

IOI

Inaugural
Issue

Vol. 1, Issue 1
April 2009

IO Journal

A publication of the Association of Old Crows' Information Operations Institute



In This Issue:

Why Warfighters Don't Understand IO
Psyop in the Age of Inter-Consciousness

Barriers to Entry for Cyber Warfare
The Role of Background Conversations



New Beginnings Bring New Challenges

With the new network-centric solutions needed to keep America safe, there will be many challenges. We have the right people to address them. We're Science Applications International Corporation — 45,000 smart, dedicated people who have the deepest understanding of their fields and a passion to find the right solution.

No job is more important to us than keeping America safe, and we take pride in knowing that we're trusted to make a difference. Designing safe network-centric solutions and keeping networks and critical infrastructure running to protect our country against threats are just a few of the missions we take to heart every day. Smart people solving hard problems.

For detailed information, visit us at www.saic.com

Energy | Environment | National Security | Health | Critical Infrastructure



© 2009 Science Applications International Corporation. All rights reserved.

IO Journal

|o| Contents

- | | | | |
|-----------|--|-----------|--|
| 6 | Barriers to Entry: Are They Lower for Cyber Warfare?
By Dorothy E. Denning | 22 | Political and Technical Roadblocks to Cyber Attack Attribution
By Jeff Wozniak and Prof. Samuel Liles, Purdue University Calumet |
| 11 | The Role of Background Conversations, Culture and a Harmonized Communications Strategy in Effecting Change
By Roberta-diane Perna, Ph.D. | 29 | PSYOP in the Age of Inter-Consciousness
By Clay Wilson, PhD, CISSP |
| 18 | Talking the Talk: Why Warfighters Don't Understand Information Operations
By Dennis M. Murphy | 36 | Information Related Terms, Trends and Myths
By Garry J. Beavers and F. H. "Skip" Allison |

EDITORIAL ADVISORY BOARD

Mr. Robert Giesler
Mr. Austin Branch, SES
Mr. Mark Johnson, SES
Dr. Dan Kuehl
RADM Andy Singer, USN (Ret)
Mr. Kirk Hunigan
BG John Davis, USA
RDML Bill Leigher, USN
BrigGen Mark O. Schissler, USAF
Col David Wilkinson, USMC
CAPT Michael Hewitt, USN
Col Al Bynum, USAF (Ret)
LTC Kevin Doyle, USA (Ret)

EDITORIAL & PRODUCTION

STAFF

Editors: Joel Harding, Dr. Dan Kuehl
Design & Layout: Deb Churchill-Basso

Submissions: The *IO Journal* welcomes article submissions for consideration. Manuscripts should be of interest to the information operations community and should include proper sourcing with endnotes. All articles are peer reviewed. Direct all submissions to Joel Harding, jharding@crowns.org.

©2009 Association of Old Crows/Naylor, LLC. All rights reserved. The contents of this publication may not be reproduced by any means, in whole or in part, without the prior written authorization of the publisher.

Editorial: The articles and editorials appearing in this magazine do not represent an official AOC position, unless specifically identified as an AOC position.



Emerging technologies.

Unpredictable threats.

Elusive enemies.

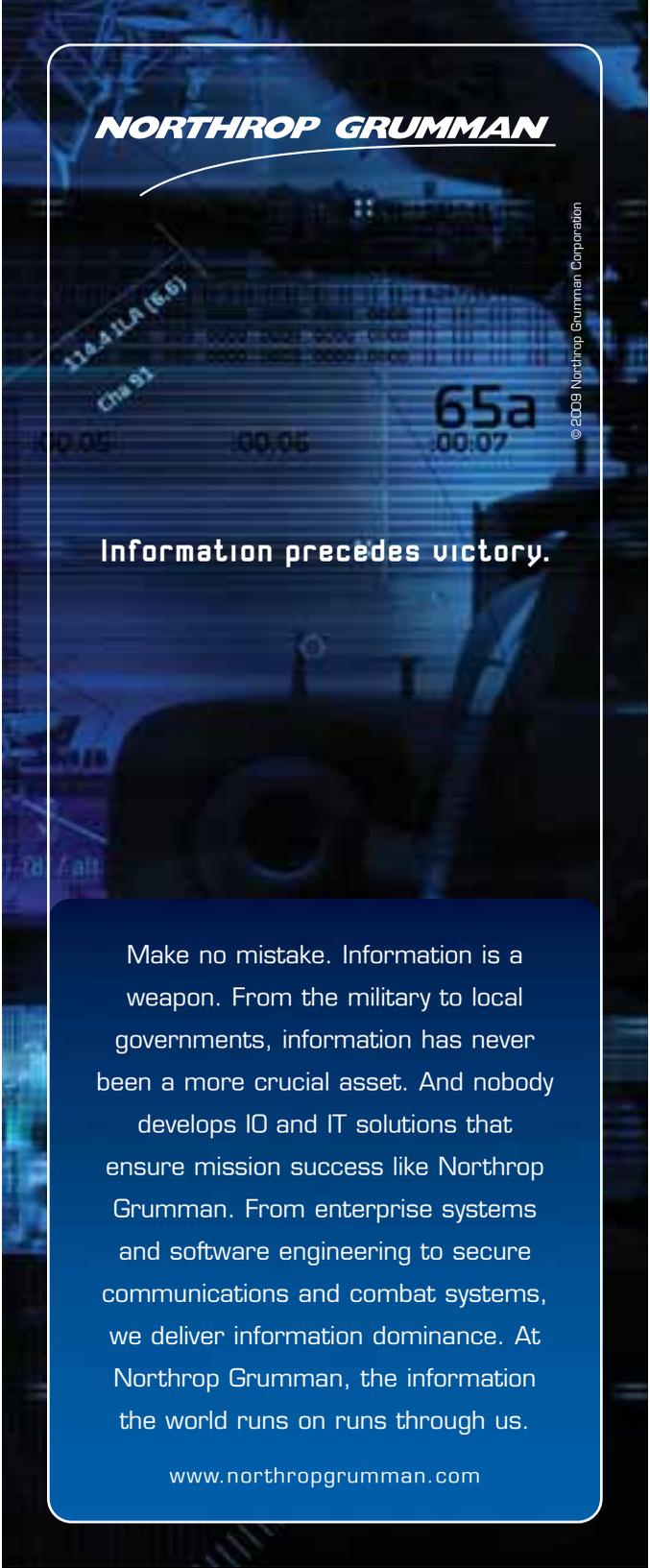
Ready for what's next.

Now more than ever, mission success depends on the ability to continually adapt thinking and operations. With the perspective, experience, and know-how from battlefields and boardrooms, the strategy and technology consultants of Booz Allen Hamilton can help you achieve your cyber goals. Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.

Ready for what's next. www.boozallen.com

Booz | Allen | Hamilton

delivering results that endure



NORTHROP GRUMMAN

Information precedes victory.

Make no mistake. Information is a weapon. From the military to local governments, information has never been a more crucial asset. And nobody develops IO and IT solutions that ensure mission success like Northrop Grumman. From enterprise systems and software engineering to secure communications and combat systems, we deliver information dominance. At Northrop Grumman, the information the world runs on runs through us.

www.northropgrumman.com

© 2009 Northrop Grumman Corporation

Introducing the *IO Journal*

April 2009 may well mark one of the key dates in the evolution of Information Operations, because of several distinct yet related events. The first is marked by this very journal, the inaugural issue of *IO Journal*, about Information Operations, written by and for information operators. Our intent is to provide a vehicle for discussion and means of advancing the state of our art across a broad and inclusive set of issues and activities focused on the use of information in national security. This issue features contributions from several of the leading and best-known experts in our field, and they have launched *IO Journal* onto a lengthy and impressive flight.

The second event is the return of *InfowarCon*. Those whose involvement in IO dates back to the 1990s will remember the annual *InfowarCon* held in Washington and hosted by Winn Schwartz. After a lapse of several years it – and Winn – has returned. Thanks to the decision of the Old Crows to take on its management and the tremendous support provided by a set of very generous contributing sponsors, this *InfowarCon* surpasses its forbears in the expertise and timeliness of its speakers and panels. Thanks to everyone involved – most especially the attendees – we have recreated the pre-eminent IO conference.

