening into policy, and to potentially have adjustments made. We need an ability to recraft.*" As already noted, the interactive capabilities of new media offer important avenues for effective strategic listening; we return to this point in Part 2.5.

> “
>
> *[Ensuring the consistency of actions and words means having the information practitioners] glued at the hip of your operations person from the early stages of the planning process.*

[47] For further discussion, see Collings and Rohozinski (2006).

2.4 Media: If you aren't in their space, you're no place

"To insert yourself into the conversation you have to engage the medium that people are tuned in to. Otherwise they will never hear you."

— Workshop participant

Participants concurred that, although the workshop was on new media, in reality engagement had to be full spectrum. The appropriate platforms are those that your audiences tune in to and trust. Increasingly, new media are going to be the "places to be." Current strategies, however, must be more broad-based. As participants noted: "*Some cultures are really face-to-face. In Iraq and Afghanistan, the successes that we've had have been in the one-to-one engagement. Face-to-face with tribal leaders and mullahs.*"

"

Blogs allow a one-on-one human interaction. And it is these human connections that count the most.

For both old and new media, message stickiness is enhanced by the "human connection." In this, new media is opening up tremendous future possibilities: "*Blogs allow a one-to-one peer connection with somebody else. Blogging is actually giving you (in the cyberworld) a capability for one-on-one human interaction. And it is these human connections that count the most.*"[48]

When it comes to new/old media, most participants agreed on the importance of engaging with and on "non-friendly" foreign media that have credibility with critical audiences: "*The channel or the platform is very important. And CNN is not it. Imagine a three star showing up on an enemy's own media station? It would make people that you are trying to reach sit up and listen. And they don't listen to CNN.*"

This strategy, however, grates against DOD's current media-and-risk averse culture: "*It seems like we're willing to send our Soldiers and Marines into combat operation, but we are unwilling to send them into adversarial media and make clear arguments. Why not? LTG Caldwell is a good spokesperson. If he shows up in an adversarial media environment it can be a very intimidating thing for them. We should probably be doing a lot more of this. It is probably the most effective tool we have in our tool box for taking guns out of the hands of people who don't like us.*"

Participants accepted that this type of engagement increased the risks: You can't control the questions, and the conversation may go in uncomfortable directions. But most thought the risk was worth it: "*We need to take risks engaging media like Al-Jeezera — to put out our narrative and the facts, even though the questions do not go as planned. Ultimately, you will be building that credibility that you need... Maybe we can minimize our risks by taking the PA guy with us.*"

A senior leader shared his experience in Iraq, where he deliberatively engaged with Al-Jazeera, because it was the only credible mass media through which to reach his target audience (see Box 8). Other participants recalled the appearances of other senior

[48] We return to this issue in Part 2.5 (messengers). Participants also noted that the growing interoperability and hybridization of new media with old is eroding the new/old distinctions. Villagers in Kyrgyzstan may still get their information from fellow villagers, but some of them have cell phones through which they access the global information grid. This trend will only accelerate.

spokespersons: "*General Kimmit did that. He went on an Al-Jazeera discussion show that is one of the most watched on Arabic media. It raised a lot of eyebrows, but it also signaled a sea change right there. It was truly significant. But…it doesn't happen enough.*"

Participants also noted that the key to attracting audiences to DOD's own media networks was to ensure the accuracy of information, as well as the coherence of actions and words. These two things together build the authority, credibility and trustworthiness of the information source: "*Credibility and authenticity are the currencies of the Internet. People go to websites they trust. They don't go to ones that they don't trust. It is as simple as that. If we want people to access our information, we need to do everything we can to ensure our credibility. This is not only about saying the truth, and admitting mistakes when they happen. It is also ensuring that Soldier-civilian interactions and other policies are ones that earn respect, rather than limit that respect.*"

> "
>
> *New media are here to stay. You can consider them to be evil because they have tended to favor our adversaries… [Or you can] say: 'We have the same opportunity.'*

Box 8.

Engaging Al-Jazeera and other media: A Colonel's story**

Media like Al-Jeezera have a profound impact in the Middle East. We have two options. We can decide that we are not going to talk to them. But then they will go ahead and use whatever information they have available to them. Alternatively, we can engage them, and try to help them form their story based on the best available factual information that we can provide.

After Al-Jazeera was kicked out of the Iraqi theater, we made a decision that we would leave Iraq every month to fly down and visit their studios. We would walk in and do taped and live interviews for a couple of hours. We found it was the only media by which we could get out our information about what the coalition forces were doing in Iraq.

The new mediums are here to stay. You can consider them to be evil because they have tended to favor our adversaries… [Or, you can] say: 'We have the same opportunity.'

There are more mediums today than ever before for us to be able to tell the story of what the American Soldier is doing in Iraq. But in fact we are inclined to do the exact opposite. There is no plan. Nobody is engaging in a systematic way. When we hired on two bloggers to do nothing except blog from Iraq, it was unheard of. I was challenged by every legal person you can imagine about how this was probably not allowed. And yet this is the medium by which the American public is communicating, and world opinion is being formulated.

We should have people who do this on a regular basis in an attributional manner, so when there is an inaccurate story we can correct it. But we can also be proactive and share the story of what is going on from the perspective of the American Soldier. It is something that we don't encourage enough.

** Source: Excerpts from the workshop's keynote speech, given by a senior leader (based on notes).

2.5 Messengers: Trusted by audience

Within the information blizzard of the GIE, appropriate and credible messengers can grab the attention of target audiences and help make messages stick. American Soldiers "telling their stories" and mil-bloggers can help to convey the ground truth to home audiences. For other audiences — including potentially hostile ones — third party validators[49] can be "force multipliers" that enhance the stickiness of U.S. strategic communication and propaganda-countering efforts.

2.5.1 Soldiers telling their stories: Informing the home front

The American and international mainstream media do not always give a fair or accurate view of what is going on in current areas of operation. There are a number of reasons for this: sensational events grab more headlines and airtime; fabricated propaganda events (which specifically target the morale of American audiences) are sometimes picked up and replayed by mainstream media before correctives are issued;[50] and, "*competition has driven traditional media to abrogate its responsibilities for authenticity and verification in favor of being first and fast.*"

“

Sharing the Soldier's story through blogs is an incredibly powerful tool.

Participants concurred that, for American audiences, an extremely effective but underused messenger is the American Soldier.[51] A senior leader emphasized a "top takeaway" from his experience in Iraq: "*The media is not the enemy. In fact, the media is a conduit to discuss with the American public what is going on in Iraq. And sharing the Soldier's story through blogs is an incredibly powerful tool. Had I not had some young people working with me — who explained to me what I needed to do to get our message out — I would never have appreciated it.*" (See Box 9).

Recognizing that this is currently under review, many participants concurred that current DOD policies on blogging were unnecessarily restrictive:

> *"You may be surprised at my opinion, given I'm an infantry officer, but…to operate in the new media we need increased flexibility with our young people. We need to give them the ability to talk. We need to give them the ability to do MySpace and YouTube. But what we do is we restrict it. We need to get past this paranoia. Sure there are things we do not want to divulge – times, places, and specifics. But with proper training these issues can be handled. Alternatively, if we get concerned about all these different mediums for distributing information so that we restrict our ability to get our word out, well guess what? There is only one message that is going to get out and that is the adversary's."*

[49] Meaning messengers who are trusted by their home audiences, independent of the U.S. military, but generally supportive of U.S. positions and policies.

[50] For specific examples from Iraq, see Dauber (2009).

[51] Participants also discussed the importance of allowing soldiers to blog home from the perspective of Soldier and family morale and the communicative expectations of the "plugged in" generation. See Part 4 on OPSEC.

> *"I have been trying to get someone to sign my blogging policy for the last two years. No one at DA or OSD will sign it. I believe you have to plan for it, train for it, and then give the permissions for Soldiers to engage."*

Allowing the army's digital natives to go forth online is not without risk — from compromising OPSEC and creating strategic communication blunders through to undermining Soldier morale. We return to these issues in Parts 4 and 5 below.

Box 9.

Encouraging Soldiers to speak: LTG Caldwell's four E's **

Encourage Soldiers to tell their stories. It has an overwhelmingly positive effect. Across America, there is a widely held perception that media coverage of the War in Iraq is overwhelmingly negative. We need to be careful to NOT blame the news media for this. The public has a voracious appetite for the sensational, the graphic and the shocking. Knowing this, we, as a military, owe it to the public to actively seek out and engage the media with our stories in order to provide them with a fuller perspective of the situation. When Soldiers do this, the media is very open and receptive. The public…also has a very strong desire to hear their personal stories. That is why we must encourage our Soldiers to interact with the media, to get onto blogs and to send their YouTube videos to their friends and family.

Empower Soldiers to tell their stories. This also means accepting some risk. A critical component of empowering is underwriting honest mistakes and failure. Soldiers are encouraged to take the initiative and calculated risk in the operational battlefield because we understand the importance of maintaining the offensive. However, once we move into the informational domain, we have a tendency to be zero defect and risk averse. Leaders have to understand and accept that not all media interactions are going to go well. Leaders need to assume risk in the information domain and allow subordinates the leeway to make mistakes. Unfortunately, the culture is such that the first time a subordinate makes a mistake in dealing with the media and gets punished for it, it will be the last time anyone in that organization takes a risk and engages with the media.

Educate our Soldiers to better deal with new media, and how their actions can have strategic implications. If Soldiers are better educated to deal with new media and its effects, they will feel more empowered and be encouraged to act. There are very few Soldiers out there who would intentionally harm the mission or intentionally do something to reflect poorly on their unit or the Army. When many of these incidents occur, and we have all seen them, it is because they just don't know that it is going to have that kind of effect and cause that kind of damage.

Equip our Soldiers by giving them the tools they need to properly share their stories. The experience of trying to gain YouTube access in Iraq and even back in the United States is a prime example. A suggestion for consideration might be equipping unit leaders with camcorders to document operations but also daily life. The enemy videotapes operations and then distorts and twists the information and images to misinform the world. What if we had documented video footage of the same operations that refuted what our enemies say? By the way, that is not enough; we have to get our images out first! The first images broadcast become reality to viewers. If we wait until we see the enemy's images, we are being reactive and we have already squandered the opportunity.

** Source: Based on LTG Caldwell's "Changing the Organizational Culture," 1 January SWJ OP-Ed Roundup, available on: http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/

2.5.2 Official and embedded bloggers

At the time of the workshop, there were six official bloggers in the State Department and six at Centcom. These official bloggers are entrusted to speak on behalf of the U.S. government. More than a few participants considered this number to be grossly inadequate.

In discussions around putting more resources into official blogging, or the development of a blogger corps, some participants argued that this strategy could backfire. "Official" blogging on behalf of an organization goes against the ethos of blogging communities on the Internet, which stress honest, transparent and personal viewpoints: "*The idea of a blogging corps could backfire…the medium is not designed for organizations, it is designed for individuals. And if users think: 'Hang on here, this is the government intruding into our sites' — this could seriously compromise the effort.*"

By contrast, other participants underlined how mil-bloggers have opened up an important participatory conversation with their readers, allowing for strategic listening and mutual learning:

“

New media is allowing us to do 'communication' rather than just 'information.'

Our bloggers are in constant communication with their readers, and with me. So in effect those readers are in constant communication with the government.

> *"We are finding that most of [our bloggers] have the interest or experience or the contextual background from which they can ask better questions. The new media environment is actually allowing us to do 'communication' rather than just 'information' – you actually have a feedback loop. Our history for the past 60 years, used to be about dissemination: I want to put a message out; I call a press conference; I disseminate. But I had no way of getting feedback other than what I read in the papers. These bloggers — particularly the guys I deal with— they are in constant communication with their readers, and they are in constant communication with me. So in effect those readers are in constant communication with the government… If you want to get to know somebody you need to sit down and talk to them. And once you have talked to them, you become more familiar with them. And through that familiarity you develop some level of trust. And that allows a whole litany of things to go forward."*

One participant suggested that one way to get around resource constraints would be to develop robot bloggers who could "*mimic our official bloggers, based on searching their computers for answers to similar types of questions. I can't buy twenty more bloggers, but I can buy 50 robot bloggers.*" Other participants, however, considered this to be a very high-risk strategy: "*Honesty and transparency are huge values within the blogging community… I wonder how a robotic blogger would play out? It sort of defeats the whole ethos of blogging, which is about having a personal connection with an individual, rather than some huge organization… If the public finds out we have mechanical bloggers, we lose credibility.*"

Overall, participants agreed that mil-blogging was still in its experimental phase: "*Some commands are open to it. Some resist it.*"

2.5.3 Citizen bloggers: The misinformed, not-so-friendly and independent friendlies

DOD cannot control what “other” bloggers have to say about them and their operations. However, when it comes to opinions based on incorrect facts, DOD can still encourage a corrective by engaging with accurate information: “*It is important when you have anti-bloggers*[52] *... to engage them and build a relationship with them.*” This strategy has been pursued by some commands, who have instituted dedicated blog-watchers. These staff monitor websites, and when they see something that isn’t accurate, they engage and point the blogger to other sources of information that are accurate: “*...and then that gets sucked into the blogosphere and gets spread all over. It has proven very effective.*”

At home, however, participants complained that DOD restrictions with respect to accessing some of the key platforms and sites acted as a form of strategic handcuffing, eliminating the possibility for proactive engagement: “*Here in America there are lots of blog sites that are anti-Department of Defense and anti-Norad. At my level — at the CoCom level — we are blinded because we can’t see these. We have to come up with policies that are more with the times. We cannot continue to be on second base when the game is over. Let’s look at the homeland, and how the necessary policies will also affect us here.*”

> *In Iraq, we had to confront a sixteen year-old blogger running an adversarial website... Is he considered a military threat?*
>
> *Before it was tribal, civic or religious leaders. But now it is a sixteen-year-old kid on the web. How do you deal with that individual?*

Within theaters of operation, the challenges posed by unfriendly bloggers — and the appropriate means for dealing with them — become murkier. As one participant asked: “*In Iraq, we had to confront a sixteen year old blogger who was running an adversarial website, but which he considered to be a neighborhood website. Is he considered a military threat? Is he someone that we would want to capture? What are the unintended consequences of pulling in a sixteen-year-old? This is something that we need to address with our rules of engagement. But also, how do we empower our subordinates to deal with something like this? Is this something that should be handled through computer network operations or is it something that we are prepared to address face-to-face, using a capture or detention mission? Before it was tribal, civic or religious leaders. But now it is a sixteen-year-old kid on the web. How do you engage and dialogue with that individual?*”

Another category of bloggers, however, represents a potential strategic asset – those with no relationship to DOD, but whose blogs reflect an understanding of DOD perspectives and goals. These independent friendlies can function as “third party validators,” to which we now turn.

[52] Meaning bloggers who write negatively about DOD or the U.S. government.

2.5.4 Third party validators: Credible and specific

> *"While the story of the American Soldier is very important to some audiences, I would wager that it is meaningless to the Iraqi people."*
>
> *"The most credible person in the world (to me), is someone just like me."*
>
> — Workshop participants

Third party validators are communicators who are trusted by their audiences, and who support a particular point of view that is favorable to an organization or business, but who are also independent. When these communicators speak, their audiences listen and usually consider their messages to be credible and authentic. Third party validators can be "force multipliers" – important conduits that enhance the stickiness and credibility of strategic communication.

Participants discussed the various ways in which third party commentators and validators played strategic roles in the 2006 Israeli-Hezbollah War. For example, the near real-time transmissions and images uploaded by Lebanese front line bloggers were picked up and replayed on major news media broadcasts. The destruction that these bloggers reported worked to validate Hezbollah's strategic narrative of Israel's use of disproportionate force. Alternatively, pro-Israeli groups ran well-orchestrated media campaigns in favor of Israel's actions (see Box 10).

> "
>
> ***Because the [front-line] Lebanese bloggers outpaced mass media reporting, major media organizations began to quote them as news sources. The result was third party validation and amplification of Hezbollah's narrative of the war.***

A number of participants thought the U.S. government should be doing more to identify and empower third party validators, much in the way that commercial entities do: "*Businesses find out who likes their products and then they talk them up, give them the opportunity to go onto a blog or on some other platform to get their message across, and then figure out other ways to reinforce that message.*"

With respect to Arab and Muslim audiences, participants concurred that fellow Arabs and Muslims were the ones with credibility. Some participants thought there should be a deliberate outreach strategy, to encourage moderate Muslims, indigenous employees of local government, and indigenous Soldiers to "*message on our behalf.*" As one participant noted:

> *"At the strategic level, in the battle over ideology, Al-Qaeda dominates at the moment. When Al-Qaeda speaks everyone listens. The U.S. and western states can't fight in that ring. But there are Islamic scholars that have a valid counter-argument that can fight in that ring. What they lack is a means to make their message heard. So any way we can help support the dialogue of this more moderate Islamic approach is [a step towards] discrediting Al-Qaeda. There are opportunities that should be better leveraged out there. When that high-ranking Al-Qaeda member turned on them — when he denounced and disclaimed Al-Qaeda — his message was never heard. It was a ripple that should have been an atom bomb."*

Box. 10

Third party validators in the Israeli-Hezbollah War: Lebanese bloggers and Internet watchdogs

During the 2006 War, part of Hezbollah's strategic communication campaign sought to establish Israel's disproportionate use of force against the civilian Lebanese population and infrastructure. IDF actions were captured as stunning visuals of war, as were the one million people who fled the south of Lebanon, along with the evacuation of foreign nationals by western nations. Hezbollah packaged and distributed gruesome photographs of destruction, which they released to the press and posted to blogs and photo-sharing sites. Graphic videos were assembled and posted to YouTube, and to email lists that were circulated widely throughout the region. These images, along with the seemingly callous remarks made by some senior Israeli leaders meant that the sympathy of the Arab street, and certain international audiences, tended to side with the suffering of the Lebanese people.

This groundswell of popular sympathy was widely evident in email campaigns, blogs and websites that were not in any way related to Hezbollah (or its affiliates), but which none the less amplified and enhanced the effectiveness of Hezbollah's own informational strategy. In addition, many front line Lebanese bloggers, again not related to Hezbollah, provided real-time details and stunning photos of Israeli actions. Because the bloggers outpaced mass media reporting, major media organizations began to quote them as news sources. Several incorporated these blogs into their main news coverage. The result was third party validation and amplification of Hezbollah's narrative of the war, even though post-war assessments showed that the scale of destruction was not as great as was first reported.

With respect to Israel, third party validators came in the form of extensive civil-society-led information campaigns that vocalized support for Israel's actions. Well-orchestrated campaigns targeted the major mass media globally, with pro-Israeli Op-Eds, letter writing campaigns and blogs.

A U.S.-based blogger effected an important information win for Israel/loss for Hezbollah. His "Little Green Footballs" website (which won a "best Israel advocacy blog" award in 2005) broke the story of a Reuters' photographer who allegedly had touched up photographs of destruction of Hezbollah's neighborhoods in Beirut. As a result, Reuters was forced to apologize and pulled all 920 images taken by the photographer out of its catalogue. Similarly several other staged media events were exposed as fake by a variety of citizen-activist-run websites.

In the end, however, Hezbollah's proportionality narrative, backed up by imagery, won out. Israel came under strong international pressure, and ceased operations before attaining its declared objectives.

However, a strategy of direct support is not without risk. From DOD's perspective, the main risk is the lack of control over the message:

> *"They are not always going to say things that we like. They will not always like the United States or what we are doing. But we are going to have to let that go, and trust that the broader message is going to be salient with the target populations that we want to reach."*
>
> *"We cannot own what third parties say. It is their message. It may not be what we like, but it's still better than anything we can say."*
>
> *"[This counter-Al-Qaeda pamphlet we have, by an Islamic scholar] does not, by the*

> *way, say that jihad is wrong. It says that this current jihad is wrong, and it is being waged the wrong way. In fact, it does not say a lot of things we would like it to say. But it does say this part of this jihad is wrong, so we're trying to figure out how to disseminate this thing."*
>
> *"If you have a formal or semi-formal relationship with bloggers who blog for you, then you become responsible for everything that they do. Whether you like it or not, anything they say can come back to haunt you. Just keep in mind you do not have total control."*

Alternatively, overt U.S. support diminishes the entire third party effect, by compromising the independence of the speaker: "*If we print up his piece — and they say, hey you guys paid for it, the U.S. paid for it — well obviously that would be bad.*"

> *If you have a formal or semi-formal relationship with bloggers who blog for you, then you become responsible for everything that they do.*

From the third party validator's perspective, DOD support may mark him as a target, especially in areas of operations: "*If this Iraqi Soldier becomes 'our' blogger, he could end up being assassinated… And they don't have to be on the payroll. Any association with the U.S. military could endanger them. So we have to be very careful about what we do here.*"

Participants also noted that popular bloggers in the Arab world were coming under increasing surveillance and harassment generally, as governments fear what free speech may unleash: "*In the Arab world, you see a popular Egyptian blogger being detained. You see both the Egyptian government and the Kuwaiti government asking bloggers to register, so their information is registered. Blogging is now being seen as a credible threat…and a forum for opposition forces.*"

American Muslims have also faced problems, because their engagement on debates around *jihad* fingers them as a potential domestic threat: "*American Muslims have said: 'I want to engage these jihadist extremists on the Internet, but as soon as I do, the FBI comes knocking on my door.' And leaders within the American Muslim community have come to the U.S. government, and said: 'Do something!' I have people that want to do something about this, but they are now afraid to. So this is a policy issue…it is being pressed right now.*"

2.5.5 Synchronicity: Essential for coherence and credibility

Synchronicity is what the adversary has and the U.S. lacks. Synchronicity is achieved when different actors and actions, messages and messengers all reflect and reinforce a larger shared conceptual framework – a common narrative.[53] Synchronized efforts reveal a coherence

[53] As defined on http://www.answers.com/synchronicity: The idea of synchronicity is that the conceptual relationship of minds, defined as the relationship between ideas, is intricately structured in its own logical way and gives rise to relationships which are not causal in nature. These relationships can manifest themselves as simultaneous occurrences that are meaningfully related—- the cause and the effect occur together. Synchronous events reveal an underlying pattern, a common conceptual framework which encompasses, but is larger than, any of the systems that display the synchronicity.

of intent and strategy, no matter how different the individual efforts may be. Synchronicity enables organizational speed and agility, by empowering actors at all levels to act appropriately: "*Speed comes from everyone understanding the core narrative. If everyone understands the core narrative then you can rapidly improvise and respond at the local level.*"

Participants observed that actors like Hezbollah have a "*core narrative, which creates a different level of capacity with respect to messaging and information.*" Moreover, they "*deliberately combine the social and political aspects of what we call civilian-military operations, and they call humanitarian aid. They rebuild the house, rebuild the schools. We do that too, but we deliberately separate it from our PSYOPS*[54] *and Public Affairs. But that is their strength, and that is how they trump our doctrine, which requires us to maintain this legal separation between civil and military activities.*" Another participant observed:

> *"We saw this immediately after the 33 Day War. Hezbollah was in there with their action committee handing out cash. Immediately they were saying: 'Your house is destroyed. Here is a thousand dinars.' Meanwhile, the Lebanese government was saying: 'No we cannot go down there. The bridges are blown out.' For Hezbollah, the actions were doing the speaking. And I guarantee that if you poll that region of Lebanon right now, Hezbollah's marks have gone right through the ceiling because they showed with their political arm that they cared. This is as important for future operations, as the conduct of the war."*

By contrast, participants concurred that current U.S. warfighting capacity was compromised by the lack of a clear core narrative that synchronized the warfighting effort and endgame from "*top-to-bottom, across the full spectrum of national power… I am not sure that everyone across the U.S. government can articulate the same message.*"

Participants noted three ways in which the U.S.' lack of an appropriate core narrative has undermined agility and credibility on the battlefield:

First, agility was lost in the hierarchy of approvals and a risk-averse leadership: "*We have to stop, get things approved, and make sure everyone is on board before doing anything. And beyond this, we have a risk-averse leadership that is very concerned with who is going to give what briefing and how messages are aligned.*"

Second, "information fratricide" occurred, where a "*piece from the Department of State suddenly undermines everything that we're trying to do.*"

Third, the original strategic narrative "*didn't get us to the endgame. It is great going in with a narrative of 'shock and*

"

Speed comes from everyone understanding the core narrative. If everyone understands the core narrative, you can rapidly improvise and respond at the local level.

I am not sure that everyone across the U.S. government can articulate the same message.

[54] Psychological Operations

awe' and how the enemy is going to lay down its arms and flee, provided that it takes you all the way to the end. But when you give a speech saying 'mission accomplished,' all the enemy has to do is show that this has not happened."

Participants stressed that synchronicity does not mean message control: "*A message that is closely and carefully coordinated is, by definition, not credible. If we hear six people come in and tell us the same things, we know that their boss told them what to say.*" Rather, the goal was a core narrative and national policy that set the left and right parameters, within which all agencies and all levels – from the President of the United States to the lowest echelons — could "nest:"

> *"That core narrative is difficult, but it is the essential part. We are failing at the very highest level, at the National Security Council, to get that clear policy out there and then disseminated down to the right people."*
>
> *"The notion of nesting does not mean a coordinated response, rather it means something that is mutually reinforcing and complementary across levels. We'd like a clear strategic message to be set, but with CoComs on the ground to have the flexibility to tailor their messages in a way that is consistent with the strategic intent, but also responds to their particular local circumstances, and is congruent with their other operational activities, not just informational activities."*
>
> *"Credibility is serviced when the message is nested both horizontally and vertically, from the President to the Soldier that is immersed in native populations."*

The challenge of synchronizing all elements of national power around a shared core narrative is compounded by the many different audiences that will hear and interpret U.S. actions and words. And ultimately, this effort is "*not always or even frequently a DOD problem or solution.*" While DOD has its own challenges to wrestle with — like the need to synchronize PA and Information Operations (IO) — overall strategic coherence requires a truly national effort. As one participant observed:

> *"The military can't do this alone. We are fooling ourselves if we restrict ourselves to the Department of Defense. This is about generating changes in behavior, belief and attitudes of people. It is about content and technology, but first we have to attack the strategy. To do that, we have to look at the people, and what we want them to do, believe or value. In other words, it is about political warfare. What we need is an organization similar to what the British had during World War II. They had a political warfare executive – a small organization that carefully constructed the entire British government response to what we now call the information environment. But they attacked the adversary's strategy – not the trenches, except where it was required to do so."*

We return to these issues in Part 5.

Part 3.

Countering new media: Special considerations

> *"New media allows penetration of the message anytime, anywhere to anybody. That makes it impossible to defend against in a kinetic sense. The media is the means; the message is the weapon. So countering is really about the message."*
>
> — Workshop participant

Countering the adversary's ability to leverage new media involves denying, degrading and disrupting **the message** and/or **the media** itself. The first part of this equation — countering the message through proactive information engagement — was addressed in Part 2 of this paper. With respect to the media itself, most participants agreed that physical attacks to disrupt the media source were either futile or wrong-headed — except for specific, short-term operations that targeted command and control channels. Some, however, noted that sophisticated, non-lethal network attacks could be very effective — causing fog and friction — and that the range of options was underappreciated by senior leaders. Countering also raises legal issues, which, while complicated, require serious consideration.

Overall, participants concurred: "*The future is not to remove the message, but respond to the message.*" This section takes a brief, but deeper, look at the challenge of responding to the "big lie,"[55] and then turns to participants' views on attacking the delivery systems directly.

3.1 Countering adversary propaganda: Plan, be proactive, be frank

As already discussed, the key to long-term countering of enemy propaganda and images is ongoing proactive engagement (leveraging SAMMMS) to establish and maintain credibility with key audiences. But participants also stressed the need for a rapid reaction capability to counter the big lie and doctored or "spun" images. Falsified images are particularly challenging, given their seemingly greater truth-value: "*In my work I constantly see photographs accompanied by text that tells a story about what that picture is. Usually it creates a very emotional impact. It may be true or it may not be true. It is very tough for anybody from the outside looking in to know. We've seen the same picture — of young girls crying — with three different captions on it [that spin different stories of why they are crying and where]. If you want to refute that, you've got to get the facts and push back fast and hard. And we're just not set up to do this.*"

> "
>
> *The future is not to remove the message, but respond to the message.*

As already noted, the need to counter should be an assumption of planning for all kinetic operations. This necessitates having capacities and authorities in place to: film all operations;

[55] Capturing some of the more specific views beyond those already presented in Part 2 on countering through proactive engagement.

determine ahead of time what can remain unclassified for this purpose; rapidly declassify evidence; and, rapidly release information at the right levels.[56] Participants also underlined the need for improved capabilities in image forensics and all-of-government investigations to get to the truth:

> *"We need the ability to do video forensics in a rapid way because we're seeing a lot of doctored photos. The white phosphorus in Fallujah argument, for example. We need to go in with a group of experts who can say: 'This is obviously false because these are desiccated bodies. White phosphorus burns both body and uniform, et cetera et cetera.'"*
>
> *"The whole government needs to be energized and able to react quickly to dig into the truth of a story or image."*

Effective countering of propaganda also means changing DOD's long-standing attitude towards *authentic* bad news stories, which is to be slow to engage them. Part of the challenge is the time required for thorough investigation. Participants concurred that investigations had to be prioritized and expedited. Some participants also cited a lingering reluctance to deal with bad news. For example, a participant expressed his frustration with trying to get accurate information to fight back on a propaganda campaign in Iraq:

> *"An Arabic blog had allegations of systematic rape at Abu Ghraib. There were a lot of details that did not look right that we could use to try to discredit the blog. We went in to try to get information. And what we got was: 'Nope, we don't talk about these things.' That is the wrong answer. There needs to be much greater sensitivity that this is important information that everybody in our government can use to tell the story correctly."*

"

The whole government needs to be energized and able to react quickly to dig into the truth of a story or image.

Bad news needs to be engaged frankly and forthrightly. Credibility demands it.

Participants concurred that not every piece of propaganda deserved a response. Some wondered whether responding – especially if the response did not supply unassailable counter-evidence – might lend credibility to false accusations. Others noted that the counter message is best provided by third party validators, where possible.[57]

Overall, leaders require more training to enable better decision-making around which attacks require engagement and how: "*Senior leaders need to be in a proactive mode and enabled to decide which events need to be taken apart.*"

Wargaming — using a "Red Team" approach to analyze "what the bad guy would do" — would help to identify potential fronts and vulnerabilities and also to proactively consider appropriate counter-responses.

[56] See Part 2.

[57] See Part 2.5.

Finally, there was a recognition that new media's many platforms call for a more extensive surveillance capability and that DOD should mobilize its digital natives to sniff out and identify lies and misdemeanors as part of its ongoing response capability: "*The military at the lowest level has to be sensitive to what information is potentially useful to a foreign audience. They need to be collecting this and forwarding it to somebody.*"

3.2 New media as self-healing and viral: *"The kinetic response no longer works"*

A number of participants observed that physically countering the message delivery system — taking down websites or knocking satellite radio stations off the air — reflects the "*military's response to a lot of things, which is: 'shut it down.'*" However, this option is becoming less effective for two reasons: the self-healing properties of new media, and the viral nature of the GIE.

"

In the next war... bombing Al-Manar will be useless.

New media's multiple nodes and self-healing properties can degrade the effectiveness of a physical attack: if you take down a delivery system in one area, it can re-route and pop back up in another.

Drawing on the case study example, participants noted how the Israelis were unable to shut down Hezbollah's television broadcasts, despite massive kinetic attacks: "*The IDF certainly attempted to take down the Al-Manar (satellite station), but were only able to do so for a short period of time*" (see Box 11, page 46). They also observed that the redundancy of communicative ability is only going to become more entrenched, as new technologies like Internet Protocol Television take hold across the world: "*In the next war, it is not just people with satellite dishes that are going to see Al-Manar. The Middle East is one of the fastest growing markets for Internet Protocol Television and for 3G mobile networks. So even if you bomb Al-Manar, people are just going to go to their desktops or one of the 3G networks, and they are going to eventually get the information over mobile handsets. Bombing Al-Manar will be useless.*"

Participants also concurred that the viral nature of content in the GIE means that shutting down delivery systems does not necessarily stop the message: "*Once information has gone out on the net, it is already mirrored to the extent that there is just nothing you can do about it.*" This lesson comes from hard-won experience in Iraq:

> *"We tried to takedown or disrupt the jihadist extremist forums on the Internet. But we found that it did not work. If we took this one down or that one down, it just popped up on other sites – even on western sites. And we have now since discovered with peer-to-peer networks — those file-sharing websites like Megaupload or Sendspace — once a propaganda video hits that, well, forget about it. You're never going to stop that message. That is what El-Sahab[58] and their sympathizers are doing right now. They are putting their videos on those sites. Once it hits there, a thousand*

[58] El-Sahab is the media wing of Al-Qaeda.

> *people are downloading them within a couple minutes. An announcement comes up on a forum: here's the URL and you can go to it. And anyone can download it onto their desktops. So even if you take it off all the extremist networks, and off of YouTube, Liveleak and Metacafe, people still have it on their desktop and can just put it right back up somewhere else."*

Box 11.

Lesson from Lebanon: Bombing the delivery system doesn't stop the message

Hezbollah possesses the largest media organization of any political party in the Middle East region and has the capacity to directly reach a population of 200 million viewers via satellite broadcast, with a further unlimited number via its many affiliated and associated websites and blogs.[59] Its media flagship — Al-Manar — dedicates some 25% of it production capacity to "resistance" music and entertainment programs, many of them glorifying Hezbollah military prowess. Al-Manar distributes its video productions through a wide network of associated sites.[60] This content is then picked up by large networks of others — supporters or the simply curious — and re-posted to YouTube and other video sharing sites. Hezbollah also created popular first-person "shooter" video games that reinforce their "resistance" narrative, while building up a warrior ethos among its young followers.

Because Hezbollah's own and associated new media resources are wide-ranging and globally dispersed, they are difficult to track or shut down by legal or conventional technical means. Moreover, the low cost of operations and willingness of audience members to replicate and further distribute content makes the elimination of Hezbollah's informational reach difficult to achieve without a truly global agreement.

During the 2006 War, IDF strikes resulted in the total destruction of Al-Manar's main broadcast studios in Beirut, as well as its critical radio relay and rebroadcast towers. The IDF also undertook additional selected strikes against other telecommunications facilities, but not enough to totally disable them.[61] A UN post-war damage assessment concluded that communications were disrupted but not severed even in the south of Lebanon where most of the fighting took place. It is unclear from the public record whether the partial communications' functioning was a deliberate IDF strategy or not (that is, whether the IDF saw greater value in allowing some channels to function in order to gather intelligence, and/or, whether they desired some retention of Hezbollah's Command and Control network to allow for a rapid de-escalation after a ceasefire). Some sources also suggest that Hezbollah's Al-Manar "raised the negatives" for further IDF attacks by co-locating their facilities with the Lebanese national communications grid, so IDF strikes would result in significant collateral damage.

In the final analysis, the kinetic and electronic attacks against Hezbollah facilities did not disrupt Al-Manar's broadcasting capability: terrestrial broadcasts continued, and the regional satellite feed remained intact. IDF public sources claim that the IDF was unable to successfully block the signals because of Al-Manar's switching of frequencies, and its redundant use of both satellite and terrestrial broadcast facilities.[62]

[59] Jorisch (2004). Available on: http://www.meforum.org/article/583

[60] Erlich and Kahati (2007).

[61] Arkin (2007).

[62] Cordesman and Sullivan (2007)

Experiences such as this have caused many practitioners to focus less on countering the media, and more on countering the message. As different participants noted:

> *"Shutting down the means is not the best method for countering the narrative of the adversary."*

> *"We struggled with this in Iraq: Is attacking a network the most appropriate way to achieve an effect? We found that normally attacking a network was not the best way of approaching the problem. Rather it was deciding what the alternative narrative was and how we will approach that to get the effect we needed."*

> *"In Bosnia, if you bombed a TV station, it was off the air. But in the 33 Day War, the Israelis learned that Al-Manar could not be taken off the air. What used to be the kinetic response – take it off the air – no longer works. This requires a change in tactics. The new tactic is to accept that the adversaries' messages will make it to the airwaves, via cell phones, text messages etc… and that you have to adjust your approach to deal with the message, not the originator."*

"

Shutting down the means is not the best method for countering the narrative of the adversary.

3.3 Physical destruction can incur negative 2nd and 3rd order effects

Participants stressed that the kinetic approach can be counter-productive on a number of operational and strategic fronts:

- **Physically destroying a communications node can create longer-term problems for post-war stability, and is often unnecessary**. In Iraq, the kinetic takedown of certain communications infrastructure created liabilities for the stability ops that followed. But the kinetic approach wasn't essential: other less lethal means could have denied the adversary's use of key nodes for the time period required, and thereby achieved the same objective. Likely, however, the commander was not aware of the potential alternatives (see Box 12).

- **Destroying radio stations and blocking websites plays into the adversary's "Goliath narrative" and can compromise the broader strategic communication effort.** Various participants stressed that heavy-handed approaches can negatively affect the broader strategic communication effort:

  > *"Countering new media by taking down your adversaries' communication means is as counterproductive as telling your Soldiers not to communicate. What gets highlighted is that you are against free speech. It never seems to work."*

  > *"Blocking websites or blasting radio stations often plays into the adversary's narrative, and ends up reinforcing a message of 'that big old nasty American Goliath.' …I want to just remind everybody that the United States is all about freedom of speech, so if we go in and temporarily take out a method of speech – how we do this can create long-term effects that we have to look at."*

Probably, there wasn't an IO guy in that planning committee.