Third is the creation of the Information Operations Institute within the Old Crows. The mission of the IOI is to be a focal point for the development of IO and information operators, an organization in which concepts can be raised, operations explored, and personal networks established. Its intent is not to be an advocate for any particular viewpoint or program, other than to be an advocate for the role and development of IO, but rather to serve as the meeting space for all IO professionals and practitioners, to advance the state of our discipline.

Add to these all of the other things that have happened and are happening with IO, whether it's on the battlefield or inside of cyberspace, and we are at a key stage in the growth and development of IO. In Afghanistan, inside the interagency, inside the web, and certainly inside the governments and militaries of friends and enemies alike, IO has become far more than an enabler or poorly-understood afterthought, it has become an indispensable element of today's security environment. Thus we extend a most-enthusiastic welcome to the *IO Journal*, The IO Institute and *InfowarCon*. It's a great time to be an Info Warrior!

– Dr. Dan Kuehl

IOI

July 29-31: Understanding Deception: A Primer in Deception History and Techniques

AOC Headquarters, Alexandria, VA
Dr. Robert Mackey

Understanding Deception is a three-day course aimed at not only the information operations professional, but leaders in a variety of fields interested in protecting sensitive information and perception shaping. The course will focus on historical examples of deception in warfare, especially the American, British and Soviet experiences of World War II, and modern U.S. military deception doctrine and techniques at the tactical and operational level of war.

Dec. 7-11: Senior Leader Info Ops Course

AOC Headquarters, Alexandria, VA
Dr. Dan Kuehl

An evening course designed for the senior leader in DC-area government, military or industry. Get up to date on critical IO issues and material without impacting your primary job responsibilities.

Barriers to Entry:

By Dorothy E. Denning

Recently, I was contacted by a group of researchers studying cyber warfare. In reading their project description, I was struck by one of their premises: “Barriers for entry to conduct activities in cyberspace are lower than in any military domain.” I thought, yes, this is the conventional wisdom, but is it really true? What about warfare on land? While it may require substantial resources to assemble an army and invade a foreign territory, it is not hard to shoot a gun, toss a grenade, or start a fire – all operations that take place on land. If these operations are considered too individualistic or simple minded to be called land warfare, then is it fair to call a common cyber attack, say a simple denial-of-service (DoS) attack against a public website, cyber warfare? If the DoS attack is considered to be a means of cyber warfare, is it fair to compare its entry requirements with those for a vastly more complex army invasion when the effects are dramatically different? The DoS attack may shut down a communication channel on the Internet for awhile, but the land invasion could result in the overthrow of a government or the seizure of territory.

Perhaps cyber attacks seem to have a lower barrier to entry because they are so commonplace. Moreover, many are simple to perform using “point and click” software tools and easy-to-follow scripts. Teenage “script kiddies” launch cyber attacks without understanding how the tools work or exactly what they do. But young people also join street gangs, and teens who are clueless about conducting DoS attacks shoot guns and mark gang territory with graffiti. Children who have never even heard of the Internet fight in war-torn areas in Africa, wielding weapons and killing other human beings. If one considers all the attacks that take place just on land – shootings, stabbings, beatings, muggings, robberies, arson, etc. etc., surely they are at least as frequent as those in cyberspace, and often as easy to perform.



Are They Lower for Cyber Warfare?

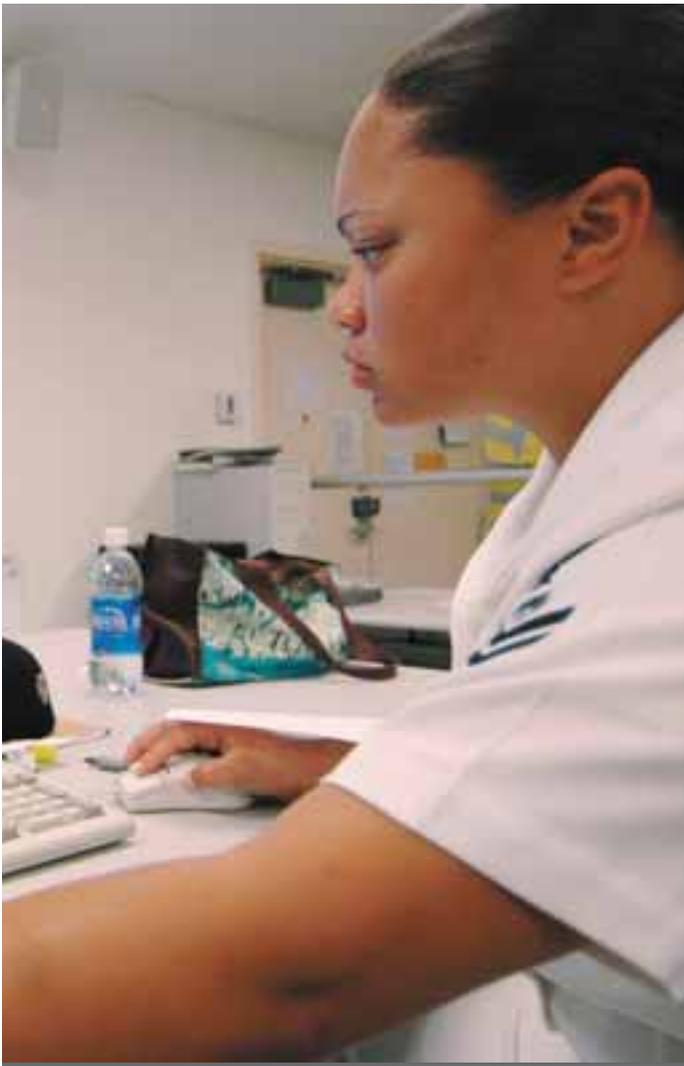


Photo courtesy US Department of Defense.

The objective of this essay is to explore the question of whether operations in cyberspace have a lower barrier to entry than operations in kinetic domains of warfare, especially land. To do this, two factors are considered: costs and effects. Costs reflect barriers to entry and cover everything needed to prepare for and carry out an operation. They include expenditures for weapons, training, tools, facilities, telecommunications, salaries, travel, and recruiting. They also include casualties and arrests that result from the operation. Effects are the outcomes of an operation and include deaths, property damage, financial losses, service disruptions, decisions made, and actions taken.

Costs, or barriers to entry, are then examined relative to their effects. In particular, an operation X in cyberspace is said to have a lower barrier to entry than an operation Y in another domain relative to effects Z if the costs of X are lower than those of Y in order to achieve Z. Stated another way, if a given effect can be achieved in cyberspace for a lower cost than in some other domain, then cyberspace has a lower barrier to entry for achieving that particular outcome.

The remainder of this essay examines costs and effects in greater depth, discusses the Estonian and Georgian cyber conflicts in terms of their barriers to entry, and draws some conclusions.

COSTS

There are several factors that contribute to a sense that the barriers to entry for cyber operations are lower than for other domains. These include remote execution, cheap and available weapons, easy-to-use weapons, low infrastructure costs, low risk to personnel, and perceived harmlessness. The following examines these factors and whether they always hold.

Remote execution. Cyber operations can be conducted remotely, even from the other side of the world. By comparison, kinetic operations generally require that personnel and equip-

ment be physically transported to the target area. This can be extremely costly, such as when armed forces are deployed to a foreign country. If borders must be crossed illegally, it also can be difficult and dangerous. However, there are exceptions to the general rule. A particular cyber operation could require a physical presence at the target site, for example, an accomplice with inside access to the target. Speed or reliability requirements could also preclude some remote attacks, such as from a site vulnerable to frequent network outages. In addition, there are kinetic operations such as the firing of long-range missiles that can be conducted remotely. Also, kinetic targets can be selected on the basis of their proximity, precluding the need to relocate persons and equipment. Instead of traveling to the US, for example, terrorists frequently attack US interests abroad, including embassies and military bases.

Cheap and available weapons. Cyber weapons are cheap and plentiful. Indeed, many are free, and most can be downloaded from the Web. Some cost money, but even then the price is likely to be well under \$100,000. By comparison, many kinetic weapons, for example, fighter jets, aircraft carriers, and submarines, can run into the millions or even billions of dollars. Again, however, there are exceptions. Custom-built software can cost millions of dollars and take years to develop, while kinetic weapons such as matches, knives, and spray paint are cheap and readily available.



BETWEEN DEFENDING AGAINST CYBER ATTACKS AND ENSURING MISSION RESILIENCE, THERE IS ONE IMPORTANT WORD: HOW.



lockheedmartin.com/how

Easy-to-use weapons. Besides being inexpensive, many cyber weapons require little skill beyond that required to operate a computer and use the Internet. By comparison, members of armed services receive extensive training to effectively use kinetic weapons. But as with the other factors, the general rule breaks down when one takes into account complex cyber weapons that require advanced skills or simple kinetic weapons like knives and spray paint that can be used by anyone.

Low infrastructure costs. In general, cyber operations require little infrastructure in the way of facilities and equipment. Even if multiple people are involved, operations can be coordinated from a website, with participants accessing cyberspace from their residences and cyber cafés. In comparison, armed services generally require substantial infrastructure, including military bases, to sustain their activities. However, the generalities do not extend to complex, tightly coupled cyber operations that require a team of people operating within a shared facility or loosely coupled kinetic operations like riots that erupt with little supporting infrastructure.

Low risk to personnel. In general, the persons involved in a cyber operation may be less likely to be captured or killed than persons involved in a kinetic operation. In part, this is because it can be difficult to determine the source of a cyber attack, especially if the attack has used proxies and hopped through multiple machines. Even if the source can be determined, the persons involved may be protected from capture or arrest by international boundaries, especially if they are operating on behalf of or with approval from their host government. In comparison, soldiers on the ground, at sea, or in the air generally risk being the targets of a lethal counter-strike. However, those launching missiles from a remote location or dropping bombs from the air may be safer than cyber operators who are careless or up against a concerted effort to track them down.

Perceived harmlessness. Many cyber attacks such as web defacements and low-level DoS attacks are perceived to be relatively harmless. Nobody dies and damages are not usually permanent. Defaced websites are quickly restored and normal traffic flow resumed when DoS attacks stop. Consequently, there may be less psychological aversion to conducting a cyber attack than a kinetic one, especially one that employs lethal weapons. A 14-year-old hacker might have no qualms about defacing a website, but never shoot a gun or detonate a bomb that would kill people or destroy property. But as with the other generalities, there are exceptions. A cyber attack could be deadly, for example, by disrupting emergency 911 systems, while a kinetic operation such as a peaceful street demonstration could have little or no harmful effects.

EFFECTS

In order to fairly compare the barriers to entry of a cyber operation with a kinetic one, the two operations must have equivalent effects. However, the immediate effects of an operation in cyberspace look substantially different than in other domains. While cyber weapons destroy and block bits, kinetic weapons destroy property, kill people, and block



At the Cyber Command (Provisional) network center at Barksdale Air Force Base, La., Staff Sgts. Benjamin Lockwood (left) and Andrew Corriveau discuss operational status. (US Air Force photo/Lance Cheung)

physical pathways. Moreover, because bits can be replicated and restored, the effects in cyberspace may be short lived in contrast to the permanency of death and longer-term effects of property damage.

Despite these differences, it is possible to frame many effects in a generic form that is domain independent. Casting effects generically provides a means of formalizing what it means for operations in disparate domains to have comparable or equivalent effects. By way of analogy, a bowl of apples is not comparable to a bowl of oranges, but the two bowls of fruit can have comparable weights.

One generic metric that applies to both cyber and kinetic domains is financial losses. Another is disruptions of service. For example, cyber attacks have caused airline delays, halted train service, and shut down ATM machines – all effects that could be achieved with bombs or even just the threat of bombs.

Although most cyber attacks do not damage physical property or result in death, those that do can be compared with kinetic operations that produce equivalent damages. For example, a cyber attack against a water treatment system in Australia caused raw sewage overflows, which in turn caused environmental damage – something that also could have been achieved with toxic chemicals. Although cyber attacks have not yet killed anyone, it is not hard to postulate scenarios that do so, for example, attacks that cause extended power outages or planes to crash.

Operations across domains could also be compared in terms of decisions made and actions taken, for example, a decision to meet an adversary's demands. ISPs, for example, have removed content from websites they host in order to halt crippling DoS attacks from persons who objected to that content. An equivalent operation in physical space might be a protest outside a bookstore or library demanding that a particular book be removed from the shelves. At a state level, a country might agree to the terms of another state as the result of either a cyber or kinetic operation.

THE ESTONIAN AND GEORGIAN CYBER WARS

In late April 2007, Russian hackers began a prolonged cyber war against Estonia. Prompted by the moving of a Soviet-era memorial, the assault in cyberspace included DoS attacks that disrupted access to selected Estonian websites belonging to the government, banks, and the media. It also included web defacements and spamming of government e-mail accounts. The cyber strikes went on for weeks, although the vast majority of the DoS attacks lasted less than an hour and only 5.5% over ten hours. (1) Some of the DoS attacks leveraged large “botnets” of compromised computers, while others involved individual participants following a script that performed a “ping” attack against target websites. (2) The total cost to the assailants was nominal, as participants volunteered their time and computers. Attack tools were free, although fees might have been paid for some of the botnets. Coordination was minimal, generally taking place on web forums frequented by Russian hackers. The risks of being caught and punished were also low, although one hacker living in Estonia was identified and fined about \$1,620. (3)

The immediate effects of the cyber war were loss of access to certain websites and government e-mail accounts. This in turn interfered with the ability of Estonians to make online banking transactions, especially from overseas, and to use their bank cards for purchases. I found no estimate of the total financial losses incurred from the assault, but one bank was said to have lost at least \$1 million. (4) Overall, the losses likely ran well into the tens of millions of dollars, taking into account the service disruptions and the efforts to mitigate, stop, and recover from the attacks.

Could the effects of the Estonian cyber attacks have been achieved with kinetic weapons at a lower cost? In fact, the memorial relocation also sparked low-cost street protests, leading to one death and 150 injuries. (5) However, to fairly compare the cyber and street actions, we need a generic metric, say, total monetary damages. Although I have not seen estimates of financial losses for Estonia's street (or cy-

ber) riots, they are available for other events. The riots in Seattle that accompanied the World Trade Organization's meeting in 2000, for example, caused an estimated \$20 million in property damage and lost sales to downtown businesses, plus at least \$3 million in added city expenses to handle the conference. (6) These damages might be roughly comparable to those of Estonia's cyber and street riots, but it is hard to say.

Even if the effects of the cyber attacks against Estonia exceeded those of the street protests, it is not clear that a repeat attack in cyberspace would have as much impact. The country's cyber defenses have been improved, and a comparable attack today might be relatively minor, with effects substantially less than those of the street riots.

Compared to the Estonian cyber assault, the one against Georgia in August 2008, also attributed to Russian hackers, was much less damaging. One explanation is that because of Estonia, the Georgians were better prepared. Also, the attacks did not persist as long – a few days rather than weeks. In addition, Georgia is less dependent on cyberspace for banking and financial transactions, so the attacks would not have affected day-to-day business as much as in Estonia. For Georgia, the Russian military's invasion of its territory had a much greater impact.

CONCLUSIONS

There are few obstacles to engaging in low-level cyber warfare, particularly DoS attacks and web defacements. Participants can join from anywhere in the world; they need little in the way of weapons, skills, and infrastructure; chances are good they will not be caught or harmed; and they might have few reservations about participating in activity they view as relatively harmless. However, this does not imply that the barriers to entry for cyber warfare are lower than for other domains. There are also few obstacles to conducting many kinetic operations such as street protests, fist fights, and gang warfare.

The important question is whether equivalent effects can be achieved in cyberspace but at a lower cost. To do that, operations must be examined in terms of generic effects that apply across domains, for example, financial losses, service disruptions, casualties, or decisions made. Only then is it fair to compare costs, which measure barriers to entry. It might have been easier and cheaper for Russian activists to engage a cyber militia to attack Estonian websites than for Iraqi insurgents to engage armed militias to attack US forces and each other, but the Iraq violence has caused vastly more damage, including substantial loss of life.