"You can do it by fires, but you have to understand the consequences. You have the U.S. taking out a media center. But we have a first amendment that says free press. So all of a sudden we get severe blowback from the American public asking why are we doing this?"

"If we are trying to build democracy, then democracy requires respect for people's points of view, once they have their own government I'm not sure how you can build that on the basis of controlling a message during the operational period. There may be short-term tactical reasons why you have to do that – why you have to take out a radio station, why you have to control a certain message. But our preference has to be on encouraging more voices to talk…but with ours being the most credible."

- **Blocking can draw even more attention to the issue you are seeking to bury.** A participant shared an example from Bahrain, where the government banned Google Earth just days before the elections. Bloggers had been using Google Earth to show how the Shia slums were buttressing up against the massive Sunni estates in the country, which was not a welcome pre-election issue. So the Bahraini government banned Google Earth for a period of time. This only drew more attention to the issue, and ended up being counterproductive in the long run.
- ***"With technologies like cell phones, we're using that infrastructure too."*** As one participant noted: "*For us the issue was a particular cell phone tower. Cell phones were being used to pass information by a particular organization. But in deciding whether to do something about it, we were stuck with the dilemma that we were using that capability as well."*

Box 12.

The negative operational consequences of kinetic action against communication nodes

Participants shared their experiences with the negative consequences of kinetic action that destroyed communication nodes in Iraq:

"I was advisor to the Minister of Communications, and my job was to reestablish the communications infrastructure. I went downtown to the Al-Mamoom switch in Baghdad. This is one of the two host switches…and we had j-dammed the crap out of it. When we did that, we knocked out communications for about two-thirds of Iraq. That means we took out the fire and rescue guys, we took out the police, and there was no way to organize citizenry. And I thought: 'What if we had used one of our other capabilities, to just suppress the use of this thing. And then when we came in and took it over, we could control the switch for positive things. We would still have achieved the effect we needed. We could have denied, suppressed, the use of communication and denied the Iraqis in Baghdad from using local telephones. And then when we came in, we could get it up and use it to organize rescue etc.'"

"Probably, there wasn't an IO guy in that planning committee, someone who could say: 'I think you want to deny this. But what if we can achieve your objective, but also keep this

> *capability so we can use it when we get in there? This capability [can help] to organize rescue and support operations, and bring leaders together…'"*
>
> What is the lesson? *"Yes, you can use kinetics to take out a command and control node. But you need to understand the longer-term consequences; you need to think down the road. [Initially in Iraq] we were all about kinetic strikes. And one of the missions was to suppress the enemy's ability to command and control. We had to cut them off, and we know how to do that. But we also need to do a little deeper thinking."*
>
> Another participant concurred: *"It was the same thing with the television stations, but immediately they were broadcasting from somewhere else. And I thought the same thing. Why did we destroy that? Because now we don't have it available for stability ops, and to communicate with the local population. And, more than that, it created a void that was filled by broadcasts from Iran and Syria that were also counterproductive to our objectives."*

3.4 Physical attack can be essential for operational success

While accepting the potential for longer-term blowback, a number of warfighters stressed the need to reserve the "physical attack option" for specific operational purposes: "*If I can jam SMS in a one block radius for twenty minutes, I might be able to do what I need to do.*" This was especially true for media used by adversaries for command and control purposes, which can be effectively disrupted for short periods of time:

> *"I'm not looking to control the debate or alter content. What I want to do is buy time."*
>
> *"There's a huge difference between jamming a radio station for twenty minutes, and putting a bomb through the building."*
>
> *"I want to retain the capability to take apart large parts of the network – to degrade and delay my adversary's capability. Whether this is for a couple of hours or a couple of days, it costs him time and money."*
>
> *"If we look at the Lebanon War, Hezbollah was getting out their casualty reports before Israel. And we saw how this proliferated on the new media… But somewhere in Lebanon there was a terminal – a communication device that was used to get that initial message out. Had the Israelis been able to interdict that for two days, they would have bought themselves the time they needed to release their reports. That's all they needed – two days. And it would have created a different effect, a different impact on perceptions. Offensively attacking a delivery system — at the right time and place — may be exactly what you need."*

Participants also concurred that, in certain circumstances, media that were actively inciting the population to violence should be targeted: "*An example is Rwanda in 1994, and the Radio Milles Collines (Radio of a Thousand Hills). The station's producers and journalists were calling for war crimes. They were literally saying: 'Let's all go kill Tutsis at this spot.'*" So while kinetic operations are not preferable, "*they are sometimes an option, and indeed a preferred option.*"

Some warfighters also contended that killing the adversary's collector of information is important for mitigating threat. The adversary's media-focused end-game has expanded the range of targets for lethal action — like the adversarial cameraman filming operations: "*If you have just been IED-ed and you see the cameraman filming it, then kill the cameraman, just like you would take out a sniper.*"

"

To go into the dot.com world as an attacking military organization? It is not a simple problem.

3.5 Network attacks: A palate of options, but complex legalities

Participant discussion of certain issues – like computer network attacks – was limited due to classification issues. However, they stressed that the geographic ambiguities of new media has raised a tangle of complicated legal issues:

> *"This is an incredibly complex problem: you can't just change legal authorities. To go into the dot.com world as an attacking military organization? It is next to impossible. You have to be able to build a package to justify going into the dot.com world and taking down a public website — because they are recruiting, for example. It is not a simple problem."*

Some participants stressed the need to train senior leaders on both the extent of the threats that are out there, as well as the many options for mitigating them. A particular challenge is that "*88% of websites are housed in the U.S.*" and commanders automatically think that they are untouchable. One participant argued that this is not necessarily the case:

> *"I want to deny access to a particular video that shows how to make an IED, okay? The first question we'll get is: 'Where is the server?' So let's say it is in Tampa, Florida or the Netherlands. Then they will tell us: 'You can't go after that.' But I tell them that they are missing the point. I'm not going to attack the server – I am after a particular piece of information. And this is the kind of discussion that we got into, because they were thinking that I was going to do something physical – that I was going to go after the physical box. But that is not my target. My target is to disrupt and degrade that information so it can't be used to train people. Do you see the debate?"*

Similarly an external Subject Matter Expert (SME) noted the range of options available to degrade information and compromise its apparent veracity in the eyes of receivers: "*Computer network attack operations... can be pretty complex. You can deny information resources, you can pollute information resources, you can compromise their seeming veracity, you can manipulate them in different ways. And you can do this in a very precise manner. Moreover most of the technology to do this is off the shelf. It exists. And there are at least 61 countries that [my research organization] knows of that deploy this capability against things that are of a political nature for them, and that they want suppressed. And we've seen it deployed in very ingenious ways – like 'just-in-time' filtering: Rather than denying a resource all the time, you just slow it down; you undermine its credibility in different ways so that people stop paying attention to it.*"

The SME wondered whether the issue was only a problem of legal authorities, or also a lack of knowledge, where "*senior leadership is not culturally attuned to recognizing that there are* *options out there that are the informational equivalent of a kinetic precision weapon."*

In response, a participant confirmed that lack of awareness was constraining the palate of options that could be pursued: "*Many of our senior leaders do not have the experience and formal training oriented to putting the [information disruption] piece first. They are not predisposed to thinking: 'What can I do non-kinetically to achieve my effect?' I have crashed many parties at CentCom – just walked into the planning meetings and said: 'Hi, I am the IO guy.' And they say: 'Oh yeah, we need some of that.' It has been getting better, and now some guys have seen us enough times to know that they need to ask for it. But I think it is going to require a generational change."*

A participant noted that although DOD has various methods for effective computer network attacks, their timeliness (and hence effectiveness) is stymied by permissions: "*We have about 10 things that we use. But you go through this very lock step, very detailed time-consuming process of getting permission and authority to use a specific capability against something. You want to deny this service or do this thing because it is encouraging attacks against coalition forces... but it takes a long period of time."*

In summation, a participant observed that, legal issues notwithstanding, DOD needs to "*overcome its lack of creativity and expand the toolkit – with someone assigned to offer the non-kinetic options that we can do. We need to understand the options better. And we need to further define the legal ways of combining lethal and non-lethal action to achieve the commander's intent."*

"

Senior leadership is not culturally attuned to recognizing that there are options out there that are the informational equivalent of a kinetic precision weapon.

3.6 Holistic approach

Overall, most participants concurred that countering the adversary's use of new media required a holistic and scalable approach – a careful combination of both soft and hard power. Engagement and establishing superior credibility with key audiences needed to be backed up by the technical capabilities to "*slap these things down when needed: If you don't have both, you're always going to be operating like a one-legged bandit."*

Participants that were well-versed in the wide palate of potential tools that can be brought to bear in this arena stressed that commanders require a better understanding of the potential options open to them, and the potential 2nd and 3rd order effects of physical action against the media from within a strategic communication perspective. The main thing is that the commander's staff needs to give him the full palate of options, based on a comprehensive situational assessment: "*The staff's responsibility to the commander is to lay out the range of responses and options so he can decide what is appropriate to address this particular requirement. You can shut it off or you can do nothing but there are a lot of things in between."*

Part 4.

Operations Security (OPSEC) in the age of radical transparency[63]

> *"As we build our strategic communication capacities, we open up OPSEC vulnerabilities. Understanding this can help us to mitigate those risks now and in the future."*
>
> — Workshop participant

Al-Qaeda's Encyclopedia of Jihad states that 80% of all intelligence needed for an operation can be sourced from Open Source Intelligence (OSINT). The remaining 20% requires direct surveillance.

The contemporary operational environment is awash in new challenges for preserving OPSEC. New adversaries are closely attuned to the prospects for aggregating vital intelligence from open sources like the media and the Internet. At the same time, the volume and global dissemination of military-related information has expanded exponentially. Examples of OPSEC challenges include:

- New media-enabled tools – such as video-enabled cell phones (which can also provide geo-located coordinates), Internet, inexpensive remote-sensing GIS, Google Earth, and satellite communication devices. Current theaters of operation are awash in a wide variety of folks — Soldiers, coalition partners, contractors, NGOs, foreign and domestic media, adversaries, local indigenous civilians — who use these devices, and can inadvertently or purposefully capture and disseminate sensitive information. Previously, "OPSEC involved controlling Soldiers; today it applies to anyone with access to new media in the military operating environment;"[64]

- Modern military forces drawn from "communication" societies, meaning those with instant and readily available communication means, and an attendant culture/ expectation of 24/7 connectivity. Constant communications back home, text messaging, participation in social networking sites and mil-blogging all have the potential to increase OPSEC risks, expose operations and endanger the lives of troops;

- The heterogeneity of coalition partners, NGOs and international organizations, which makes strict OPSEC rules difficult to set and enforce. Communication discipline can become compromised, as communications equipment and protocols are geared towards information sharing and coordination: "*There is a cloud of people around you with communication feeds that you can't interfere with*;"

- DOD's new imperative for speed in communications – to explain events, pre-empt propaganda and get the accurate story out.

[63] Chapter title from Murphy (2009).

[64] OSIA (Open Source Intelligence Analysis Network). Sourced from: http://osianintel.com/AQOSINT.aspx

“

Many Soldiers think that with all the emails that people send all across the world, who is going to be looking at mine?

Participants concurred that the commander’s ability to control OPSEC has been greatly diminished. Discussions centered on five main issues linked to new media: internal challenges (expectations and use by Soldiers, Sailors, Airmen and Marines); external challenges (use by others in the operational environment); the speed-OPSEC conundrum; planning and risk; and, enhanced OPSEC opportunities. We look at each in turn.

4.1 Internal challenges: The expectations and culture of deployed digital natives

The current generation of servicemen and women are digital natives. They have expectations for 24/7 communication and are savvy in their use of, and presence on, any number of digital communications platforms. Most also embody a culture of communicative openness, with few qualms about sharing private information and thoughts on “personal” communication media. Disturbingly — especially concerning recruits into the military — the proclivity for openness is not always tempered by a sound understanding of the potential for unintended “others” to view personal postings or listen in on cell phone conversations. As various participants observed:

> *“This generation has grown up with a different attitude about private and public and being able to separate those two – especially on social networks. They will say, ‘Well that’s my private space — why should you care what is on there — on my private space?’... And I can simply go to my son’s MySpace page and I will tell you he doesn’t get it. He doesn’t get it that his grandmother can potentially see what’s on that page. That is how I try to shame him into changing it. But my son isn’t any different from any young person who’s a Soldier, Sailor, or Marine. It is an issue we face. And it is hard — in my experience — to drill this caution into them.”*

> *“The acceptable behavior for our generation is not exactly the same for the generation that is actually using and engaging in the new media technology.”*

> *“Many Soldiers think that with all the emails that people send all across the world, who is going to be looking at mine? Why can’t I tell my wife that we’ve moved to Baghdad from somewhere else?”*

> *“In Lebanon, IDF Soldiers blabbed their locations and other sensitive information during cell phone conversations home. When confronted, offending Soldiers said: ‘But I was speaking in Hebrew. Hezbollah doesn’t speak Hebrew.’”* (Box 13 on page 56 provides other examples of how new media were implicated in IDF OPSEC violations or vulnerabilities in Lebanon.)

> *“It is pretty easy to maintain OPSEC when you can’t call your wife from the battlefield. But when you send her an email every two hours and give her a call every night...well...”*

> *"There is a group on Facebook that is called the American Intelligence Community. It makes me wonder: 'What are you guys thinking?' Even if they are overt employees… this is really, really foolish. But they are doing it. I don't know if it is legal or not."*
>
> *"Back in my day, when my Mom sent me cookies, I burnt the return address. I think that one of the challenges related to new media is to instill that same kind of fear and healthy paranoia into the Soldiers about things like Facebook and MySpace as well. I certainly would not have either of these things if I were still on active duty."*
>
> *"These [new] guys don't make the connection between OPSEC and MySpace or Facebook. And let's face it: 'A nineteen year old kid has been on Facebook a whole lot longer than he has been in the Army.'"*

Experts noted that social networking sites can be a "disaster for national security:" "*Give me the name of somebody in your unit, and in five minutes I can map the entire unit. I can draw a lot of valuable intelligence from these sites, that would otherwise take me hours or days of interrogation.*" Another participant stated: "*If I were a commander in the field, I would forbid my Soldiers to have a Facebook site. I would check, and I would forbid any kind of social networking account – certainly while we were deployed.*"

A challenge, here, is that senior staff are often digital immigrants – meaning they do not understand the range, scope and potential exposure of new media platforms. As one participant noted: "*We have been slow in reacting… The reason we have not had a crackdown on Facebook or MySpace is because the senior NCOs and officers are too old – they are these immigrants that we are talking about. So we have been slow in responding to the problem.*"

"

A nineteen year old kid has been on Facebook a whole lot longer than he has been in the army.

Participants concurred that the solution for improved OPSEC was not to cut communication off or prohibit cell phones. They noted that times had changed. Thus, some participants remembered deployments and training deployments where the rule was no communication for seventeen days. Current cohorts, however, have different expectations: "*We have realized that the medium of the cell phone has permeated the ranks. So instead of trying to uphold a policy that we can't hold our Soldiers to, we have to figure out what is the right way to do this – what it is OK to say.*"

Especially in light of the longer deployments, commanders stressed the need for Soldiers to communicate with family and friends: "*Our experience has been to allow them to do the things that they can do to make that deployment better for them. So that when they come off of an intense operation they can come back and relax. If they can't talk to their circle of friends, this can become dangerous, especially after 15 months, or even after 8 months. I mean these people are dying.*" And, as another participant observed: "*When you are on a 15 month deployment, you get lax. You start to break down a little bit… It is easier to keep OPSEC in the first three months that you are deployed than in the last three.*"

Box 13.

Lesson from Lebanon: New media and OPSEC in the Israeli-Hezbollah war

The 2006 Israeli-Hezbollah War revealed OPSEC challenges that are inherent to the contemporary operational environment — from Soldiers calling and blogging home through to detailed media reporting and cell phone geo-location. Throughout the war, Israeli tactical intelligence — such as frequencies, war room and operational maps, battle plans, special weapons, and even Soldiers' interactions and internal dynamics during battle — was available on the Internet. In the words of IDF General Amidror: "The Internet guarantees the intelligence community a long life of mutual challenge though I have doubts as to who will win in the end."

Many IDF Soldiers went to war with their mobile phones. Israeli Soldiers are used to being "plugged in" within their mainstay deployment areas – the West Bank and Gaza. These territories are covered by commercial Israeli ISPs and cell phone providers, and Palestinian militants possess no significant SIGINT capability or expertise. As a result, it became the norm for IDF Soldiers to carry consumer electronic devices into operational settings, and many took their phones along to Lebanon. As one analyst reported, "While in most units, the quartermaster collected all phones prior to entering Lebanon, some Soldiers kept their phones with them, and when possible, made use of them for calls, SMSing and even photography." When IDF Soldiers called home, they often revealed operational details to their loved ones (e.g., location, what they were doing) and at least some of this made its way into media reports and websites.

Soldiers also blogged, at times revealing operationally sensitive information. The military censor was forced to call upon all bloggers and forum contributors to exercise self-censorship.

Post-war reviews by high-ranking IDF intelligence staff and other data security researchers concluded thaat some of the operational information available on the Internet during the war — gleaned from cellular communications, digital photography and video — very likely compromised operations. For example, operational information was readily available <u>during</u> the battles in Bint Jubeil and Debbel, where Israel suffered severe losses.

There are strong indications that Hezbollah made significant use of OSINT — gathering valuable intelligence from Israeli press and news broadcasts as well as websites. Reports suggest that Hezbollah used Israeli press reports to plot the location of its rocket strikes in Israel, and may have used Google Earth to help re-calibrate the accuracy of its fire.*

Hezbollah apparently also used SIGINT, as evidenced by the IDF capture of sophisticated intelligence equipment from Hezbollah bunkers. Evidence suggests that Hezbollah used this SIGINT product in at least two ways:

1. To ascertain IDF location and deployment information. Hezbollah seems to have exploited IDF mobile phone usage as a surrogate "blue force tracker," to reveal location information. While it is difficult to prove this point for certain, some of the equipment seized by the IDF from Hezbollah bunkers revealed a capacity to hack into commercial Israeli cellular phone towers along the border. This would have allowed them to geo-locate the cell phones carried by IDF Soldiers in the South of Lebanon. Hezbollah may also have broken into the IDF's tactical cellular phone communication system (MountainRose).** It is likely significant that, immediately following the war, the IDF reactivated a unit (Ayit) tasked with monitoring IDF communications and OPSEC, which had been deactivated a few years earlier, following the withdrawal from South Lebanon.

2. **To report IDF casualties accurately, and more quickly, than the IDF itself, which caused a "credibility gap" for the IDF.** Throughout the conflict, Hezbollah media sources consistently reported the number and location of Israeli casualties faster than IDF sources. This had a negative effect on Israeli public perceptions, as reports made by Al-Manar were picked up by Israeli media or disseminated on Hezbollah's Hebrew language service. The slowness of IDF reporting may have been a function of OPSEC considerations (as an early release could threaten ongoing operations), as well as the need to verify casualties (and their identities) to ensure that families of the deceased were the first to be notified.

* Several groups unaffiliated with Hezbollah used Google Earth to plot the geographic and temporal location of both Hezbollah and Israeli strikes during the war. Hamas has been reported to use Google Earth to calibrate its rocket fires.

** "Mountain Rose" was extended as IDF units advanced by use of transmitters in tethered AEROSTATs. Israeli press reports (not published in English) suggest that the system itself may have been inherently insecure potentially allowing unauthorized access to highly sensitive material such as classified documents, which could be obtained by way of a simple search. (For more information on Mountain Rose in general, see: http://defense-update.com/products/m/mountain-rose.htm)

Some participants noted how in certain areas in Iraq, one of the first capabilities set up for Soldiers was Iraqi Internet access:

> *"I operated in some remote areas and before I could ever produce any kind of Internet capability to even talk to my company commanders – I would leverage an Iraqi in a small time business to set up a connection for the Soldiers. We let our Soldiers use that system so they could email home – to fulfill that 24/7 expectation. But we were very clear with them. We would say, 'Look you put yourself at risk, you put the unit at risk, understand that.' And occasionally sergeants would check on them to make sure they were not saying something stupid on the web cam or something. You catch one every once in a while, you have to keep checking and reinforcing it."*

A number of participants expressed alarm at this policy: "*If I were an adversary, the first thing I would do is set up an Internet café the Soldiers could come to — because I could capture all that data on my own in-house server.*" Some wondered whether DOD currently has SIGINT capability to understand "*who else is listening when these guys are emailing home at vendor-operated Internet cafés.*"

Overall, the challenge is to balance issues of Soldier morale and expectations, DOD's new imperatives for information engagement,[65] and the potential security risks. Participants concurred that the main antidote was a combination of education, training, discipline and trust. The circle of education and trust must also include Soldiers' families, so they understand the potential risks:

> “
>
> ***If I were an adversary, the first thing I would do is set up an Internet café the Soldiers could come to — because I could capture all that data on my own in-house server.***

[65] Which, as already discussed in Part 2.5 above, places a premium on encouraging servicemen and women to engage in blogs and other platforms to "tell the Soldier's story."

> *"Since the late 1970s when we made this an all volunteer force we moved away from the idea of controlling to the idea of educating, training, encouraging, and influencing. You know, when I was an enlisted Soldier in 1979 they were opening my mail. When I became an officer in 1983, we were no longer opening anybody's mail. Instead we focused on educating, training, encouraging, and influencing – and this has been successful with the all volunteer force."*

> *"I think the majority of these issues are really about Soldier discipline."*

> *"All OPSEC is based upon our culture, which means trust. I work in a classified environment. The only thing that keeps me from walking out with a ream of Top Secret classified documents is trust. I have swipe access and can do anything I want. But it is the trust in who I am, and people knowing who we are and what the mission is, etc. That is what OPSEC is all about. And it can be reinforced by the chain of command inside that brigade, but that is what it boils down to."*

> *"We can overcome the OPSEC piece if we educate our Soldiers properly on the ramifications of the use of the new media and the kind of messages they're putting out across it. We give Soldiers M4s, live ammunition, and we trust that they're not going to shoot their buddy in the back because we properly trained them to use that M4. We've got to do the same thing with new media. We've got to properly train them on how to engage targets or engage audiences with the new media apparatus."*

> *"The families have to be trusted too because their loved ones could be put in harm's way. The families blog openly. They need to be aware of the risks."*

"

We give Soldiers M4s, live ammunition, and we trust that they're not going to shoot their buddy in the back beause we properly trained them to use that M4.

While some participants thought that most users – whether civilian, military or intelligence – had a healthy paranoia about putting too much personal information out on the social networking sites, others disagreed and stressed the need to instill this caution from the beginning – during basic training. One participant shared his experience with adjusting the training piece so that the digital natives "got it." He noted that the traditional training material was often still stuck in the "loose lips sinking ships" era, which didn't resonate:

> *"When you go through the OPSEC briefings...you usually get the same old World War II posters with loose lips sinking ships. But these guys on MySpace and Facebook – they don't relate to that. So, as I was briefing a National Guard unit preparing for deployment, I said: 'If I was Al-Qaeda, Facebook would be a gold mine for me.' And then I made up a story about a family being killed by terrorists, while a Soldier was on deployment. They said: 'Where did that happen?' I said: 'It didn't...but do you want to be the first? What do you have up there?' And that resonated throughout, not only with those being deployed, but also with those back home."*

Participants concurred that leadership needs to set the rules of engagement for new media use, along the same kind of paradigm used for kinetic strikes. As one participant summarized: "*Essentially, you provide your Soldiers a field to play on. You tell them what they can do, where the boundaries are, and – if they start moving toward the edges of those boundaries – you have something in place, whether it is retraining, or punishment, or whatever, to bump them back into the playing field.*"

Of course, violations will happen, and monitoring is important.[66] One participant recounted how one of his bloggers released pictures that inappropriately revealed capabilities. The challenge when this happens is dealing with the problem in a way that doesn't scare everyone else into silence (as this counters the push for encouraging DOD's information engagement). Participants concurred that violations had to be dealt with on a case-by-case basis, with a clear understanding of the intention of the Soldier.[67]

4.2 External challenges: The need to better define critical information

Participants concurred that the "internal" challenges around OPSEC were, in the end, more easily dealt with than the external ones: "*When we start looking at the third country nationals out there and someone else that has a cell phone – that is much, much, more difficult.*" The move towards greater interagency coordination and information sharing has also increased risk.

This broadened risk environment requires greater attention to the careful definition of *essential* OPSEC information – the stuff that must be secured in order to protect the operation and mission. And then, "*you put things in place so that even if there are people inside the wire with their cell phones, we can focus on what not to talk about as opposed to 'don't talk about anything.*'" This new imperative, participants agreed, goes back to the old imperative of planning.

> *We just stamp everything secret... because a more nuanced assessment requires a tremendous amount of work, and we don't have the time to sort out what should really be secret.*

4.3 Speed versus OPSEC conundrum

OPSEC considerations often underpin the "system latency" that makes DOD so much slower than the adversary in getting their story out into the public domain (see Part 2). Some participants thought that DOD's caution with information was unnecessarily restrictive: "*In my experience, it seems we just stamp everything secret. It is the safest thing to do, because a more nuanced assessment requires a tremendous amount of work, and we don't have the time for it – to sort out what should really be secret.*"

[66] Some participants observed that the 2007 U.S. Army regulations on blogging – such as the requirement to register blogs – could be counterproductive to the entire concept of blogging (which values personal opinions and freedom of speech). Moreover, others noted that according to the Army audit, DOD's official sites were responsible for some 1,800 breaches of OPSEC, compared to only 28 breaches that occurred on Soldier blogs. See also Melber, (2008).

[67] See also discussion on Soldier's blogging in Part 2.5.

A participant explained the two-step process: "*First the INTEL guys have to scrub it – remove anything that is going to compromise OPSEC in terms of protecting assets, locations etc. And then once they are okay with it, there is a process leading to the decision as to whether the remainder can actually be released for use.*"

More than a few participants agreed that — given the stakes — it is important to start with stamping everything secret, even if that means a delay in getting the story out:

> *"We have been told to get the story out. When we do that we sometimes have OPSEC violations. For instance, we had a situation where the Air Force released an image, but they didn't check with the Army or the Marines. It contained information on certain equipment and capability that turned out to be an OPSEC violation. So the question is, who should have released this photo?"*

> *"There is a balance with getting the story out and OPSEC. Is it worthwhile to tell this particular story? It may result in a short-term ephemeral victory. But it may also incur a long-term compromise in capability."*

“

We have been told to get the story out. When we do that we sometimes have OPSEC violations.

Others, however, thought that "*sometimes your story* ***is*** *the most important thing to get out,*" and that much more could be done to enhance the speed part of the equation. Evidence from Iraq — where powered down authorities and an *in situ* capability for rapid declassification (see Box 7 above) — was cited as a promising example for the future.

4.4 Planning, Red-Teaming and a more sophisticated risk calculus

Ultimately, the key for maintaining essential secrecy in the age of radical transparency is planning, backed up by Red-Teaming, training and diligence. Absolutely critical information must be identified and protected, with full knowledge of the enhanced potential for information leaks (new media, internal cultures, external players, pressures to engage) and the adversary's enhanced capabilities for OSINT:

> *"There is an information environment that I cannot control, but that doesn't mean that I cannot plan to mitigate risk as I go forward in my operation. As long as I am attuned to it and understand it and realize that there are things that can happen. I will therefore take steps to mitigate risk... It remains an inherent command responsibility executed through the operations staff — not the security or intelligence staff — to choose those critical bits of information that we must protect from Red."*

> *"You have to recognize in the planning phase that everything you are doing is being observed by someone, and their ability to share information is much quicker than before. So you need to ask: 'What are they seeing of me?'"*

Red-Teaming is an essential part of this exercise – a lesson re-learned by the Israelis during the 2006 war with Hezbollah.[68] Participants noted that DOD was already doing this. However a number thought that the effort was likely underfunded, and "*with the pervasiveness of new media, probably needs more enhancement.*"[69] (See also Red-Teaming discussion in Part 3 above).

4.5 Leveraging new media to enhance OPSEC: Reducing footprints, OSINT and deception

New media can also be used to enhance OPSEC, although DOD's efforts and creativity in this regard are still limited. One participant stated that more thought should be given to using collaboration and information tools to reduce the military signature and "*oozing of information. You can connect and share information electronically, so you don't have to move units around as much. You can set up your own Internet cafés. You can provide capabilities to the locals so that if you have to deal with the local mullah or you have to deal with the local leaders — you have a means to also meet electronically, to reduce the need for constant movement.*"

> "
>
> ***Al-Qaeda has been using Facebook and other social networking sites to pursue deception.***

Other participants thought that DOD was not exploiting the OSINT available on places like Facebook aggressively enough. An example was the car-bomb attempt at Glasgow airport, where the perpetrators had written about it in advance on their Facebook account: "*This is something that could have been tracked. But unfortunately, the intelligence community has not been aggressive enough about exploiting the social networking platforms.*"[70]

Of course, there is no "truthometer" that screens the information on these sites or establishes whether a "person" is real or not, so Blue Team collectors could also be deceived by the OSINT they find. Indeed, reports suggest that Al-Qaeda has been using Facebook and other social networking sites to pursue deception.[71] At the same time new media — and new adversaries' strategies for monitoring it — provide an excellent opportunity for Blue Team deception to protect OPSEC: "*to put out wrong information on various platforms to confuse them if they are monitoring us. You can do deceptive OPSEC this way with very little effort.*" Some participants wondered, "*Why aren't we doing deception across Facebook?*" Others, however, confirmed that tactical deception with new media in mind has been happening: "*I can say that I personally have led or planned operations that appeared to look one way specifically because people would see it, report it, and blog it.*"

[68] Following the war, the IDF reactivated its counter-surveillance capability, whereby it conducts SIGINT on itself. The purpose is to identify the various weak-points for information security and message security, both in terms of official military channels, as well as in terms of private communications.

[69] They also noted the challenge with retaining this capability: *"People trained to that level of surveillance are very desirable. So you end up training people that often times get poached or go to better compensated jobs. It is a difficult problem."*

[70] The Open Source Center was set up to get at this shortcoming.

[71] See, for example, Bruhl (2009). Available on: http://soldierblogging.blogspot.com/search?q=some+lurking+OPSEC

While participants noted that deception and OPSEC often go hand-in-hand, others sounded a note of caution around using new media for this purpose, given the lack of control over information once it is out: "*You have to be very careful with using deception in an environment that you do not have much control over. Traditionally, deception and OPSEC have gone hand in hand to support each other. But this environment makes deception much more difficult because of the risk of being compromised. If your deception gets out in the free press, the damage to your credibility can be dramatic.*" This potential for blowback is especially strong in counterinsurgency and stability operations. The dilemma is that the same people you may need to deceive to protect OPSEC (NGOs, contractors, and especially the indigenous population) are the people that you want to trust you. Once the operation is over and the deception is apparent, will you ever be credible again? This is a big price to pay in an environment when maintaining the trust of the indigenous population is a top strategic priority.

Part 5.

Seizing the new media offensive: Priority issues

> *"There are incredible opportunities in this new media today. We have two options in the DOD. One is that we keep our heads buried in the sand. The other is that we embrace it and use it."*
>
> — Senior leader at the workshop

Participants concurred that: "*New media are a reality. It is not something that is coming. It is here. It is pervasive. And, we must adapt to it.*" They also recognized an array of cultural, bureaucratic and legal impediments that were hindering DOD's ability to achieve strategic agility in the new media age. Priority issues include:

1. **Recognize that the winning strategy is *information engagement*, not *information control*.** New adversaries seek political victory as determined by the popular opinion of key audiences.[72] Their warfighting strategies prioritize the creation of "information effects"[73] rather than decisive military operations, and new media have extended their reach to distributed global audiences. Beyond this, new media have made it impractical to control information. Winning in today's operational environment demands proactive information engagement — meaning an ongoing conversation with key audiences at the local level, in the idioms and on the media that resonate — to establish and maintain trust and credibility. This is true for current areas of operations, as well as areas of future concern.[74] Participants concurred: "*We need to establish, plan and train for a culture of engagement from top-to-bottom and across the spectrum, with rules of engagement that enable the freedom to act with acceptable risk.*"

2. **Embrace new media as a significant enabler of "*that element of combat power called information.*"** While the strategic impact of new media is already evident in today's wars, tomorrow's wars are "*going to be fought through new media. Because that is how messages are being disseminated and received.*" Participants agreed that the first overarching step for the U.S. government, and DOD in particular, must be to **recognize and accept** that new media are having a "*significant impact as the reach, influence and interoperability of the Internet and other devices are expanding... The U.S. government as a whole needs to accept this in terms of how they determine policies and allocate resources... And I'm not sure that we've accepted it yet.*" Other participants agreed, and noted that new media were often treated as a threat, rather than an asset: "*At a time when we are trying to deploy new media, we are actually shutting down the channels that allow us to use that new media. We need to look at access as one of the challenges*

[72] For example, ensuring that their own audiences accord them support and legitimacy, or undermining the political will of their enemies' domestic audiences and international supporters.

[73] As noted in the Introduction, a strategy that prioritizes the creation of information effects uses communication campaigns (often involving the careful media packaging of tactical lethal encounters) to shape the perceptions and attitudes of key audiences, to thereby influence their political will.

[74] As one participant noted: "*Leveraging new media to engage now with non-adversaries at the local level can help to diffuse future conflict.*"

we are looking at. I know that in the Air Force, I can't go to a blog site. I can't even get to blog sites from my office at the Air Force Academy. I imagine that is fairly true throughout the Department of Defense. If we are going to look at using new media, we need to look at the challenges that access presents from a security point of view."[75]

Overall participants concurred: "*We need to embrace new media better than the adversary, and to become so adept at it that we become — as we claim to be at the tactical level — the most proficient and professional force in the world. When do we turn to* ***this*** *arms race, embrace it and win it?*"

3. **Prioritize research and development, and organizational change, to exploit new media as a warfighting capability.** At present, the pace of technological change strongly favors new adversaries who are ready to exploit whatever means become available, and are unconstrained by permissions and process: "*We're constantly behind the ball. While we're figuring out whether we can blog or not, our enemy is already using wiki sites. So we start building wiki sites, and he is onto Twitter. There is a whole suite of tools that is coming out of Silicon Valley faster than we can figure out what they can do. And an unorganized enemy can use it at will, because it takes them 30 minutes to figure out what it does. But for us it takes 30 days, or 30 months to figure out whether we are allowed to use it or not.*"

   Beyond investing in research and development on new media, participants stressed the need for organizational change: "*We need to look at our modernization programs. The equipment that commanders have at their disposal now to move information around the battlefield is far better than it was even two years ago. But it is not yet enough to effectively exploit pictures and videos. How do you get that information out? Do you have the appropriate network? The size of the network? And we don't, not yet... We need to look at force structures across all services, down to the tactical levels especially. We can't leave it to chance – to the commander or soldier who happens to pick up his cell phone. There needs to be a process in place – a network that rapidly moves the information to the point it needs to get to. And we need to have battle drills to support this.*" And as another participant asked: "*Does the infantry company of the future have an officer advising the company commander about how to use new media devices?*" (See also Points 11 and 12.)

   There also needs to be a fundamental shift from a defensive to offensive mode for information engagement. As a participant observed: "*I believe that in every tactical operation now, there is some sort of recording medium. But it is used predominantly for evidence recording. What we have not done is to figure out how to exploit this. We need to open more doors to get it out. And imagery capture should be standard operating procedure.*"

4. **Educate "digital immigrants" to begin the process of cultural change.** Moving towards information engagement represents a paradigm shift for DOD — away from a culture of hierarchical information control and media avoidance towards distributed

[75] While the Army has loosened some restrictions in this area, there remains a debate over whether these will be reinstated.

and decentralized communication authorities, capabilities and requirements. Participants concurred that a major challenge will be cultural change: "*One of our concerns is senior level education. If you are 35 and below you get it; if you are older, you probably do not*." The older *digital immigrants* — who tend to be those in charge — rarely have full awareness of either the potential or the dangers of new media from a warfighting perspective. But simply ignoring new media is not an acceptable option in today's operational environment, within which information is pervasive: "*All media – including new media – are a key terrain on the battlefield. And just like a hilltop – if you ignore that piece of terrain, the enemy will use it to their own advantage. It is like a bridge – you can take it out – but if you do, then you can't use it either. You must consider it and use it to your advantage in the battlefield.*"

The need for awareness-raising, education, and training is urgent, and requires attention across the board: "*We need a bold effort with operational and strategic decision-makers...so they understand that every commander needs his information Vulcan.*"

5. **Exploit "digital natives" – encourage, educate, empower and equip.** DOD's digital natives — those young service members who are savvy in the use of new media devices, platforms, networks and possibilities — are underexploited assets in the information-led wars against new adversaries. Their knowledge, proclivities and aptitudes should be tapped, encouraged, empowered and equipped. In addition, many participants argued that Soldiers should be required to tell their stories: "*They should have as much responsibility to tell the story of what the American Soldier is doing, as to prepare for that next lethal combat. In fact, they should be doing this together.*" While this strategy is not without risk, risk mitigation is possible through appropriate education, planning and rules to define the acceptable left and right parameters within which they have freedom to act.[76]

6. **Enhance DOD's capacity for commanding the attention and trust of key audiences through improved capacities for appropriate messaging, achieving a distributed global presence on relevant media, and finding and leveraging suitable messengers (third-party validators).** In today's operating environment, achieving "resonance" with key audiences requires the ability to reach them in the idioms they understand, on the media they frequent, and through speakers they trust: "*In future wars, the organizations that lose the information war will be those that are still operating in an information economy, rather than the current world of the attention economy. Having the ability to push out information doesn't matter anymore. You have to grab audience attention. This requires two things: access and influence. If you don't have access, you won't have influence. But if you do have access, you have to make sure that your information is constructed in a way that sticks.*" And as another participant summarized: "*We keep going around this loop of culture,[77] but it goes deeper than that. The people you are trying to train, educate or influence – how do they receive and process information? How do they disseminate information? Whom do they trust?*"

[76] See Points 9 and 10.