When examined in terms of equivalent effects, the barriers to entry for cyber operations may, on average, be about the same as for kinetic operations. It does not take much to cause a few thousand dollars of damages in either domain. However, if the knowledge, skills, and disposition of individual participants are factored in, there are likely to be persons willing and able to inflict that damage through

a cyber attack but not a kinetic one, and conversely. Someone may join a cyber militia who would never participate in a traditional militia, while someone else may be more attracted to guns and bombs than bits. Thus, rather than competing, the two domains of warfare may draw from different constituents and affect different targets.

Seen from this perspective, cyber warfare opens up a new form of warfare to people who otherwise might not participate. This is especially evident in al-Qa'ida's global jihad, which includes cyber jihadists who attack websites in addition to terrorists who plan and conduct deadly strikes. The barriers to entry for electronic jihad may be lower than for terrorism, but then the effects pale in comparison to the wanton death and destruction of terrorism.

For now, the effects of cyber attacks are relatively minor compared to what is achieved with armed forces, especially military operations that lead to the overthrow of governments, seizure of land, and human casualties. The discrepancy may narrow with more sophisticated cyber attacks that affect physical systems, but such attacks are likely to also have higher costs, raising the barriers to entry.

In the end, there will be different levels of cyber warfare, with low barriers to entry for the patriotic and activist hackers who just want to cause a bit of disruption, not unlike that caused by street demonstrations and other kinetic operations with low barriers to entry. The barriers to entry will be higher for militaries using cyber strikes to achieve national objectives, but whether they will be lower or higher than for kinetic strikes that produce comparable effects is difficult to say without examining the details of specific operations.

Dr. Dorothy E. Denning is Professor of Defense Analysis at the Naval Postgraduate School, where her current research and teaching encompasses the areas of conflict and cyberspace; trust, influence and networks; terrorism and crime; and information operations and security. She is author of Information Warfare and Security and over 140 articles. She has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University. Dr. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University.

ENDNOTES

- 1) "Estonian DDoS – A Final Analysis," Heise Security, 31 May 2007.
- 2) Joshua Davis, "Web War I," Wired, September 2007.
- 3) "Estonia Convicts First 'Cyber-War' Hacker," AFP, 24 January 2008.
- 4) Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," The New York Times, 29 May 2007.
- 5) Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," Culture Mandala, 8:1, October 2008, pp. 28-90.
- 6) "WTO Protests Hit Seattle in the Pocketbook," CBC News, 6 January 2000.



U.S. Army Sgt. 1st Class Ian R. McKnight and Capt. Philip A Borrelli, both with the 324th Tactical Psychological Operations (PSYOP) Company, prepare to drop leaflets down to an Afghan village in Khowst province, Afghanistan. (U.S. Army photo by Sgt. Jessica L. Sheldon/Released)

The Role of Background Conversations, Culture and a Harmonized Communications Strategy in Effecting Change

By Roberta-diane Perna, Ph.D.

The subject of change is endemic in today's literature and a favorite topic of the authorities who appear on network and cable TV. In bygone eras, many of the subject matter experts, each in their own time, rucked up and went forth with the weapons of choice in an attempt to change the physical environments. The United States military is very good at what it does...changing physical environments and deposing dictators. Unfortunately, however, the abundant deliberations of today's experts frequently overlook an important component – the psychological domain – and the need to employ a good communications strategy as an important tool in the process of change. What people think is happening is more important than the reality. (1)

Change often fails because leaders do not give enough strategic thought

to communicating the rationale, the progress, and the consequences of the change all within the context of the cultural environment. A well-planned and executed communications strategy is important as leaders prepare and carry out changes. Strategic thinking about what and how to communicate ameliorates many difficulties often associated with significant change. As a result, a well-planned communication process can ease the way to a more effective change process. (2) Such a process will leverage the effects resulting from coordinated sets of actions directed at shaping the behavior of those affected by the change to conform to a desired outcome. This holds true whether change occurs in the private sector or in the military arena. As an example, when LTG David Petraeus realized the value of the University of Mosul and its importance to the local population, he immediately

assigned the 4th Brigade Commander to assist the university in resuming normal operations. This brought a measure of pride and stability to Mosul creating an atmosphere of cooperation for the changes to come. Unfortunately, not all of the actions of the military forces produced such a positive result as a later example will illustrate.

Implementing a major change in perception across non-western cultures requires a change in the basic information culture in which those populations operate. The challenge this presents is two-fold. First, numerous constituencies, each with its own constructed reality, live within the exiting cultures. Sub-conscious assumptions that comprise a culture's collective state of mind, as well as its religious leanings, form a diverse palimpsest. These include the cultural mythologies that relate stories and customs mirroring the culture, opinions,



An Iraqi army soldier assists U.S. Marine Corps Capt. Mike Fehn, an information operations officer from Regimental Combat Team 5, in putting up a wanted poster onto a T-wall barrier at a tactical control point on Route Phoenix during a combat operation. (U.S. Marine Corps photo by Cpl. Tyler Hill/Released)

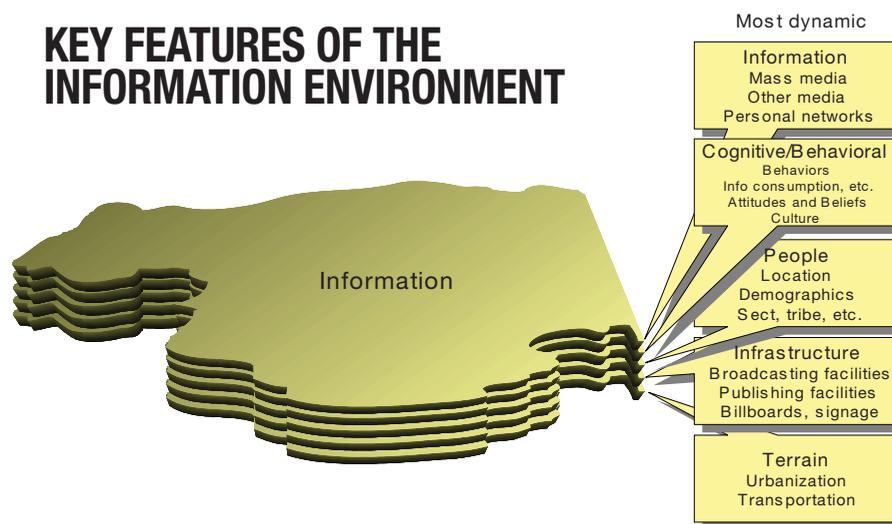
and attitudes surviving from the past; or screens onto which the populations project fantasies that serve as safety valves, sanctions, expressions of “outlawed emotions,” or scapegoats. (3) These background conversations form an implicit, unspoken “backdrop” or background against which explicit, foreground conversations occur, and represent both a context and a reality. If someone from outside the culture is unaware of these cultural backdrops, unexpected negative consequences of actions can occur. For example, the exuberant troops, justifiably proud of their mission and fired up by their successes during the drive to Baghdad, who assisted the Iraqi crowd in pulling down the statue of Saddam Hussein, created a situation with negative ramifications by placing an American flag over the dictator’s head. While their action resonated positively in the western press, it reinforced the background conversations that exist in the Arab world which cast the Americans as conquerors. Such conversations result both from direct and from inherited experiences within a tradition, and provide a space of possibilities that directs the way individuals listen to what another says and does not say, all of which affect the level of resistance to change. (4) While some stories seem to challenge the culture, they in fact preserve it, and others that appear to support norms and values actually indict them. (5) In short, background conversations create the socially constructed reality that forms a culture and its operative assumptions. (6) The contextual reality of the existing environment must change to allow the new culture to grow. If this does not happen, then any change has little chance of success.

Secondly, the key features of the information environment are as layered as those of the culture in which it exists. As the following graphic illustrates, the most dynamic features of this environment are the people, their cognitive/behavioral patterns, and the information sources.