[77] Meaning, acquiring appropriate cultural capabilities.

7. **Prioritize agility in the information domain.** "*We are swimming in molasses – bogged down by the culture, the approving authorities, the procedures and so on. We need to change all this, and build up appropriate capacities*." **Agility will require the interrelated transformations that are captured in points 8-12 below:**

8. **Enhance speed of communication, through:**

    - **Proactive information engagement** to actively shape the operational environment and audiences' understandings of events before they happen. This strategy contains the enemy's ability to get out in front with propaganda and force you into a defensive mode;

    - **More refined classification efforts** during planning, to facilitate speed of communication post-execution. Policies and regulations need to be used upfront to ensure that only essential security information is classified (rather than current practice where everything is automatically "classified");

    - **In-field declassification authorities and capabilities, and removal of barriers to inter-agency and inter-service declassification.** A number of participants stressed the "*higher level issues*" that undermine DOD's speed and agility in the information realm: "*For example, most airborne platforms that collect imagery belong to CENTAF (Air Force Central Command). To get that imagery, I have to know the procedures to make the CENTAF commander happy. There are a lot of issues around which component, platform or service collected what information, because all of the services will tell you: 'No, that is mine. I collected it, and my intercepts may not be touched by you.' So we must follow the rules. Following the rules by the letter for it to be unclassified takes a long time.*"

9. **Move towards decentralized authority and decentralized execution by setting the information rules of engagement.** The radical transparency of the current operational environment — with its attendant imperatives for speed, accuracy, credibility and authenticity of communication — requires "*our leadership …to adopt a much higher risk tolerance… and delegate the authority to speak and act to the lowest possible level — by allowing mid-grade officers at battalion level to respond. This would provide the necessary agility, but increases the risk for Blue-on-Blue cross-messaging. This goes against our strategic communication effort to make sure we have tight message control and alignment. But we need to be able to communicate and counter on the fly. We need to have the flexibility and freedom to do what we need to do [in the information arena] and make the decisions we need to make.*" While decentralization can also increase risk, the current practice of permissions, hierarchy and time-lags has also proven disastrous.[78] Participants believed that risk could be mitigated through appropriate rules of engagement (see next point).

10. **Identify and mitigate risk, through a more sophisticated risk assessment process.** "*One thing the Army is good at is developing rules of engagement with measures of risk. We are talking about getting policies that will allow us to get our rules of engagement straight with good, acceptable measures of risk in this area.*" Participants concurred

[78] See, for example, Box 5 in Part 2.

that appropriate rules, training and trust were the winning recipe as for other areas of warfighting: "*We allow a soldier to pull the trigger after he's been trained and has thought through the rules of engagement. And, we'll live with the occasional mistake. It needs to be the same for communication and information. We need to realize that we win on percentages — we can't have zero defects in this business. We need to get those authorities down to people that we have trained and trusted to be able to deal with it fast — locally.*" Participants noted that clear policies and rules of engagement would encourage the necessary cultural transformation towards embracing information engagement. By contrast, currently a lot of people are "*terrified to get in front of a camera, because they are afraid it will blow up in their face.*" Participants emphasized the need for senior leadership to "*provide cover for anyone who does go out and engage*" and "*not resort to military punishment for things incorrectly said.... And this has to be communicated up and down the chain of command.*" Nurturing a culture of information engagement requires it.

11. **Ensure commanders have non-lethal options commensurate with traditional lethal options.** Expert participants were concerned that many commanders were not aware of, nor adequately prepared to leverage, the many effective non-lethal options that are available to address a particular requirement in the information environment. And yet, the informational dimension of today's operational environment can strongly alter the commander's calculus for how to achieve both operational effectiveness and a given strategic endstate. They stressed the responsibility of the commander's staff to provide a full palate of options, based on a comprehensive situational assessment. Participants also noted, however, that the "*commander has a lot to handle these days — with a network warfare new guy, a human terrain guy, and then his own staff. I think he is in constant information overload.*" Participants agreed that as the military's warfighting strategy continues to evolve towards a more holistic approach, the commander's need for an integrated vision must be better addressed and serviced.

12. **Require commanders to define the information endstate.** The commander's intent should specify the desired **information endstate**, as part of the overall military endstate, which should then "*trickle down as it does for kinetic engagement. We need to think in the same manner.*" Currently, as participants observed, "*this is not common practice. Rather the informational endstate is usually derived from the larger intent: 'Okay here is what is likely to be the matching information environment that supports the larger intent...' But there should be explicit guidance, with articulated objectives, like: 'I don't want this message coming out from the enemy.'*" As another observer has noted elsewhere: "A properly articulated information endstate will drive both planning and execution of the military operation with sensitivity toward the new media environment. ...Sensitized to the commander's intent, planners 'wargame' the courses of action with that endstate in mind. ...Where previously a kinetic solution may have been the preferred choice (driven by inherent organizational culture) the information endstate may instead drive the unit toward a different approach that achieves the stated cognitive effect on perceptions, attitudes and behaviors."[79]

[79] Murphy (2008). Available on: http://www.carlisle.army.mil/DIME/documents/Fighting%20Back%20(Murphy).pdf

13. **Exploit new media for better measures of effectiveness.** Establishing and assessing measures of effectiveness represents a huge challenge for commanders: "*We are very good at putting out messages, but not very good at assessing how they are received: are we modifying perceptions and behaviors? Nor are we good at understanding the most effective modes of transmission – social networking, viral transmission?*" A number of participants stressed that new media offered significant potential in this regard, as their interactive properties enable an unprecedented capacity for strategic listening and feedback.

14. **Streamline DOD policies and guidance.** Participants were concerned that policies dealing with the informational aspect of the operational environment are coming out piecemeal. This is anathema to the "*holistic view that is needed to effectively operate in the information domain. Piecemeal policies require lower commanders to think about how to put it together. But we need to think through this more…to ensure all the policies across all the services and the joint environment are integrated…and not 'here's a band-aid for this thing, and a band-aid for that thing.'*"

    This is not just about defining policies for blogging, or Internet activity. Rather it touches on policies that exist within each of the services — declassification policies, for example — that have to be simultaneously changed in order to enable proper planning, organization and equipping: "*We need a holistic review of a host of policies to see what needs to be done to allow us to achieve operational and tactical effectiveness...and give flexibility to commanders at all levels to use new media to benefit mission success. What policies are in place, and what policies need to be in place? Do our public affairs and information policies match our network policies; match our command policies? Those things have to be in synch. We need to look at this across the board.*" And, as another participant observed: "*Leveraging new media has to be across all practices. It cannot just be one. The Information Operations folks may have specific needs, but Public Affairs need to know what they are doing, and IO needs to know what PA is doing. Plus, they need to collaborate. And they need to collaborate with the visual information folks. Soft power cannot be stovepiped. Capabilities need to be on a continuum. We have to start looking at doctrine, at capabilities and how capability is going to be used to achieve the desired effects. An information effect may take everybody... what is vital is the synergy of all the different tools we have to achieve the operational endstate.*"[80]

15. **Synchronize, synchronize, synchronize – across all-of-government.** Participants emphasized that the radical transparency of new media has increased the imperative for synchronicity of vision and effort across all aspects of national power: "*There needs to be clear linkages between national security policy and how that filters down to the Department of Defense – which is really just one tool in the tool box. DOD is not the be all and end all of this.*" Some participants suggested that perhaps an interagency information division was needed, as well as "information platoons" at the tactical or company level, which the commander could deploy to capture imagery, stories, blog, undertake rapid media response etc: "*I know this workshop is on new media and the*

[80] Participants also observed that a lot of existing policy is about "*what you cannot do. If we are trying to encourage the use of new media and culture change, we need to specify what can be done. We need to make it less restrictive and more flexible so that the guy at the lowest level can do his job*."

warfighter, but this issue is so intricately related all the way up to the highest levels of our national policy and Secretary of State, I'm going to state that we [need]... an organization that lives and breathes this stuff; that is knowledgeable in the different policies and technologies to fight the information battle... like we had when we were fighting the ideological battle with the Soviet Union."

At the same time, participants wondered about the appropriate limits of DOD's current responsibilities: "*What is the military expected to achieve when we speak of wins? We need the capabilities to achieve that defined endstate. But these days, is it just the military win? Or is the military now responsible for the diplomatic win, the informational win, and the economic win?"* And, as another participant queried: "*Who is responsible for achieving that endstate in the information realm? Is it the military and if it is then let's define it, and give them the capability to do it. If it isn't then give it to whoever it is and hold them accountable. But I think that in the society that we are living in today, the American people expect the American military to achieve the win. They don't define a win or loss by some other government organization. We are talking about perception."*

16. **Pursue a holistic approach.** Overall, new media is forcing an "*ultimate shift in how you fight wars.*" The informational aspect of the operational environment must become a primary consideration in the commander's intent and planning, and all capabilities – hard and soft, actions and words – must be integrated and deployed to achieve the desired endstate. Participants were adamant that the informational aspect can no longer be stuffed into the annexes of official doctrine, tacked on as an afterthought to battle plans, or stovepiped between IO and PA. Rather, what is needed is a holistic, multi-echelon approach, "*just as we do with training, where each tier is considered – whether strategic, operational or tactical – and assigned clear responsibilities, and given the authority to act.*"

17. **Engage the legal debate.** New media, with its dissolution of time and distance and muddying of sovereign borders, has engendered a whole host of complicated legal issues around what operations are legal and appropriate for containing or disabling adversaries in the information realm. Just as new media have fundamentally transformed the operational environment, so too must the attendant legal issues be charted, debated and reframed: "*We need to further define the legal ways of combining lethal and non-lethal action to achieve the commander's intent.*"

APPENDIX:

WORKSHOP CASE STUDIES: New Media and Information Effects during the 2006 Israeli-Hezbollah War in Lebanon

Prudens Futuri

New Media and Information Effects during the 2006 Israeli-Hezbollah War in Lebanon

CASE STUDY 1: Operations Security (OPSEC) and new media

The 2006 Israeli-Hezbollah War in Lebanon reveals some of the OPSEC challenges that are inherent to the contemporary operational environment. On the one hand, the case study illuminates the challenge of OPSEC for those modern military forces that are drawn from "communication" societies, meaning those awash with instant and readily available communication means, and where the culture of 24/7 connectivity has become a socially accepted norm and expectation. On the other hand, the war showed how a non-state military actor leveraged OPSEC to its advantage: Hezbollah exercised a highly disciplined approach to OPSEC as an inherent part of its campaign strategy, denying the IDF both operational details and the raw material for PSYOP product (such as casualty figures).

New media can directly affect OPSEC on different levels.[1] For example, military bloggers ("mil-bloggers") can compromise the effectiveness of military actions, and risk the security of troops. At an overall strategic level, new media can allow for communication disasters, as the circulation of photographs from Abu Ghraib starkly demonstrated. Moreover, as the military increasingly combines forces to work with local partners, NGOs and international organizations, communication discipline can become compromised, as communications equipment and protocols are geared towards information sharing and coordination. This makes strict rules difficult to set and enforce. Finally, new media enabled tools — such as inexpensive remote sensing GIS, video-enabled cell phones, satellite communications and pervasive Internet — create degrees of transparency in the battlespace that can fundamentally compromise OPSEC.

Failures in OPSEC that result in casualties are a serious and sensitive matter for military leaders. The following examples of such failures in the 2006 Israeli-Hezbollah War — drawn from multiple sources — are directly attributable to new media.[2]

A. The IDF: Various OPSEC challenges caused by new media

Post-war assessments attribute many of the IDF's tactical reverses to poor leadership and inappropriate training of Soldiers (that is, Soldiers were unprepared for the demands of the Lebanon campaign, as opposed to the counter-insurgency and policing duties well-honed in the West Bank and Gaza). Many reports contend that the IDF lacked discipline as well as basic attention to battle drills.[3] Some of these lapses involved new media, and were of direct consequence to Israeli OPSEC — from Soldiers' use of mobile phones through to mil-blogs.

[1] Thomas Rid (2007) cites a DOD Public Affairs Officer: "Today, every soldier has a cell phone, beeper, game device, or laptop, any one of which could pop off without warning. Blogging is just one piece of the puzzle."

[2] Unless otherwise referenced, material cited in this Case Study was drawn from exit interviews with Israeli Soldiers, after the 2006 Lebanon War.

[3] See: Matthews (2006); Winograd (2007).

In Lebanon, many IDF Soldiers went to war with their mobile phones. Israeli Soldiers are used to being "plugged in" within their mainstay deployment areas — the West Bank and Gaza. These territories are covered by commercial Israeli ISPs and cell phone providers, and Palestinian militants possess no significant SIGINT capability or expertise. As a result, it became the norm for IDF Soldiers to carry consumer electronic devices into operational settings, and many took their phones along to Lebanon. As one analyst reports, "while in most units, the quartermaster collected all phones prior to entering Lebanon, some Soldiers kept their phones with them, and when possible, made use of them for calls, SMSing and even photography." [4]

This had at least two effects on the course of the campaign. First, when IDF Soldiers called home, they often revealed operational details to their loved ones (e.g., location, what they were doing).[5] At least some of this information made its way into media reports and websites. Soldiers also blogged. And, as dissatisfaction mounted with the IDF's logistical failures to supply Soldiers with sufficient food, water and ammunition, the blogs began to log these complaints.[6] This served to further undermine soldier morale, and also increased public pressure on the Israeli political leadership, which was already struggling with a domestic crisis caused by the Hezbollah rocket attacks against the North, and the displacement of the population. Second, and perhaps more importantly, there are strong indications that Hezbollah made significant use of both Open Source Intelligence (OSINT) (targeting Israeli media and websites)[7] and SIGINT (against IDF tactical communications and cell phones carried by IDF Soldiers).[8] IDF troops seized sophisticated intelligence equipment from Hezbollah bunkers that had been used to tap IDF cellular phone lines, and possibly (according to some accounts) may have broken into the IDF's tactical net.[9] Evidence suggests that Hezbollah used this SIGINT product in at least two ways:

1. **To report IDF casualties more accurately, and more quickly, than the IDF itself, which caused a "credibility gap" for the IDF.** Throughout the conflict, Hezbollah media sources were consistently able to report the number and location of Israeli casualties faster than IDF sources. This had a negative effective on Israeli public perceptions, as reports made by Al-Manar were picked up by Israeli media or disseminated on Hezbollah's Hebrew language service. The slowness of IDF reporting may have been a function of Israeli OPSEC considerations (as an early release could threaten ongoing operations), as well as the need to verify casualties (and their identities) to ensure that families of the deceased were the first to be notified.

[4] Dahan (2007).

[5] "Sensitive information was also leaked in Israeli blogs, forcing the military censor to call on all bloggers, forum contributors and talkbackists (basically community of user generated content) to exercise self censorship", Ibid.

[6] Dahan notes: "Blogs were used to express criticism of the political and military leadership, to support the Soldiers and civilians, to disseminate information, to protest the war and also served to open lines of communication between Lebanese and Israeli civilians , for the first time during a war in the region." Ibid.

[7] At a recent conference on "info war" in Israel, it was noted that much of the intelligence gathering done by Hezbollah during the war was collected from Israeli news broadcasts.

[8] In a conference held at Tel Aviv University on December 13th 2006, General (ret.) Yakov Amidror, former head of the Research Section of IDF Military Intelligence, noted that Israel failed to prevent sensitive operational information from leaking to the Internet during the war. This was echoed by other speakers at the conference who noted that the use of cellular communications, digital photography and video severely compromised certain operations. Shai Blitzblau, CEO of Magal Technologies (a data security company with close ties to the military establishment) noted that during the war they discovered operational information open and readily available during the battles in Bint Jubeil and Debbel, where Israel suffered severe losses.

[9] Harel (2007).

A cumulative effect caused by the speed and accuracy of Hezbollah reports and the slowness of IDF confirmation was to create a “credibility gap” for the IDF. This was particularly evident following Hezbollah’s successful attack on the Israeli Naval Ship *Hanit* (July 13 – See discussion in Case Study #2). Al-Manar reported the attack in real time, while the IDF took 24 hours to confirm the event. The IDF delay may have been necessitated by OPSEC, but the result was a major negative “information effect,” as the Israeli public felt that the IDF was being needlessly deceitful with their information.

2. **To ascertain IDF location and deployment information.** Hezbollah also seems to have exploited IDF cell phone usage as a surrogate “blue force tracker,” to reveal location information. While it is difficult to prove this point for certain, some of the equipment seized by the IDF from Hezbollah bunkers showed their capacity to hack into commercial Israeli cellular phone towers along the border. This would have allowed them to geo-locate the cell phones carried by IDF Soldiers in the South of Lebanon. Moreover, it is likely significant that, immediately following the war, the IDF rapidly reactivated a unit (Ayit) tasked with monitoring IDF communications and OPSEC, which had been deactivated a few years earlier following the withdrawal from South Lebanon. [10]

There are also some unconfirmed Israeli reports that the IDF’s tactical cellular phone communication system (“Mountain Rose”[11]), which was extended as IDF units advanced by use of transmitters in tethered AEROSTATs, may have compromised the integrity of IDF operational details.[12] Israeli press reports (not published in English) suggest that the system itself may have been inherently insecure, allowing unauthorized access to highly sensitive material such as classified documents, which could be obtained by way of a simple search.[13]

There are also unconfirmed indications that Hezbollah made extensive use of real time OSINT generated from the Israeli press to plot the location of its rocket strikes in Israel. As was revealed after the conflict, several groups unaffiliated with Hezbollah had used Google Earth to plot the geographic and temporal location of both Hezbollah and Israeli strikes.[14] One observer noted that there is also some anecdotal information available regarding the use of Google Earth by the IDF during the war.[15] It is unknown whether Hezbollah used Google Earth to calibrate the accuracy of its fire. However reports suggest that Hamas and other militant groups leverage Google Earth to adjust the accuracy of rockets fired from the Gaza strip.[16] The dilemma is that non-state actors can now leverage commonplace Internet tools such as Google Earth to serve military ends.