Source: Rand Corporation

Part of the reason that it is frustratingly difficult to describe a culture’s

KEY FEATURES OF THE INFORMATION ENVIRONMENT



collective state of mind is that the individuals within the culture have different background conversations and draw different conclusions from the same physical evidence. (7) Each reality produces a particular view of life within which what someone says derives its meaning from the background conversations or the context in which that person says it – not from a one-to-one relationship with the objects and actions they denote in the observable world. (8) All cultures resemble an onion with layers that peel back the various layers or segments of their contextual reality. What the western world, especially the United States, often fails to realize is that contextual reality is as varied as the different world cultures and that no matter how well intended some actions are, they can have unintended effects. An incident that occurred during the Soviet invasion of Afghanistan demonstrates one such example. Readers will recall that the United States provided various levels of support to the Afghani freedom fighters. Appalled at the logistical difficulty in getting supplies to the mountainous areas, the United States contracted with the old Flying Tigers freight line to fly in some donkeys to assist with the convoy operations. Overjoyed by the donation, the freedom fighters expressed their gratitude at a huge celebration. Sadly by western standards, the featured item on the menu was roasted donkey! After an explanation that the donkeys were beasts of burden not food

– a somewhat incomprehensible concept to the Afghani fighters who operated in austere conditions – the United States shipped over more donkeys...this time accompanied by crates of sunglasses to protect the fighters’ eyes from harmful UV rays. Harmful UV rays meant nothing to the recipients but looking “really cool” in their new sunglasses did, and they proceeded to wear them continuously – even in the dark. (9) One can only wonder how many fighters lost their lives falling down the sides of the mountain passes because the sunglasses obstructed their vision at night.

Transforming the constructed reality of the diverse segments also requires transforming the individuals within each segment. Moreover, transforming the culture and individuals within a culture is never a two-step process but one that must happen simultaneously. The culture and its individuals will transform together or not at all. (10)

One such example occurred during the first elections in Iraq. Officials expressed concern that the blue dye used as a voter identification process would mark those who voted as targets for insurgent violence. Little did anyone realize that the blue finger would become a unifying badge of honor in the new cultural environment that was emerging. It turned into a public relations coup instead of the mark of death they anticipated.

All these facets demonstrate some of the complexity surrounding the desire

to extend democracy in a region where the word has no contextual meaning. To do so, first requires determining what preconceived realities shape how individuals perceive such a concept and to what extent those perceptions drive the resistance to change. To accomplish this, the United States must learn the art of apperception if it expects to accomplish change successfully in environments that do not share a western perspective. Without it, gaining an understanding of the various aspects within each culture is an impossible task. However, once those advocating change accomplish this – and it is admittedly no small undertaking – then they must take the steps necessary to shift the background conversations in ways that will change the perceived realities. Harold Lasswell, a pioneer in the study and practice of propaganda, defined the art of information transmission as the management of collective attitudes by the use of significant symbols. He further differentiated

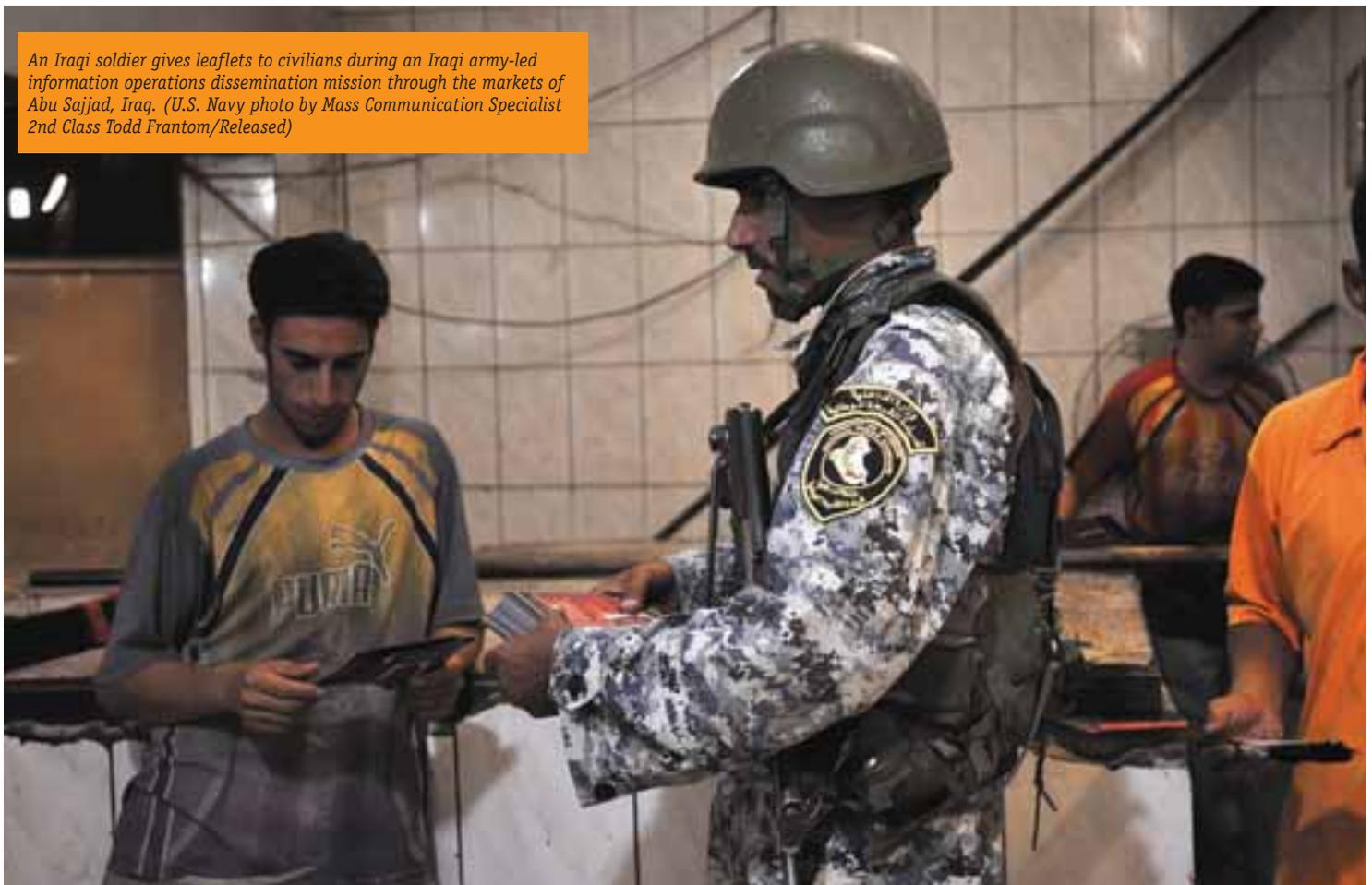
between education and propaganda, defining the former as the passing on of accepted skills, and the latter as the passing on of controversial attitudes. (11)

In the early days of the CPA, Ambassador Paul Bremer's well intentioned but not well-planned actions that abolished the Ministries of Defense and Information released thousands of Iraqis from service instead of making them friends and allies. Had he acted otherwise, the United States would have had indigenious ambassadors who possessed the requisite skills to win the Iraqi people to the cause of democracy. As an education process, shifting the focus of conversations can produce breakthroughs in performance and change. (12) Saying something new provides the opportunity to challenge, engage, and create – all the facets required by a culture of change. Since most of what individuals know about their world they gain from shared conversations rather than from

direct experience, what someone says, and to whom, makes a big difference. (13) These conversations are not simply reports of perceptions but a process that socially constructs the reality of the culture. (14) Unfortunately, the individuals within an environment do not perceive it as a product of their conversations. Instead, they believe their conversations present factual reports on an existing world. Changing the background conversations involves making individuals consciously aware that they are operating in a socially constructed context. (15) The good news is that the context is not limiting. Instead, it empowers individuals to create another one. When the background conversation shifts, the foundation on which individuals construct their understanding of the world shifts also, thereby opening new vistas in which to feel, think, and behave.

The reinvention process will not effect change as such. Instead, it is a consciously undertaken course of action

An Iraqi soldier gives leaflets to civilians during an Iraqi army-led information operations dissemination mission through the markets of Abu Sajjad, Iraq. (U.S. Navy photo by Mass Communication Specialist 2nd Class Todd Frantom/Released)



to undo what exists, and provides the opportunity to create something new. (16) Once this happens, a new context can emerge constituting a second order (17) or ontological change. (18) Learning to reassess their responsibility in generating and sustaining different background conversations allows individuals to choose a different response. Reclaiming responsibility provides new opportunities to create different responses to proposals for change. Admittedly, individuals will build the new background the same way they built the old one. However, what individuals say from this point forward matters more than ever because it is now more deliberate with a new recognition of building a reality that makes way for the new culture to gain a foothold. (19)

Strategies to change the mindset must include a communication strategy designed specifically to address the change. Individuals must fully comprehend both the necessity for the

change and how such a change will ultimately affect them. Simply stated, a good communication strategy is critical to a successful change. Combining several empirically founded principles provides a solid, effective communications strategy.

All the disciplines within Information Operations absolutely must interrelate, and at a minimum, tell the same story so that those who advocate change can attain the decisive operations the desired end state envisions. For example, Public Affairs and Public Diplomacy should not each go its own way. It is counterproductive. Instead, leaders advocating change should coordinate a well-grounded strategic communications strategy that harmonizes the strengths of Public Diplomacy, Public Affairs, and military Information Operations. In addition, the information environment extends beyond the disciplines of Information Operations. Collaborative efforts that draw on harmonized communications strategies from across the organizations comprising all instruments of national power will contribute to message redundancy – something that directly correlates to message retention. A harmonized communications strategy will go a long way toward ensuring successful change. Equally important is that along with understanding the target audience, leaders advocating change must possess a detailed understanding of friends, allies, and themselves.

Understanding the information environment requires achieving pervasive knowledge through a network-centric environment, and a shared understanding at all levels and among the disparate organizations. Agents for change achieve this through a process that transforms data into information and then distills the information into knowledge. Sharing that knowledge among all the players helps to gain the understanding necessary to craft a good communications strategy. While this requires combination of technology, training, and collaboration to aid this process, the human dimension remains the dominant consideration. Anticipatory understanding of the target audience's options should underpin the

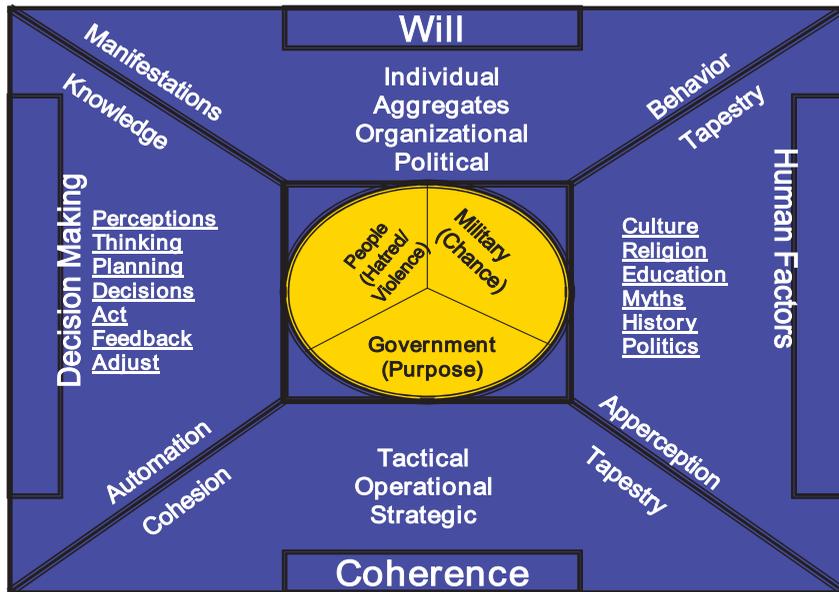
planning to counter those options unfavorable to successful change. Gaining this anticipatory understanding goes beyond identifying the target audiences resistance to change. It also requires gaining knowledge of the adversary's culture, support structure, and value system. This depth of understanding allows the use this knowledge to war game the possibilities, a practice that, in turn, results in a better understanding of the range of possibilities and the success of the anticipated change. This enhanced understanding provides reference points for setting up the network designed to detect key indicators of intentions and behavior as they relate to change. These indicators can help to anticipate likely options the target audience could choose. Understanding the environment will allow tailoring the capabilities of all instruments of national and multi-national power, and applying them holistically to achieve specific objectives, is the adaptable, provides an "option rich" solution in the information environment of the anticipated change.

A communication strategy that uses all the instruments of national power in addition to the traditional Information Operations disciplines enables leaders to focus on creating effects on the critical areas of mind, will, coherence, and human factors of the target audience.

The following quad chart shows potential areas where this approach can create desired results by applying appropriate persuasive or coercive pressure. These four areas shown in the quad chart frame thought processes and focus attention and efforts on what is important to a population. They provide a framework for designing actions most likely to create desired effects that attain stated objectives. An holistic communications strategy requires coherent actions at every level by harmonizing all instruments of national, multinational, governmental, and non-governmental powers with those of the various disciplines of Information Operations. (20)

Ensuring that the communications strategy remains appropriate, and that the actions or tasks achieve desired results, requires continuous assessment





and adaptation. Messages must remain relevant to the change, redundant, and consistent. The repetition of messages across several mediums increases individuals' memories of the message. (21) The ancient Romans used a similar strategy through a strict hierarchy and the rotation of officials to govern their vast empire. (22)

While the problems of reach will always exist in less technologically developed countries or in those with inefficient infrastructure, it is a mistake to discount the importance of the human factor. Due to its intimacy and emotional context, face-to-face communication produces a greater effectiveness than any other single medium. (23) While the consequence may result from its immediacy, the real measure of effectiveness is the interactive potential. (24) The two-way give and take of conversation encourages participation in the process, clarifies ambiguities, and increases the probability that both the sender and the receivers will interact appropriately. Additionally, communicators can use the immediate feedback to correct deficiencies in the communication process. (25) In particular, face-to-face communication in a group context provides a powerful dynamic in a successful change. It provides the communicator with an opportunity to capitalize on the different perspectives and interpretations that result from a complex message by providing timely explanations and clarifications relevant

to variations of understanding that can arise. (26)

Communications coming directly from those in authority carry both practical and symbolic weight. (27) The credibility of a message relates directly to the status of the source of that message, and individuals normally accord a higher status to the line hierarchy. (28) The voice of authority enhances the distribution of influence down through the hierarchy especially if it keeps each successively lower level fully informed and makes it a communications partner. (29) Of particular note, if leaders use opinion leaders, especially those active in the culture's affairs who are not part of the culture's hierarchy, it has a disproportionate effect on the opinions and attitudes of others. (30) Any communications plan should not discount the influence of the culture's "heroes" such as athletes or other well-recognized figures who are outside the realm of politics. Moreover, if the message is to have the "face" of the culture, the United States risks not attaining the goal by using U.S. soldiers and equipment for message distribution. Unfortunately, in the early days of OIF, the United States never used a local figure as a spokesperson. This was unfortunate especially since individuals retain personally relevant information better when the content relates directly with their home, work, or well-being – some which in this case, a westerner could not fully appreciate. In other words, individuals attend to and

retain information that directly affects them, (31) and culture matters!

Leaders attempting to effect change must have a good communications strategy reinforced by action – and a communications strategy is not always verbal. It bears repeating...what people believe is happening holds more importance than the events actually transpiring. A good example of this happened during the period immediately following the cessation of active combat. An infantry battalion commander, tasked to link up and meet with the Moslem cleric Sustani in al-Najaf, realized enroute that the people began reacting to his progress towards the mosque as a threat to a revered religious leader. Recognizing this, the Colonel immediately ordered his men to take a knee and point their weapons towards the ground in a non-threatening manner. While this action not only calmed the crowd but also gave the impression of respect to their leader, the colonel had the foresight to realize that pressing and accomplishing his mission would result in a needless confrontation between his soldiers and the people trying to protect al-Sustani. With cultural awareness in mind, he withdrew.

In the end, victory is not just about destroying targets but attaining the desired end state, a goal that is usually political. A successful communications strategy can serve as a catalyst by assisting the agents of change in attaining it. However, such a strategy must harmonize all instruments of national power with the disciplines of Information Operations and craft it to address the background conversations and cultural ramifications that affect the proposed end state.

Roberta-diane Perna, Ph. D. is an independent consultant based in Leesburg, Virginia. She is a highly regarded Strategic Communications Analyst with over ten years experience as a writer and editor both within DoD and the private sector. In addition to her professional writing, Dr. Perna is a member of the Army Science Board, an appointment she has held since 2000, and also serves as a member of the Senior Information Operations Advisory Council.