[10] Ibid.

[11] Mountain Rose IDF Mobile Communications Network.

[12] On the Israeli side though, tactical intelligence, such as frequencies, war room and operational maps, battle plans, special weapons, and even soldier interactions and internal dynamics during battle were available on the web. In the words of General Amidror: “The Internet guarantees the intelligence community a long life of mutual challenge though I have doubts as to who will win in the end.”

[13] Harel (2007).

[14] Arkin(2007).

[15] As was widely reported in the press, logistics were in a large part responsible for Israel’s defeat. An Israeli reservist serving in an infantry unit during the war said that his unit and others made use of Google Earth.

[16] Chassay (2007).

B. Hezbollah's iron-clad OPSEC

The 2006 Israeli-Hezbollah War confirmed the degree to which non-state military forces (like Hezbollah) have become much more savvy with respect to SIGINT capabilities and consequences (theoretical or experienced). Throughout the conflict, Hezbollah practiced extreme message discipline and communications security.[17]

At the command level, mission orders were broad and decentralized which negated the necessity for a "lit up" command and control network. Where necessary, communications lines were hardened, using specially laid fiber optic channels. Tactical communication was enabled by hand-held radios, but messages were coded using plain language but that was familiar only to the communicating parties. Reportedly, even when the IDF was able to intercept or decode messages, they could not understand their meaning.[18]

Hezbollah maintained a high degree of overall security around all of its military operations. Hezbollah fighters were not allowed to be photographed by anyone, nor did they grant interviews to any media, (formal or informal). In fact, at one stage of the war there was speculation that the IDF was fighting a phantom enemy. Figures of Hezbollah casualties were kept secret, and to date Hezbollah claims an improbably low number of fighters killed (although low figures may also be attributed to the fact that the bulk of fighting was carried out by Hezbollah village defense forces who where considered irregulars and thus counted as civilians rather than core members of its military wing). Nonetheless, the absence of credible evidence for the high casualty numbers claimed by Israeli forces undermined IDF claims that it was successful eliminating Hezbollah's military capabilities.

All of these factors contributed to Hezbollah remaining a "black box" for the majority of the war and thereafter. It is reasonably clear that Israel had gathered a significant amount of intelligence about Hezbollah forces and installations in the lead up to the war — a factor that allowed the IDF to neutralize most of Hezbollah's long and medium range rocket forces in the first 24 hours of the conflict. However, after this initial success, the IDF did not appear to further exploit Hezbollah OPSEC for battle or PSYOP wins. Whether this gap was due to a deliberate IDF decision (to protect intelligence), or because they were simply unable to further tap into Hezbollah's ongoing OPSEC, is unknown.[19] But open sources do not suggest that IDF used such product after the first 24 hours of the conflict.

C. Issues and questions for discussion

(Ground discussion in concrete examples where possible)

The degree to which new media have become embedded in a rapidly globalized world and the complex nature of the military's contemporary operational environment are fundamental challenges to traditional notions of OPSEC. Overall, the commander's ability to control OPSEC has greatly diminished in a variety of ways.

[17] Exum (2006).

[18] Helmer (2007).

[19] According to Shai Blitzblau, CEO of Magal Technologies, Hezbollah made use of sophisticated surveillance equipment including cameras, but nothing leaked to the net.

1. **Globally, societies are becoming media rich.** Two-thirds of humanity now own a cell phone and a third are connected to the Internet. There are few areas of the globe that are not "connected" somehow, either by the Internet or terrestrial or satellite radio or TV. In addition, the cost of technology that can be used to create an information "product" deliverable by these means is constantly falling. Whereas communication with a mass audience was once prohibitively costly, today anyone armed with a hundred dollar digital camera and a connection to the Internet is a potential Spielberg or Riefenstahl.[20] From an OPSEC perspective, this means the military now operates in a radically more transparent environment than previously: the volume and global dissemination of military-related information has expanded exponentially. New adversaries are closely attuned to the prospects for aggregating vital intelligence from open sources like the Internet. For example, Al-Qaeda's Encyclopedia of Jihad states that 80% of all intelligence needed for an operation can be sourced from Open Source Intelligence. In addition, new media have empowered new adversaries to reach mass audiences with their version of "the truth" within minutes of lethal encounters.[21] This has created new imperatives for the speedy release of images and information following lethal encounters, which in turn can lead to OPSEC violations.

    - Has the new transparency changed the military planner's calculus for operations, and for managing OPSEC? If so, how: at the tactical level? at the strategic level?

    - Do military planners have appropriate tools and resources to assess the effect that new media (transparency, alternative "truths") may have on OPSEC at the tactical and strategic levels?

    - There is an obvious tension between the need to get the true story out as quickly as possible, while also ensuring OPSEC. Are commanders sufficiently aware of the new imperatives for speed? Are there adequate systems in place to enhance speed of communication while preserving OPSEC? What more could/should be done?

2. **Newer cohorts of Soldiers are "digital natives."** They come from a hyper-connected generation, are used to 24/7 Internet connectivity and are well-versed in the use of new media technologies in their civilian lives. Solders on deployment now expect to be in touch electronically with their families on a daily basis. Enforcing a ban on such communications is difficult if not impossible. The communicative expectations of digital natives, when combined with the fact that new media devices can be surveilled and mined by media-savvy adversaries for critical information, can create serious challenges for preserving OPSEC.

    - Mil-blogging is a growing phenomenon with both positive and negative effects. What are the positive effects? What are the OPSEC challenges? How can the benefits of mil-blogging be emphasized, while minimizing its liabilities?

    - Proscription or prescription: balancing OPSEC consideration against Soldier morale is tricky. Should there be stricter rules? Or do we need a more flexible approach to their implementation?

[20] See, Rohozinski (2003).

[21] See, Collings and Rohozinski (2006); Dauber (2009).

- Are senior leaders — who are usually of the generation considered to be "digital immigrants" (that is, *not* savvy in their knowledge or use of new media) — sufficiently aware of the potential OPSEC challenges posed by their Soldiers' use of new media?

3. **The environment in which U.S. Forces must operate is increasingly complex, often requiring interoperability with local forces, NGOs or international organizations, all of whom are awash with new media devices and actively communicating information, often from within areas of military operations.** Enforcing military OPSEC with these actors is difficult if not impossible: Previously, "OPSEC involved controlling your soldiers; today it applies to anyone with access to new media in the military operating environment."[22] Additionally, mission profiles may change rapidly under conditions of "mosaic war," forcing a shift from combat to stability operations, and demanding that Soldiers and their leaders shift from "warfighting" to "communicator" roles. The rapidity of change can cause confusion, and may also compromise OPSEC, thereby endangering force protection, or the success of the tactical and strategic objectives.

   - The expansion of external friendly actors now working within areas of operation – and expecting the sharing of information — can significantly increase OPSEC risks. What are some solutions?

   - OPSEC requirements may change rapidly during the course of a single campaign (or deployment) requiring Soldiers to shift roles, and in some cases use heterogeneous communications networks in the execution and coordination of their mission. Are current OPSEC communication tools sufficiently flexible to rapidly adapt to changing levels of OPSEC/interoperability, as dictated by mission objectives? If not, is it a technology problem, or a personnel management or training issue?

   - As OPSEC has become a more critical issue for U.S. Forces, are there additional training requirements that could help address solutions, and if so who must they focus on: Soldiers, commanders, or both?

References

Arkin, W. M. (2007). *Divining Victory: Airpower in the 2006 Israel-Hezbollah War*. Maxwell Air Force Base, Alabama, Air University Press. http://aupress.maxwell.af.mil/books/arkin/arkin-small.pdf

Chassay, C. (2007). "Google Earth used to target Israel." *Guardian*, 25 October. http://www.guardian.co.uk/technology/2007/oct/25/google.israel

Collings, D. & Rohozinski, R. (2006). *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations*. Carlisle, U.S. Army War College. http://www.csl.army.mil/usacsl/publications/ShiftingFireMenu.pdf

Dahan, D. M. (2007). "The "Infosphere" during the second Lebanon-Israel War." Unpublished Research Report, commissioned by the Information Society in Palestine Project, University of Cambridge, Advanced Network Research Group.

Dauber, C. (2009). "The truth is out there: Responding to insurgent disinformation and deception operations." *Military Review*, Jan-Feb 2009. Accessed from http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art005.pdf

[22] Murphy (2009).

Exum, A. (2006). “Hizbullah at War: A Military Assessment.” *Policy Focus* 63. Washington, DC, The Washington Institute for Near East Policy. http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf

Google Earth Blog (2006). “Israel-Lebanon Conflict Illustrated in Google Earth.” 21 July. http://www.gearthblog.com/blog/archives/2006/07/israellebanon_c.html

Harel, A. (2007). IDF to reestablish unit aimed at monitoring military telephones. *Haaretz* (*Hebrew version*), Tel Aviv.

Helmer, D. (2007). “Not quite counterinsurgency: a cautionary tale for U.S. forces based on Israel’s operation change of direction.” *Armor*, January-February. http://www.defence.gov.au/army/lwsc/docs/aaj_winter_2008_2_2.pdf

Matthews, M. (2006). Interview with BG (ret.) Shimon Naveh (IDF). *Operational Leadership Experiences in the Global War on Terror*. Fort Leavenworth, Kansas, Combat Studies Institute.

Mountain Rose IDF Mobile Communications Network. http://www.defense-update.com/products/m/mountain-rose.htm

Murphy, Dennis (2009). “Operations Security in the Age of Radical Transparency.” Center for Strategic Leadership Issue Paper, Volume 2-09. USAWC: Pennsylvania. http://www.carlisle.army.mil/DIME/documents/Murphy%20OPSEC%20and%20Radical%20Transperancy.pdf

Rid, D. T. (2007). “War 2.0.” *Policy Review*, February. Stanford, Hoover Institution. http://www.hoover.org/publications/policyreview/5956806.html

Rohozinski, R. (2003). “Bullets to Bytes: Reflections on ICT and “Local Conflict”,” in Latham, R. (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between IT and Security*. New York, New Press.

Winograd (2007). The main findings of the Winograd partial report on the Second Lebanon War. Tel Aviv, Government of Israel.

New Media and Information Effects during the 2006 Israeli-Hezbollah War in Lebanon

CASE STUDY 2: Leveraging new media effects

During the 2006 Israeli-Hezbollah War in Lebanon, Hezbollah demonstrated a refined capability to leverage new media to create positive informational effects. Many different actors in areas of kinetic operations — the press, Israeli and Lebanese civilians, IDF soldiers and Hezbollah – used a variety of new media to document and blog the war, with some seeking to influence the political will of key audiences. As one analyst noted: "The ease and speed of transmission (not to mention the ease of "touching up" photos) of these images formed another aspect of the war: Israeli Soldiers sending SMS messages home; Hezbollah and the IDF distributing videos of the fighting; and, civilians posting photos on blogs and websites, most notably YouTube. Satiric flash movies humiliating Hezbollah and Nasrallah were posted on YouTube.[1] Computer games, primarily flash based, were produced by Israeli civilians during the war. It thus seems that these media tools are becoming a permanent fixture in violent conflict; they are ubiquitous and almost impossible to control."[2]

However, on this playing field, Hezbollah clearly outpaced the IDF. Hezbollah's information strategy formed an integral and integrated component of its overall military strategy. Hezbollah's information "wins" reflected its heavy investment in a robust, flexible and professional broadcast and Internet capability.[3]

This breakout groups considers Israeli and Hezbollah attempts to "leverage" new media modalities to produce and control "information effects" in order to score symbolic, moral or political wins.

A. Hezbollah's information war

While Hezbollah may be best known internationally for its military wing, the movement has deep national roots, strongly grounded in the Shia communities of South Lebanon. Hezbollah's mantle of resistance to Israel's occupation of the south formed part of a broader "patriotic" Lebanese agenda, while also serving to strengthen Shia political claims within Lebanon's confessional system of government. While Hezbollah is an Islamic Shia organization, it is also highly pragmatic, and does not seek to impose Islamic mores on the broader Lebanese society. This restraint has won Hezbollah considerable support from a broad cross-section of moderate Lebanese patriots including, significantly, from within the Christian community.[4]

Hezbollah's emphasis on communications goes to the core political objectives of the organization. Hezbollah leverages new media in all aspects of its work as a political, military

[1] YouTube. "*satla nassralla*."

[2] Dahan (2007).

[3] For an excellent analysis of new media and its implications for confronting asymmetrical actors, see Rid (2007).

[4] Ya Libnan (2006).

and social organization. Hezbollah's military strategy, generally, has been to make up for its military limitations by generating strategic informational effects. Recognizing the enormous popular appeal of being an "underdog" in relation to the Israeli army, Hezbollah has popularized a "narrative of resistance" against perceived Israeli aggression against Lebanon/Palestinians. War objectives focus on "winning by not losing" and scoring "political" triumphs.

Hezbollah possesses the largest media organization of any political party in the Middle East region and has the capacity to directly reach a population of 200 million viewers via satellite broadcast, with a further unlimited number via its many affiliated and associated web sites and blogs.[5] Its media flagship – Al-Manar – dedicates some 25% of its production capacity to "resistance" music and entertainment programmes, many of them glorifying Hezbollah military prowess. Al-Manar distributes its video productions through a wide network of associated sites.[6] This content is then picked up by large networks of others – supporters or simply the curious — and re-posted to YouTube and other video sharing sites. Hezbollah also created popular first-person "shooter" video games that reinforced the "resistance" narrative, while building up a warrior ethos among its young followers.

Because Hezbollah's own and associated new media resources are wide-ranging and globally dispersed, they are difficult to track or shut down by legal or conventional technical means. Moreover the low cost of operations and willingness of audience members to replicate and further distribute content makes the elimination of Hezbollah's informational reach difficult to achieve without a truly global agreement.

Hezbollah's well-honed media instrument was put to effective use during the war. Hezbollah's information strategy appears to have been focused on undermining the credibility and reliability of Israeli accounts of the war in the eyes of all audiences (especially the Lebanese and Israeli audiences).

Hezbollah rapidly and accurately reported battlefield incidents, which were packaged into multimedia products and distributed via the Hezbollah network and beyond in multiple languages. These reports established the credibility of Hezbollah's news products with a wide-range of internal and external audiences.[7] Reports prepared and broadcast or electronically disseminated in Hebrew signalled Hezbollah's deliberate targeting of Israeli domestic audiences, and indeed, Hezbollah reports were picked up and re-reported by Israeli media sources.[8] By staying ahead of the Israeli reporting cycle, Hezbollah managed to undermine the Israeli public's faith in Israel's own reporting efforts.[9]

Spectacular tactical actions were staged, timed, reported and packaged for maximal strategic effect. For example, within minutes of Hezbollah's successful missile attack on the Israeli

[5] Jorisch (2004).

[6] Erlich and Kahati (2007).

[7] "Hezbollah made use of Al-Manar to appeal directly to Israeli civilians, and at one point during the war there was a brief, almost hallucinatory, live exchange between Israeli TV journalists on channel 10 and the Al-Manar news anchor," (Dahan, 2007).

[8] Ibid.

[9] As Dahan observes, "Via Al-Manar and other media outlets, Nasrallah was viewed by the Israeli public as being more credible than the Israeli media outlets. This was also the first war where Israeli citizens were more fully exposed to what was happening in Lebanon, in almost real time, via different media outlets. After the war this led to severe criticism of the media in Israel." Ibid.

Naval Ship *Hanit,*[10] Hassan Nasrallah (Hezbollah's secretary general and chief spokesman) was on the air, telling viewers to look to the sea to see the burning Israeli vessel. This was backed up by Al-Manar footage of the missile launch. It took Israel some 24 hours before it confirmed the attack. By then, Israeli audiences already knew of it from the Al-Manar video and media coverage, which was carried globally through dense networks of new media.

Hezbollah's information efforts focused on "exposing" the destruction wrought by Israel (to stir popular outrage) as well as Israeli casualties (to undermine Israeli morale), while maintaining a strict silence about the conduct and status of Hezbollah forces and casualties (See Case Study #1).

Hezbollah reaped "collateral benefits" from popular "outrage" at the physical destruction and casualties caused by IDF firepower.[11] IDF actions provided stunning visuals of war, as did the one million people who fled to the south of Lebanon, along with the evacuation of foreign nationals by western nations. Hezbollah packaged and distributed gruesome photographs of destruction, which they released to the press and posted to blogs and photo-sharing sites. Graphic videos were assembled and posted to You Tube, and also to email lists that were circulated widely throughout the region.[12] These images, along with the seemingly callous remarks made by some senior Israeli leaders (see Case Study # 3) meant that the sympathy of the Arab street, and certain international audiences, tended to side with the Lebanese people. This groundswell of sympathy for the Lebanese victims dovetailed in important ways with Hezbollah's narrative of resistance against a disproportional IDF response. Such sympathetic views were widely evident in email campaigns, blogs and websites that were not in any way related to Hezbollah (or its affiliates), but which nonetheless amplified and enhanced the effectiveness of Hezbollah's own informational strategy.[13]

Hezbollah's information strategy was enhanced by careful management of press visits to sites of devastation, and in some cases the circulation of touched up photographs and deliberately staged events, although the latter resulted in "blowback" when third party "whistleblowers" revealed the falsifications[14] (see Case Study #3 – Countering New Media).

Beyond this, Hezbollah's position was buttressed by the emergence of many Lebanese "bloggers" who provided real time details and photos of Israeli actions (note: a quarter of the Lebanese population is connected to the Internet[15]). As Lebanese "bloggers" outpaced mass media reporting, major media organizations began to quote them as news sources, with several incorporating blogs into their main news coverage.[16] Post-war, it was clear that despite stunning visual images, the scale of destruction was not as great as was first reported.[17]

Civil society and other non-state groups also leveraged new media to map the conflict, some

[10] Wikipedia. "INS *Hanit*."

[11] Kalb and Saivetz (2007).

[12] For an excellent analysis of Hezbollah's military-political war strategy, see: Crook and Perry (2006a; 2006b; 2006c).

[13] Thomas (2007).

[14] Kalb and Saivetz (2007).

[15] Internet World Statistics. "Middle East." http://www.internetworldstats.com/middle.htm

[16] Ward (2007).