ENDNOTES

- 1) Remark attributed to GEN Martin Demsey and verified by the author with the General during the U S Army's Unified Quest 2005 war game.
- 2) Klein, S.M. (1996), "A management communication strategy for change", *Journal of Organizational Change Management*, Vol. 9 No. 2
- 3) Jones, M.O. (1991), "What if stories don't tally with the culture?", *Journal of Organizational Change Management*, Vol. 4, No. 3
- 4) Berger, P. and Luckmann, T (1966), *The Social Construction of Reality*, Anchor Books, New York, NY; Harre, R. (1990), *Social Being: A Theory for Social Psychology*, Littlefield, Adams & Co., Totwa, NJ; Heidegger, M. (1971), *On the Way to Language*, Harper Row, San Francisco, CA; Winograd, T. and Flores, F. (1987) *Understanding Computers and Cognition: A New Foundation for Design*, Addison-Wesley, Boston, MA
- 5) Jones, 1991
- 6) Schein, E. (1993), "On dialogue, culture, and organizational learning", *Organizational Dynamics*, Vol. 22 No. 2
- 7) Schrage, M. (1989), *No More Teams! Mastering the Dynamics of Creative Collaboration*, Currency Paperbacks, New York, NY
- 8) Ford, J.D., Ford, L.W. and McNamara, R T. (2001) "Resistance and the background conversations of change", *Journal of Organizational Change Management*, Vol. 15 No. 2
- 9) The retelling of these incidents came from two different sources. The first was one of the pilots who flew the first shipment of donkeys; and the other was a former CIA agent who was on the ground at the time.
- 10) Owen, H. (1991), "Learning As Transformation", In *Context: A quarterly of humane sustainable culture*, Winter
- 11) Perna, Rd.J. (1992), *Caesar Augustus, Benito Mussolini, and the Ara Pacis Augustae*, unpublished Master's thesis, Norwich University, Northfield, VT
- 12) Oakley, E. and Krug, D. (1991), *Enlightened Leadership: Getting to the Heart of Change*, Fireside, New York, NY; Scherr, A. (1989), "Managing for breakthroughs in productivity", *Human Resource Management*, Vol. 28 No. 1
- 13) Oakley and Krug, 1991
- 14) Ford, Ford, and McNamara, 2001
- 15) Marzano, R., Zaffron, S., Zraik, L., Robbins, S. and Yon, L. (1995), "A new paradigm for educational change", *Education*, Vol. 116, No. 2
- 16) Ford, Ford, and McNamara, 2001
- 17) Levy, A. and Merry, U. (1986), *Organizational Transformation: Approaches, Strategies, Theories*, Praeger, New York, NY
- 18) Marzano, et al, 1995
- 19) Ford, Ford, and McNamara, 2001
- 20) Much of this section comes from an unpublished white paper from Joint Forces Command, J-9 covering the important of global planning and regional execution of operations designed to achieved a specific end state.
- 21) Bachrach, S.B. and Aiken, M (1977), "Communication in administrative bureaucracies," *Academy of Management Journal*, Vol.20; Daft, R.I. and Lengel, R. H. (1984), "Information richness: a new approach to managerial information processing and organization design", in Staw, B. and Cummings, L.L. (Eds), *Research in Organizational Behavior*, Vol. 6, JAI Press, Greenwich, CT; Dansereau, F. and Markham, S.E. (1987), "Superior-subordinate communication: multiple levels of analysis", *Handbook of Organizational Communication: An Interdisciplinary Perspective*, Sage, Beverly Hills, CA
- 22) Perna, 1994
- 23) D'Aprix, R. (1982), "The Oldest and Best Way to Communicate with Employees," *Harvard Business Review*, September-October; Jablin, F.M. (1979), "Superior-subordinate communications: the state of the art", *Psychological Bulletin*, Vol. 86; Jablin, F.M. (1982), "Formal structural characteristics of organizations and superior-subordinate communication", *Human Communication Research*, Vol. 8
- 24) Gioia, D.A. and Sims, H.P. (1986), "Cognitive-behavior connections: attribution and verbal behavior in leader-subordinate interactions", *Organizational Behavior and Human Decision Process*, Vol. 37
- 25) O'Connor, V. (1990), "Building internal communications (two-way) management-employee communications", *Public Relations Journal*, Vol. 46, June
- 26) Weick, K. E. (1987), "Theorizing about organizational communication", *Handbook of Organizational Communication: An Interdisciplinary Perspective*, Sage, Beverly Hills, CA
- 27) Klein et al, 1974; Snyder, R.A. and Morris, J.H. (1984), "Organizational communication and performance", *Journal of Applied Psychology*, Vol. 69; Young, M. and Post, J.E. (1993), "Managing to communicate, communicating to manage: how leading companies communicate with employees", *Organizational Dynamics*, Vol. 22 No. 1, Summer
- 28) Kiesler, C.A. and Mirson, P.A. (1975), "Attitudes and Opinions", in Rosenzweig, M.R. and Porter, L.W.(Eds), *Annual Review of Psychology*, Vol. 26, Annual Reviews, Palo Alto, CA
- 29) Daft, R.I. and Huber, G.P. (1986), "How organizations learn: a communication framework", in Bachrach, S. and Tommaso, N. (Eds), *Research in Sociology of Organizations*, Vol. 5, JAI Press, Greenwich, CT Katz, D. and Kahn, R. I. (1978), *The Social Psychology of Organizations*, 2nd ed., Wiley, New York, NY;
- 30) Cialdini, R.B., Petty, R.E. and Cacioppo, J.T. (1981), "Attitude and attitude change", *Annual Review of Psychology*, Vol. 32
- 31) Pincus, J.D. (1986), "Communication satisfaction, job satisfaction, and job performance", *Human Communication Research*, Vol. 12



Talking the Talk: Why Warfighters Don't Understand

By Dennis M. Murphy

Back in 2006 Army Colonel Rob Baker published an article in *Military Review* entitled "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations." (1) Any information practitioner who reads this excellent piece will immediately latch on to the fact that Baker's brigade was not really conducting information operations (IO), but in fact was using strategic communication as its primary enabler. But wait...can you conduct strategic communication at the tactical level? And if, from the lofty ivory tower of academia or the hallowed halls of service doctrine organizations you told Baker that he was not conducting IO would he really

care about your nuanced interpretation? In other words, does it really matter?

The value of information as a military enabler has always been a factor in warfare. But the rapid evolution of the information environment has caused information to rise in importance to where it is effectively used by adversaries as an asymmetric weapon of choice. The improvised explosive device may be a tactical kinetic weapon, but it is, more importantly, a strategic information weapon when the detonator is paired with a videographer. In an attempt to both counter this information-savvy enemy, as well as exploit that same environment to achieve military objectives, the United States military has struggled to establish definitions and

doctrine concurrent with applying those nascent concepts in combat. The result is a developmental process that has muddied the waters outside the very narrow subset of military service members and academicians who claim some form of "information" as their primary specialty; ironic, given the communications and marketing expertise espoused by some of those very same practitioners.

A review of current military and U.S. government information-related lexicon and definitions points out a very obvious flaw: this stuff is confusing... and in some cases, self-defeating. It's time for a doctrinal pause to allow a clean slate review of information operations, strategic communication and, yes, cyberspace opera-

U.S. Army Soldiers from 350th Tactical Psychological Operations, 10th Mountain Division conduct a leaflet drop in several villages in Rashaad Valley in the Kirkuk province of Iraq. (U.S. Air Force photo by Staff Sgt. Samuel Bendet/Released)

tions. Such a review may find that simpler is better.

WORDS (AND DEFINITIONS) MATTER

Information Operations

Any detailed review of current information-related terminology and definitions used by the United States government should be considered from the perspective of a warfighting commander. Remember, if information is an enabler that supports the achievement of a military objective, then the warfighter needs to know where it fits in his plan and how to exploit it. In other words, the warfighter needs to “own” the information capabilities... and in order to own it, he must understand it. Consider information operations.