[17] Arkin (2007).

of which worked to the benefit of Hezbollah. For example, several groups independently mapped incidents of Israeli air and artillery strikes, as well as Hezbollah rocket launches and posted the results to Google Earth.[18] These maps worked against Israeli interests by demonstrating the asymmetry in relative firepower used by the different sides, which reinforced the Hezbollah "underdog" image.

B. Israel's efforts to leverage new media

By contrast to Hezbollah's integrated approach to strategically leverage old as well as new media, Israel's efforts were more modest and less systematic. Instead, the IDF and Israeli establishment relied largely on conventional Information Operations (IO) techniques, as well as "collateral support" from the traditional powerbase of the Israeli diaspora and pro-Israel supporters. The IDF made some limited use of new media. As one Israeli observer notes, "The Army spokesperson apparently uploaded morale building video clips to a local version of YouTube[19] and Flicks.[20] Indeed, YouTube and other video content sites served as a virtual extension of the battlefield – with news and other reports leading the fight over the hearts and minds of both local and global publics."[21]

As during the Palestinian Intifada, Israel made use of rapidly declassified intelligence to bolster its factual reporting.[22] In the wake of the conflict it released the names, addresses, cell phone numbers and call signs of close to 600 alleged Hezbollah fighters as proof that this number had been killed. By contrast Hezbollah claimed only 150 deaths.[23] Other sources contested the higher Israeli figure arguing that this was not supported by the number of funerals held by Hezbollah (who are usually quick to celebrate martyred fighters).

Israel also released video footage of Hezbollah rocket launches from built up areas and Israeli surgical strikes against specific targets of a military nature. While this footage was compelling, it could not compete with the abundant visual imagery of Israeli destruction of civilian property and loss of life. Moreover, IDF's clear tactical losses only served to reinforce the image of Hezbollah as a "surprisingly tough and efficient" force

In fact, the majority of Israeli activity to leverage new media appears to have come from civil society-led initiatives, with only limited (overt) support from the government. These included Israel's extensive "hasbara"[24] (or "explanation") information networks, which targeted major mass media globally, with pro-Israeli Op-Eds, letter writing campaigns and blogs. As always, the "hasbara" networks seek to explain and justify Israeli positions and actions. In recent years the effectiveness of "hasbara" has been boosted by the Internet as well as the development of software tools that automate the process of letter writing, greatly increasing both volume

[18] Google Earth Blog (2006).

[19] Some movies were also openly uploaded by the IDF to YouTube. One example was available online at: http://www.youtube.com/watch?v=qQz0NSsqF_I – however, the video was removed due to "terms of use violation."

[20] An example video is available online at: http://www.tapuz.co.il/flix/myFlix.asp?id=2027766

[21] Dahan (2007).

[22] Intelligence and Terrorism Information Center. *Website*.

[23] Crooke and Perry (2006a; 2006b; 2006c).

[24] Wikipedia. "*Hasbara*."

and reach. One such tool developed by the World Union of Jewish Students – Megaphone — automated the process of voting in on-line polls as well as letter writing. While developed by a private group, the tool allegedly has the tacit support of the Israeli foreign ministry.[25]

Members of civil society also prepared various media products that were widely circulated on the Internet and various broadcast media. For example, two Israeli musicians developed a catchy music video, whose refrain was: "Bring it on Nasrallah; we'll kill you soon inshallah; we'll send you back to Allah; with the rest of Hezbollah." The song became an instant hit in Israel, but also unexpectedly in Lebanon.[26] One report claims that the IDF inserted the video on Al-Manar during one of its electronic attacks on the station.

There is also some indication that Israeli intelligence services were behind a number of "false flag" websites, although there has been no official confirmation.[27] The impact of such sites is difficult to judge.

C. Issues and questions for discussion

(Ground discussion in concrete examples where possible)

1. **The "underdog" advantage.** Leveraging new media effects seems to favor the underdog, who can attract collateral support and "reverberation" of his story by way of a compelling narrative of "injustice/resistance," backed up by graphic visual evidence. The underdog's domination of the informational space is buttressed by his ability to rapidly get his message out, which allows him to stake out an early "moral" advantage, which then becomes difficult to counter. (Once the story has been spun and retold, it quite often sticks).[28]

   - Are Combatant Commands agile enough? Are there adequate systems in place to support a rapid declassification of intelligence product that could have PSYOP or strategic communications value if disseminated in a timely and accurate manner? Are there examples of how rapid informational response has yielded information wins? Is rapidity of information dissemination prudent? Can it lead to unacceptable OPSEC risks? (examples) Can it lead to blowback if swiftness compromises accuracy? (examples).

   - At the tactical level, is there sufficient evidence from current experience to suggest that low lethality, high accuracy attacks are effective in eliminating high value targets and threats? Is the "pinpoint" approach one way to contain the negative emotive "blowback" of more broadly kinetic approaches? Is current doctrinal sentiment in favor of such an approach?

2. **Getting the word out, with credibility.** As both the Israeli and Hezbollah examples show, new media is especially conducive to creating informational wins when (non-military)

[25] Wikipedia. "Megaphone desktop tool."

[26] Wikipedia. "Yalla Ya Nasrallah."

[27] Pahlavi (2007).

[28] Collings and Rohozinski (2006).

sympathetic bloggers and websites voluntarily endorse, reproduce and reinforce the military's informational product and perspective ("reverberation"). However, reaching and engaging the global community of bloggers and new media producers requires a much broader approach than that currently practiced by public diplomacy, which tends to focus on international broadcasting and the use of websites as information portals. Blogging and counter-blogging raise complex issues of authority, effectiveness (value for effort), as well as legal and ethical issues over the use of un-attributed strategic communication (perceived as black propaganda).

- Given that the most successful leveraging of new media (in Israel) came from the private initiative of Israeli citizens and their supporters abroad, is there any case to be made for developing a strategy / capacity for blogging and counter blogging by Combatant Commands as an operational requirement?
- Is there merit in an expanded effort to develop an open and covert "blogger corps" at the "all-of-government" strategic communication level? What advantages/ disadvantages would this present to the Combatant Command?
- Media pools and "embedded" reporting has worked well to nurture "message discipline" and to ensure reporters understand the military perspective in operations. Is there an analogous "blogger" pool that could be harnessed for specific operations/ and, if so, what are the practical issues/liabilities that this could raise?

3. **"Winning" the war of information effects.** Because it is primarily a political organization with limited military capabilities, Hezbollah's war plans focused on "winning" through the generation of strategic information effects. As noted, their war objectives were to "win by not losing," and to force a political end to the confrontation while maximizing the visibility of Israeli casualties and tactical reverses (so as to give the impression of humiliation). This kind of war aim has implications for the forces seeking to oppose such an actor/agenda, in terms of their choice of military options (both strategic and tactical). While not all future opponents will be as sophisticated as Hezbollah, U.S. Forces must be prepared to plan campaigns that engage militarized opponents whose goal is to effect strategic informational and political/moral "wins" by exploiting the collateral effects of U.S. kinetic force.

   - To what extent is current U.S. doctrine adaptable to dealing with actors like Hezbollah, who possess a sophisticated capacity for blending military competence with strategic information effects? To what extent must current doctrine evolve to recognize new forms of engagement that lie along a continuum between counterinsurgency and maneuver warfare? Is there a need to develop a new doctrine that addresses the kind of hybrid actor environment presented by Hezbollah-type actors?

References

Arkin, W. M. (2007). *Divining Victory: Airpower in the 2006 Israel-Hezbollah War.* Maxwell Air Force Base, Alabama, Air University Press. http://aupress.maxwell.af.mil/books/arkin/arkin-small.pdf

Collings, D. & Rohozinski, R. (2006) *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations*. Carlisle, U.S. Army War College. http://www.csl.army.mil/usacsl/publications/ShiftingFireMenu.pdf

Crooke, A. & Perry, M. (2006a). "How Hezbollah Defeated Israel - Part 1: Winning the intelligence war." *Asia Times Online*, 12 October. http://www.atimes.com/atimes/middle_east/hj12ak01.html

Crooke, A. & Perry, M. (2006b). "How Hezbollah Defeated Israel – Part 2: Winning the ground war." *Asia Times Online*, 13 October. http://www.atimes.com/atimes/middle_east/hJ13Ak01.html

Crooke, A. & Perry, M. (2006c). "How Hezbollah Defeated Israel – Part 3: The political war." *Asia Times Online*, 14 October. http://www.atimes.com/atimes/middle_east/hJ14Ak01.html

Dahan, D. M. (2007). "The *Infosphere* during the second Lebanon-Israel War." Unpublished Research Report, commissioned by the Information Society in Palestine Project, University of Cambridge, Advanced Network Research Group.

Erlich, R. & Kahati, Y. (2007) "Hezbollah as a case study of the battle for hearts and minds." Hezeliya, Intelligence and Terrorism Information Center.

Google Earth Blog (2006). "Israel-Lebanon Conflict Illustrated in Google Earth." 21 July. http://www.gearthblog.com/blog/archives/2006/07/israellebanon_c.html

Intelligence and Terrorism Information Center. http://www.intelligence.org.il

Jorisch, A. (2004). "Al-Manar: Hizbullah TV, 24/7." *Middle East Quarterly* 9:1. http://www.meforum.org/article/583

Kalb, M. and Saivetz, C. (2007). "The Israel-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." Kennedy School of Government Faculty Working Paper Series. Boston, MA, Harvard University. http://www.brookings.edu/~/media/Files/events/2007/0217islamic%20world/2007islamforum_israel%20hezb%20war.pdf

Kinniburgh, J. & Denning, D. (2006) Blogs and Military Information Strategy. *IO Sphere*, 5-13.

Internet World Statistics. "Middle East." http://www.internetworldstats.com/middle.htm

Pahlavi, P. C. (2007). "The 33 Day War: An Example of Psychological Warfare in the Information Age." *Canadian Army Journal* 10:2, 12-24. http://www.army.forces.gc.ca/caj/documents/vol_10/iss_2/CAJ_vol10.2_05_e.pdf

Rid, D. T. (2007). "War 2.0." *Policy Review*, February. Stanford, Hoover Institution. http://www.hoover.org/publications/policyreview/5956806.html

Thomas, T. (2007) "Hezballah, Israel and the Cyber PSYOP." *IO Sphere*, 31-35.

Ward, W. (2007). "Uneasy Bedfellows: Bloggers and Mainstream: Media Report the Conflict in Lebanon." *Arab Media & Society*, February. http://www.arabmediasociety.com/articles/downloads/20070312144654_AMS1_Will_Ward.pdf

Wikipedia. "Hasbara." http://en.wikipedia.org/wiki/Hasbara

Wikipedia. "INS *Hanit*." http://en.wikipedia.org/wiki/INS_Hanit

Wikipedia. "Megaphone desktop tool." http://en.wikipedia.org/wiki/Megaphone_desktop_tool

Wikipedia. "*Yalla Ya Nasrallah.*" http://en.wikipedia.org/wiki/Yalla_Ya_Nasrallah

Ya Libnan. (2006). "Full English text of Aoun-Hezbollah agreement." 9 February. http://yalibnan.com/site/archives/2006/02/full_english_te.php

YouTube. "*satla nassralla.*" http://www.youtube.com/watch?v=llp1iob9fEA

New Media and Information Effects during the 2006 Israeli-Hezbollah War in Lebanon

CASE STUDY 3: Countering new media

In the 2006 Israeli-Hezbollah War in Lebanon, both Hezbollah and the IDF sought to shape the information environment and to counter each other's messaging capabilities and content through defensive and offensive IO initiatives. This breakout group considers Israeli and Hezbollah "counter-measures" to disrupt, destroy or otherwise inhibit the opponent's use of new media.

The IDF's "countering" campaign was largely offensive and kinetic, seeking to physically destroy Hezbollah's capacity to communicate. By contrast, Hezbollah's strategy was more "defensive," seeking to limit the IDF's ability to use Hezbollah's new media capabilities against itself (e.g., by compromising Hezbollah OPSEC, for example. See discussion in Case Study #1).

A. Israel's new media "counter measures"

In general, the IDF's IO capabilities and techniques are largely similar to those available to U.S. Forces. During the war, the IDF pursued a sophisticated and full spectrum IO campaign, although most accounts suggest the effort was highly conventional and unimaginative (i.e. with no special attention to leveraging new media). The strategy was also based mostly on intimidation and coercion, and did not seek to engage or sway the Lebanese population against Hezbollah in any meaningful way.[1]

Israel's strategic communication campaign also suffered from "mixed messaging." Thus, Israel sought to justify its use of force and reassure U.S. and European audiences that its intent was to target only Hezbollah, while linking this goal with the Global War on Terror. However, the credibility of this message was severely undermined by ill-timed statements by senior Israeli leaders, such as Army Chief of Staff Lt. Gen. Dan Halutz, who warned that the IDF intended to target infrastructure and would "turn back the clock in Lebanon by 20 years."[2] Such statements "hollowed out" the Israeli strategic communication effort and cast Israeli actions as callous and vengeful in the eyes of some audiences.

Open source literature provides the following examples of IDF efforts to "counter" Hezbollah's new media capabilities or information effects:

1. **Direct kinetic strikes against critical Hezbollah communication targets.** IDF strikes resulted in the total destruction of Al-Manar's main broadcast studios in Beirut, as well as critical radio relay and rebroadcast towers. The IDF also undertook additional selected strikes against other telecommunications facilities, but not enough to totally

[1] Pahlavi (2007).

[2] BBC (2006)

disable them.[3] A UN post-war damage assessment concluded that communications were disrupted but not severed even in the south of Lebanon where most of the fighting took place. It is unclear from the public record whether the partial communications' functioning was a deliberate IDF strategy or not (that is, whether the IDF saw greater value in allowing some channels to function in order to gather intelligence, or, whether they desired some retention of Hezbollah's Command and Control network to allow for a rapid de-escalation after a ceasefire). Some sources also suggest that Hezbollah's Al-Manar "raised the negatives" for further IDF attacks by co-locating their facilities with the Lebanese national communications grid, so IDF strikes would result in significant collateral damage.

2. **PSYOP and electronic attacks involving Hezbollah radio and TV assets.** Several times during the war the IDF managed to hijack Al-Manar frequencies and broadcast a PSYOP message (a video of Hassan Nasrallah looking at the ground, followed by the sound of two shots, and the caption, "Your time is coming, soon").[4] Electronic attacks against Hezbollah facilities were unsuccessful as Al-Manar continued its terrestrial broadcast and the regional satellite feed remained intact. IDF public sources claim that the IDF was unable to successfully block the signals because of Al-Manar's switching of frequencies, and its redundant use of both satellite and terrestrial broadcast facilities.[5]

3. **Use of leaflets and e-leaflets.**[6] The IDF air dropped leaflets extensively in the South warning inhabitants not to support Hezbollah. A similar technique was used whereby automated message systems called individual subscribers of fixed and mobile networks warning them to leave areas of military operations.

4. **Computer network attacks against selected Lebanese and Arab Internet resources resulted in some sites being hijacked or denied service.**[7] However, these attacks cannot be directly attributed to the IDF, which never officially claimed them; the attacks may have been the work of other "patriotic" hackers.[8]

5. **Deliberate deception.** Israeli intelligence is reported to have set up the "all4lebanon.org" website in Arabic, English and French, as well as other un-attributed websites and blogs that were used to advocate for pro-Israeli positions.[9] (This effort to counter Hezbollah support and sow confusion is also a form of "leveraging" new media).

6. **Strategic communication.** Israeli spokespersons regularly briefed the domestic and international press. Extensive use was made of news conferences as well as sanitized intelligence product to rationalize the choice of targets, demonstrate the effectiveness of IDF "kills" and expose Hezbollah duplicity and propaganda techniques. In addition, Israeli

[3] Arkin (2007).

[4] Pahlavi (2007).

[5] Cordesman and Sullivan (2007).

[6] Friedman (2006).

[7] Pahlavi (2007).

[8] The following references are in Hebrew: http://www.ynet.co.il/articles/0,7340,L-3277380,00.html; http://www.ynet.co.il/articles/0,7340,L-3273447,00.html; http://www.ynet.co.il/articles/0,7340,L-3268400,00.html; http://net.nana10.co.il/Article/?ArticleID=383514&sid=127

[9] Dahan (2007).

diaspora networks were mobilized and encouraged to write pro-Israel editorials and OpEds in foreign national papers (See discussion in Case Study # 2).

Interestingly, some of the greatest successes in countering Hezbollah's information effects were generated not by the IDF, but by civil society and civic watchdog organizations that were supportive of Israel's positions. The private U.S. web site "little green footballs" for example broke the story of a Reuters' photographer who allegedly had touched up photographs of destruction of Hezbollah's neighborhoods in Beirut.[10] As a result, Reuters was forced to apologize and pulled all 920 images taken by the photographer out of its catalogue. Similarly several other "staged" media events were exposed as fake by a variety of citizen activist run websites.

Pro-Israeli supporters were also (and still are) operating several Internet watchdog organizations that work to smoke out and deregister Hezbollah websites by legal means. Two sister organizations – Internet Haganah[11] and the Society for Internet Research[12] (both run by Aaron Weisburd, a U.S. citizen[13]) – have used legal means to force ISPs to stop hosting Hezbollah and other sites that are somehow connected to the State Department's list of terrorist organizations.[14]

B. Hezbollah's new media "counter measures"

Hezbollah lacked the capability to conduct full spectrum offensive countermeasures against Israeli "new media" capabilities, although it did appear to exploit the IDF's reliance on certain forms of new media to compromise IDF OPSEC (see discussion in Case Study #1). Unlike the IDF, then, Hezbollah's new media related "counter measures" were largely defensive in nature, focused on protecting itself from "exposure" to the IDF through new media means by exercising a very low level of visibility (especially for its military wing), relying on more "old fashioned" means of communication, using redundant communication capabilities, and exercising a highly centralized and disciplined control over its strategic communication. (See discussion in Case Study # 1).

C. Issues and questions for discussion

(Ground discussion in concrete examples where possible)

Techniques used to counter or inhibit new media (used by the opponent) touch on important issues of international law, and raise questions concerning the practicality of certain "control and denial" measures, as well as their effectiveness (e.g., cost benefits/liabilities of certain techniques such as network-based attacks).

1. Cost-benefit and legal implications of direct kinetic attacks against ostensibly civil assets. Direct kinetic attacks against television stations and civilian communications

[10] Little green footballs (2006); and Kalb and Saivetz (2007).

[11] Internet Haganah. *Website*.

[12] Society for Internet Research. *Website*.

[13] Wikipedia. "Internet Haganah."

[14] Ibid.

systems have been used in the past by U.S./NATO forces, notably in Bosnia and Kosovo. In the case of strikes directed against Al-Manar, these were not successful in disrupting the station's operations due to the degree to which Hezbollah had planned for this contingency. Kinetic attacks also raise questions of whether they contravene Article 147 of the Fourth Geneva Convention,[15] which prohibits "extensive destruction and appropriation of property not justified by military necessity and carried out unlawfully and wantonly."[16]

- Is there evidence that deliberate, kinetic targeting of an opponent's media capacity has yielded a positive tactical or strategic win? What are the legal considerations that require clarification to ensure freedom of action for Combatant Commands?

2. **Network-based attacks: legal and "collateral" issues.** Computer network attacks are an emergent form of warfare, much of which remains, for good reason, in the classified realm. Computer Network Attacks were used extensively during the 2006 Israeli-Hezbollah War in Lebanon. This form of attack raises issues of legality. Moreover, given that software code and attack vectors used to execute them generally must pass through Internet connections not owned by your opponent (e.g., in sovereign spectrum space, or belonging to a neutral third party) there is an issue of potential collateral damage. There are also serious questions about how to measure the real effectiveness of such attacks (versus the effort necessary to mount them).

   Another form of Internet-focused control, which was not used by either party during the war, is that of selective "filtering" of websites and communications services (such as cell and SMS services) by technical means. The effect of these techniques ranges from total denial (via the use of strong adaptive 24/7 filtering technologies) to a selective "just in time" basis that disables the website or devices during certain critical periods of time. Certain states are increasingly employing filtering techniques to disrupt the activities of groups seen as a threat to state interests. Evidence-based examples can be found in Burma,[17] Belarus,[18] Ethiopia, Iran, Uzbekistan and China.[19] However, filtering techniques are also used for other purposes, for example, in the U.S., to block pornography and other unacceptable materials on computers at public libraries and other government-funded institutions.

   Given the increasing use of filtering technologies both domestically (in the United States) and by other states, there is a growing international acceptance of these techniques:

   - To what extent would filtering techniques be acceptable and deemed effective for use by Combatant Commands in the pursuit of suppressing opponents' use of new media? (For example, preventing the uploading of videos to YouTube and other video sharing sites)?

   - What are the potential liabilities of opting for such methods, including unintended blowback?

[15] Exum, A. (2007).

[16] Wikipedia. "Fourth Geneva Convention."

[17] OpenNet Initiative (2007).

[18] OpenNet Initiative (2006).

[19] OpenNet Initiative. "Research."

3. **Third party efforts in support of IO?** During the war, various "third parties" undertook activities that targeted Hezbollah information operations and use of new media. These included legal action by civil society organizations to close down Hezbollah operated assets in the United States and Europe, as well as "watchdog" campaigns to expose Hezbollah fabrications of "evidence." Civil society initiated activities reside outside the military sphere, although they can be supported through associated capabilities in public affairs (such as blog and counter blog teams and the rapid dissemination of information).

    - To what extent would DOD benefit from an expanded capacity to support civil society third party efforts rather than leaving this to other government entities, or maintaining an entirely hands-off approach? What are the potential benefits and liabilities of such an approach?

References

Arkin, W. M. (2007). *Divining Victory: Airpower in the 2006 Israel-Hezbollah War.* Maxwell Air Force Base, Alabama, Air University Press. http://aupress.maxwell.af.mil/books/arkin/arkin-small.pdf

BBC (2006). "Hezbollah warns Israel over raids." 12 July. http://news.bbc.co.uk/2/hi/middle_east/5173078.stm

Cordesman, A. H. & Sullivan, W. D. (2007). *Lessons of the 2006 Israeli-Hezbollah war*. Washington, D.C., CSIS Press.

Dahan, D. M. (2007). "The "Infosphere" during the second Lebanon-Israel War." Unpublished Research Report, commissioned by the Information Society in Palestine Project, University of Cambridge, Advanced Network Research Group.

Exum, A. (2007) "Illegal Attack or Legitimate Target? Al Manar, International Law, and the Israeli War in Lebanon." Arab Media & Society, February. http://www.washingtoninstitute.org/opedsPDFs/45f6c5d5b3f57.pdf

Friedman, H. A. (2006). "Psychological Operations during the Israel-Lebanon War 2006." http://www.psywar.org/israellebanon.php

Internet Haganah. *Website*. http://internet-haganah.com/haganah

Kalb, M. and Saivetz, C. (2007). "The Israel-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." Kennedy School of Government Faculty Working Paper Series. Boston, MA, Harvard University. http://www.brookings.edu/~/media/Files/events/2007/0217islamic%20world/2007islamforum_israel%20hezb%20war.pdf

Little green footballs (2006). "Reuters Doctoring Photos From Beirut?" 5 August.
http://littlegreenfootballs.com/weblog/?entry=21956_Reuters_Doctoring_Photos_from_Beirut

OpenNet Initiative (2006). "The Internet and Elections: The 2006 Presidential Election in Belarus."
http://opennet.net/blog/2006/05/oni-releases-belarus-internet-watch-report

OpenNet Initiative (2007). "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma." http://opennet.net/research/bulletins/013

OpenNet Initiative. "Research." http://opennet.net/research

Pahlavi, P. C. (2007). "The 33 Day War: An Example of Psychological Warfare in the Information Age." Canadian Army Journal 10:2, 12-24. http://www.army.forces.gc.ca/caj/documents/vol_10/iss_2/CAJ_vol10.2_05_e.pdf

Society for Internet Research. *Website*. http://www.sofir.org

Wikipedia. "Fourth Geneva Convention." http://en.wikipedia.org/wiki/Fourth_Geneva_Convention

Wikipedia. "Internet Haganah." http://en.wikipedia.org/wiki/Internet_Haganah

References and further readings

Alarilla, J. (2009). “Iran election protests harness power of Twitter, New Media.” *CNET Asia*, June 16. http://asia.cnet.com/blogs/babelmachine/post.htm?id=63011506

Arkin, W. M. (2007). *Divining Victory: Airpower in the 2006 Israel-Hezbollah War*. Maxwell Air Force Base, Alabama, Air University Press. http://aupress.maxwell.af.mil/books/arkin/arkin-small.pdf

BBC (2006). “Hezbollah warns Israel over raids.” 12 July. http://news.bbc.co.uk/2/hi/middle_east/5173078.stm

Bruhl, J. (2009). “Some lurking OPSEC dangers….” *Soldiers in the Blogosphere*, 14 February. http://soldierblogging.blogspot.com/search?q=some+lurking+OPSEC

Caldwell, W.B. (2008). “Changing the Organizational Culture.” *Small Wars Journal* Blog, 1 January. http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/

Chassay, C. (2007). “Google Earth used to target Israel.” *Guardian*, 25 October. http://www.guardian.co.uk/technology/2007/oct/25/google.israel

Collings, D. & Rohozinski, R. (2006) *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations*. Carilisle, US Army War College. http://www.csl.army.mil/usacsl/publications/ShiftingFireMenu.pdf

comScore (2009). “Russia has World’s Most Engaged Social Networking Audience.” Press Release, July 2. http://www.comscore.com/Press_Events/Press_Releases/2009/7/Russia_has_World_s_Most_Engaged_Social_Networking_Audience

Cordesman, A. H. & Sullivan, W. D. (2007). *Lessons of the 2006 Israeli-Hezbollah war.* Washington, D.C., CSIS Press.

Crooke, A. & Perry, M. (2006a). “How Hezbollah Defeated Israel - Part 1: Winning the intelligence war.” *Asia Times Online*, 12 October. http://www.atimes.com/atimes/middle_east/hj12ak01.html

Crooke, A. & Perry, M. (2006b). “How Hezbollah Defeated Israel – Part 2: Winning the ground war.” Asia Times Online, 13 October. http://www.atimes.com/atimes/Middle_East/HJ13Ak01.html

Crooke, A. & Perry, M. (2006c). “How Hezbollah Defeated Israel – Part 3: The political war.” *Asia Times Online*, 14 October. http://www.atimes.com/atimes/Middle_East/HJ14Ak01.html

Dahan, D. M. (2007). *The ‘Infosphere’ during the second Lebanon-Israel War*. Unpublished Research Report, commissioned by the Information Society in Palestine Project, University of Cambridge, Advanced Network Research Group.

Dauber, C. (2009). “The TRUTH is out there: Responding to Insurgent Disinformation and Deception Operations.” *Military Review*, January-February. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art005.pdf

Department of the Army. (2008). *FM-07, Training for Full Spectrum Operations*. Washington, D.C. Available on Army Knowledge Online, www.us.army.mil

Erlich, R. & Kahati, Y. (2007). *Hezbollah as a case study of the battle for hearts and minds*. Hezeliya, Intelligence and Terrorism Information Center.

Exum, A. (2006). “Hizbullah at War: A Military Assessement.” *Policy Focus* 63. Washington, DC, The Washington Institute for Near East Policy. http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf

Exum, A. (2007). “Illegal Attack or Legitimate Target? Al Manar, International Law, and the Israeli War in Lebanon.” *Arab Media & Society*, February. http://www.washingtoninstitute.org/opedsPDFs/45f6c5d5b3f57.pdf

Friedman, H. A. (2006). “Psychological Operations during the Israel-Lebanon War 2006.” http://www.psywar.org/israellebanon.php

Google Earth Blog. (2006). "Israel-Lebanon Conflict Illustrated in Google Earth." 21 July. http://www.gearthblog.com/blog/archives/2006/07/israellebanon_c.html

Harel, A. (2007). "IDF to reestablish unit aimed at monitoring military telephones." *Haaretz (Hebrew version)*, Tel Aviv.

Helmer, D. (2007). "Not quite counterinsurgency: a cautionary tale for U.S. forces based on Israel's operation change of direction." *Armor*, January-February. http://www.defence.gov.au/army/lwsc/docs/aaj_winter_2008_2_2.pdf

Hoffman, Frank (2009). " Hybrid Threats: Reconceptualizing the Evolving Charcter of Modern Conflict." Strategic Forum, No. 240 (April). Washingtong, D.C: Institute for National Strategic Studies. National Defense University. http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=127094&ord588=grp1&fecvid=21&v21=127094&ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=98862

Holt, J. (2008). Discussion contribution to "Public Affairs and Information Operations." *Small War Journal* Blog, 30 December. http://smallwarsjournal.com/blog/2008/12/public-affairs-and-information/

Intelligence and Terrorism Information Center. http://www.intelligence.org.il

Internet Haganah. *Website*. http://internet-haganah.com/haganah

Internet World Statistics. "Middle East." http://www.internetworldstats.com/middle.htm

Internet World Stats. (2009). "World Internet Usage Statistics News and World Population." http://www.internetworldstats.com/stats.htm

Jorisch, A. (2004). "Al-Manar: Hizbullah TV, 24/7." *Middle East Quarterly* 9:1. http://www.meforum.org/article/583

Kalb, M. and Saivetz, C. (2007). "The Israel-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict." *Kennedy School of Government Faculty Working Paper Series*. Boston, MA, Harvard University. http://www.brookings.edu/~/media/Files/events/2007/0217islamic%20world/2007islamforum_israel%20hezb%20war.pdf

Kinniburgh, J. & Denning, D. (2006) "Blogs and Military Information Strategy." *IO Sphere*, 5-13.

Kreps, Sarah (2007). "The 2006 Lebanon War: Lessons Learned." *Parameters*, Spring. US Army War College. http://www.carlisle.army.mil/USAWC/Parameters/07spring/kreps.pdf

Little green footballs. (2006). "Reuters Doctoring Photos From Beirut?" 5 August. http://littlegreenfootballs.com/weblog/?entry=21956_Reuters_Doctoring_Photos_from_Beirut

Matthews, M. (2006). Interview with BG (ret.) Shimon Naveh (IDF). *Operational Leadership Experiences in the Global War on Terror*. Fort Leavenworth, Kansas, Combat Studies Institute.

Melber, A. 2008. "US Soldiers Blocked From Blogging." *The Nation*, 27 August. http://www.thenation.com/doc/20080915/melber

Mountain Rose IDF Mobile Communications Network. http://www.defense-update.com/products/m/mountain-rose.htm

Murphy, D. (2008). "Fighting Back: New Media and Military Operations." *Issue Paper*, Center for Strategic Leadership, US Army War College, November. http://www.carlisle.army.mil/DIME/documents/Fighting%20Back%20(Murphy).pdf

Murphy, D. (2009). "Operations Security in the Age of Radical Transparency." *Issue Paper*, Center for Strategic Leadership, US Army War College, January. http://www.carlisle.army.mil/DIME/documents/Murphy%20OPSEC%20and%20Radical%20Transperancy.pdf

Open Source Intelligence Analysis Network. *Al Qaeda's Open Source Intelligence*. http://osianintel.com/AQOSINT.aspx

OpenNet Initiative. (2006). *The Internet and Elections: The 2006 Presidential Election in Belarus*. http://opennet.net/blog/2006/05/oni-releases-belarus-internet-watch-report

OpenNet Initiative. (2007). *Pulling the Plug: A Technical Review of the Internet Shutdown in Burma*. http://opennet.net/research/bulletins/013

OpenNet Initiative. "Research." http://opennet.net/research

Organization for Economic Cooperation and Development (OECD). (2009). *Armed Violence Reduction: Enabling Development*. Paris. http://www.oecd.org/document/21/0,3343,en_2649_33693550_42281877_1_1_1_1,00.html

Pahlavi, P. C. (2007). "The 33 Day War: An Example of Psychological Warfare in the Information Age." *Canadian Army Journal* 10:2, 12-24. http://www.army.forces.gc.ca/caj/documents/vol_10/iss_2/CAJ_vol10.2_05_e.pdf

Rid, D. T. (2007). "War 2.0." *Policy Review*, February. Stanford, Hoover Institution. http://www.hoover.org/publications/policyreview/5956806.html

Rohozinski, R. (2003). "Bullets to Bytes: Reflections on ICT and "Local Conflict"," in Latham, R. (Ed.), *Bombs and Bandwidth : The Emerging Relationship Between IT and Security*. New York, New Press.

Society for Internet Research. *Website*. http://www.sofir.org

Thomas, T. (2007) "Hezballah, Israel and the Cyber PSYOP." *IO Sphere*, 31-35.

Tryhorn, C. (2009). "Nice talking to you ... mobile phone use passes milestone." *The Guardian*, March 3. http://www.guardian.co.uk/technology/2009/mar/03/mobile-phones1

Ward, W. (2007). "Uneasy Bedfellows: Bloggers and Mainstream: Media Report the Conflict in Lebanon." *Arab Media & Society*, February. http://www.arabmediasociety.com/articles/downloads/20070312144654_AMS1_Will_Ward.pdf

Wass de Czege, H. (2008). "Rethinking IO: Complex Operations in the Information Age." *Military Review*, November-December. http://www.carlisle.army.mil/DIME/documents/MilitaryReview_20081231_art006%5B2%5D.pdf

Wikipedia (2009). "Crowdsourcing." http://en.wikipedia.org/wiki/Crowdsourcing

Wikipedia. "Fourth Geneva Convention." http://en.wikipedia.org/wiki/Fourth_Geneva_Convention

Wikipedia. "Hasbara." http://en.wikipedia.org/wiki/Hasbara

Wikipedia. "INS *Hanit*." http://en.wikipedia.org/wiki/INS_Hanit

Wikipedia. "Internet *Haganah*." http://en.wikipedia.org/wiki/Internet_Haganah

Wikipedia. "Megaphone desktop tool." http://en.wikipedia.org/wiki/Megaphone_desktop_tool

Wikipedia. "*Yalla Ya Nasrallah*." http://en.wikipedia.org/wiki/Yalla_Ya_Nasrallah

Winograd (2007). The main findings of the Winograd partial report on the Second Lebanon War. Tel Aviv, Government of Israel.

Ya Libnan (2006). "Full English text of Aoun-Hezbollah agreement." 9 February. http://yalibnan.com/site/archives/2006/02/full_english_te.php

YouTube. "satla nassralla." http://www.youtube.com/watch?v=llp1iob9fEA

GLOSSARY

CENTAF	Air Force Central Command
CENTCOM	United States Central Command
DA	Department of the Army
DOD	Department of Defense
Digital Natives	The generation that has grown up plugged into new media (essentially under 30)
Digital Immigrants	The generations who have come to new media as adults, or not at all
FDOs	Feature Data Objects
GIE	Global Information Environment
GPS	Global Positioning System
IDF	Israeli Defense Forces
IED	Improvised Explosive Device
IO	Information Operations
ITU	International Telecommunications Union
JDAM	Joint Direct Attack Munition
JAM	*Jaish Al-Mahdi*
LICUS	Low Income Countries Under Stress
NCO	Non-Commissioned Officer
NGO	Non-Governmental Organization
OECD	Organization for Economic Cooperation and Development
OSD	Office of the Under Secretary of Defense
OPSEC	Operations Security
OSINT	Open Source Intelligence
PA	Public Affairs
ROE	Rules of Engagement
SIGINT	Signals Intelligence
SME	Subject Matter Expert
UAV	Unmanned Aerial Vehicle
USAWC	United States Army War College
USIA	United States Information Agency

Bullets and Blogs: New Media and the Warfighter

In the contemporary operational environment symbolic informational wins can precipitate strategic effects equivalent to, or greater than, lethal operations. New adversaries understand the power of "information effects." They realize that new media have leveled the playing field between state and non-state actors in the area of strategic communication. Anyone with access to a digital camera and the Internet can be an *infowarrior* and reach a global audience. In recent wars, new adversaries — exploiting new media capabilities and an information-led warfighting strategy — have proven capable of denying victory to stronger conventional military forces.

In recognition of the challenge that new media represents, the U.S. Army War College (USAWC) hosted a two-day workshop — "*Bullets and Blogs: New Media and the Warfighter*" — that brought together leading practitioners from the Department of Defense (DOD), Department of State, Intelligence Community and academia.

Participants considered the manifold ways that new media and the Global Information Environment are changing the geo-strategic calculus for warfighting: How are adversaries leveraging new media for strategic wins? What are the institutional, organizational and cultural barriers that compromise or unduly restrict DOD's agility on this playing field? What does the age of "radical transparency" mean for Operations Security? Does the shift of capabilities to address multiple and hybrid threats take sufficient account of the need to transform DOD's approach to the informational battlespace?

Participants concurred that the informational terrain is an integral component of today's operational environment. Warfighters need to be able to use all the means at their disposal to achieve the desired endstate, "*whether that is firing a tank round, or pushing a button to deliver the 'blue screen of death.'*"

DOD needs to plan for combat against opponents employing an information-led war fighting strategy, who are adept in the tactical use of new media. This requires a paradigm shift away from an emphasis on information control and toward information engagement. It will require cultural and organizational change as DOD navigates the world of digital natives – which includes both its own Soldiers, Sailors, Airmen and Marines, as well as its media-agile adversaries. Most of all, it will force the sustained adaptation and evolution of the way the U.S. military thinks and fights.

TheSecDevGroup