The first question one may ask is whether information *operations* (emphasis added) are separate operations in and of themselves, or part of the greater military operation. To some, this may seem trivial and perhaps inconsequential, but to the uninitiated, the lexicon itself defines the

definition can provide clarification... so here goes. Information operations is:

The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations (PSYOP), military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own. (3)

Unfortunately, the reader’s focus tends to move directly to the listed core capabilities within the definition at the expense of the rest of the verbiage. Consequently, IO becomes PSYOP or IO is computer network operations in the mind of the warfighter. (4) This focus on capabilities further obfuscates the definition when civilians, often in the mainstream media, take the next logical leap that PSYOP equals propaganda which in turn equals lies. (5) And since IO is perceived to be PSYOP, and the definition of IO includes deception...well, you get the obvious (albeit incorrect) conclusion.

Not only is the listing of the capabilities an issue, but the mere number

PSYOP and electronic warfare if those capabilities are synergistically integrated to achieve the appropriate effect against the appropriate target audience. That desired effect is to influence disrupt, corrupt or usurp. Its target audience is adversarial human and automated decision-making. Given this target audience it’s evident that IO can impact the cognitive, informational and/or physical dimensions of the information environment. By explicitly excluding a laundry list of capabilities, the definition is no longer self-limiting since the tools available are now constrained only by the imagination of the commander and his staff. While it may not be about everything you do, it certainly can be about anything you *can* do to achieve the desired information effects in support of the military operation, to include physical attack, i.e. actions.

Strategic Communication

If you think IO is confusing outside of a small circle of information experts, consider strategic communication. Strategic communication is an emergent concept with several definitions floating about, no doctrinal base and a lexicon that fails completely to convey the desired understanding. No small wonder that U.S. Southern Command’s Admiral James Stavridis recently paraphrased World War II’s great naval commander and strategist Ernest King, stating “I don’t know what the hell this [strategic communication] is that Marshall is always talking about, but I want some of it.” (6) In this case it may be more beneficial to first look at the definition and then analyze the term itself. The 2006 Quadrennial Defense Review roadmap on strategic communication defines it as:

Focused USG (United States Government) processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs and actions synchronized with other elements of national power. (7)

The roadmap goes on to list the primary supporting capabilities of strategic

Information Operations

concept. Consequently, the commander, who probably hasn’t read IO doctrine, and who may have received, at most, a three hour block of instruction three years ago in a senior service college, is left to his own devices. And so anecdotal evidence exists of commanders and operations officers directing IO staffs to “sprinkle some of that IO stuff” on the already completed military plan. Understandable perhaps, since if information operations are separate operations, then it’s pretty easy to push the IO staff out of the core planning group to the side trailer or tent. By the way, the U.S. military’s Joint Publication 3-13 clearly states that IO is in support of the overarching joint operation and should be fully integrated into the planning process. (2)

If the term “information operations” is an issue in and of itself, perhaps the defi-

of them detracts from an understanding of the concept. Since there are five core capabilities and eight additional supporting and related capabilities, to include physical attack, the perception is that IO is either everything you do (more on this later) or simply so complex that it must be left to the expert staff section to handle.

But remove the reference to capabilities from the definition and the clarification is telling. Information operations is:

The integrated employment of ... capabilities ... to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own.

Now it should become obvious that IO is an integrating function, first and foremost, and not a separate operation or a separate single capability. In other words IO can’t be PSYOP alone, but it can be



U.S. Army 1st Lt. Nicholas Lacroix works on signs for the Information Operations section of the 3rd Brigade Combat Team, 4th Infantry Division, at Forward Operating Base War Eagle, Iraq. (U.S. Army photo by Spc. Joshua E. Powell/Released)

communication as public affairs, aspects of information operations (principally psychological operations), military diplomacy, defense support to public diplomacy, and visual Information. (8) Once again, the listing of capabilities within the roadmap muddies the waters for the warfighting commander and in fact limits the perceived means available to *communications* (emphasis intentionally added) based activities and so reinforces the lexicon of the term itself. However, parsing the definition to its essential parts again provides clarity:

Focused USG processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives....

So, strategic communication is a process of understanding and engaging. This implies a two way conversation. The desired effect is to create, strengthen and preserve conditions favorable to national interests and objectives. The target audience is intentionally large and vague, i.e. simply "key audiences." Strategic communication focuses on the cognitive dimension of the information environment. Removing the capabilities listing once

again removes some of the mystery from the term. (9)

Simplifying definitions also allows one to easily compare strategic communication to IO. Strategic communication is the more broadly overarching concept targeting *key audiences* and focusing on the cognitive dimension of the information environment. IO as an integrating function, on the other hand, more specifically targets an *adversary's decision making capability* which may be in the cognitive, informational and/or physical dimensions of the information environment. Considering the targets and effects described above, it should be clear that both strategic communication and IO can be employed at all levels of warfare (tactical, operational, theater strategic and national strategic). Tactical commanders routinely employ strategic communication in Iraq and Afghanistan today based on their interactions with key audiences in their area of responsibility to a potential strategic end. On the other end of the scale, IO could certainly be employed strategically as part of a Phase 0 shaping operation or a Phase 1 deterrent operation against a potential adversary's decision-making capability.

JUST PLAIN "INFORMATION": RECOMMENDATIONS AND CONCLUSION

The Joint Staff recently published the definition of cyberspace operations stating that it "should encompass computer network operations and activities to operate and defend the Global Information Grid." (10)

Eschewing further analysis, you can see where this is going. With the rapid evolution of the information environment, "cyberspace operations" is the latest example of inventing terminology and definitions on the fly, often overlapping with current doctrine and lexicon. (You'll note that "computer network operations" is a core capability in the definition of IO.) Additionally, as the terms IO, strategic communication and cyberspace operations gain greater usage, confusion increases while codification proceeds, often as separate doctrine development for each concept. For instance, U.S. Joint Forces Command recently published a "pre-doctrinal" publication on strategic communication. (11) No doubt, someone, somewhere on the Joint Staff is working on the embryonic beginnings of cyberspace operations doctrine.

Given the above analysis, the U.S. military would be much better off pausing to review current publications and then consolidate and simplify what is currently confusing, overlapping and disparate guidance. The result should be an overarching joint doctrinal effort that both considers existing concepts and focuses on an understanding of information as a warfighting enabler. Entitle it (again, simply) "Information." The review may find that it is totally appropriate to include information operations, strategic communication and cyberspace operations *concepts* (emphasis added). But in doing so the reviewers should specifically consider changing the lexicon of the terms where appropriate and parsing the existing definitions to their simplest essentials. Capabilities can be addressed within this proposed publication, but not within the definitions themselves. In fact, the definitions should focus on the desired effects and the targeted audiences. Given the rapid acceptance of strategic communication and the nascent emergence of cyberspace operations as warfighting constructs, no doubt a new concept is just

around the corner. A doctrinal approach to information writ large will allow the overarching focus and understanding that warfighters need in order to “own” the enablers, while providing the flexibility to incorporate whatever new concept may appear on the horizon.

There are glimmers of hope in this regard. The Army, in its overarching field manual “Operations” (FM 3-0) makes little reference to IO but instead adopts the term “Information.” Additionally, joint doctrine writers are in the process of revising Joint Publication 3-13 (“Information Operations”). The final coordination program directive proposes a chapter on information operations’ relationships to other concepts to include strategic communication and cyberspace operations, perhaps in an attempt to gain clarification. But that same directive warns against a change in terminology stating that “new or modified...terms should only be used when such terms are essential to the development and understanding of proposed doctrine.” (12) The Joint Staff would be well served to consider the revision of Joint Publication 3-13 as an opportunity for a doctrinal pause. The time is ripe for a clean slate review of the current terminology and definitions and to provide an overarching doctrinal manual that strikes a balance between providing an understandable baseline as well as a practical implementing blueprint. In the rapidly changing information environment sometimes simpler is better.

Dennis M. Murphy is a Professor of Information Operations and Information in Warfare at the US Army War College. Professor Murphy teaches information operations and strategic communication electives and conducts workshops on the information element of power.

ENDNOTES

1) Baker makes a compelling case for the importance of information effects as a main effort while a brigade commander in Iraq. He refers to his actions as “information operations” but a close read reveals that his unit was primarily conducting strategic communication. See “The Decisive Effort: A Brigade Combat Team Commander’s Perspective on Infor-

mation Operations” in the May-June 2006 issue of *Military Review*.

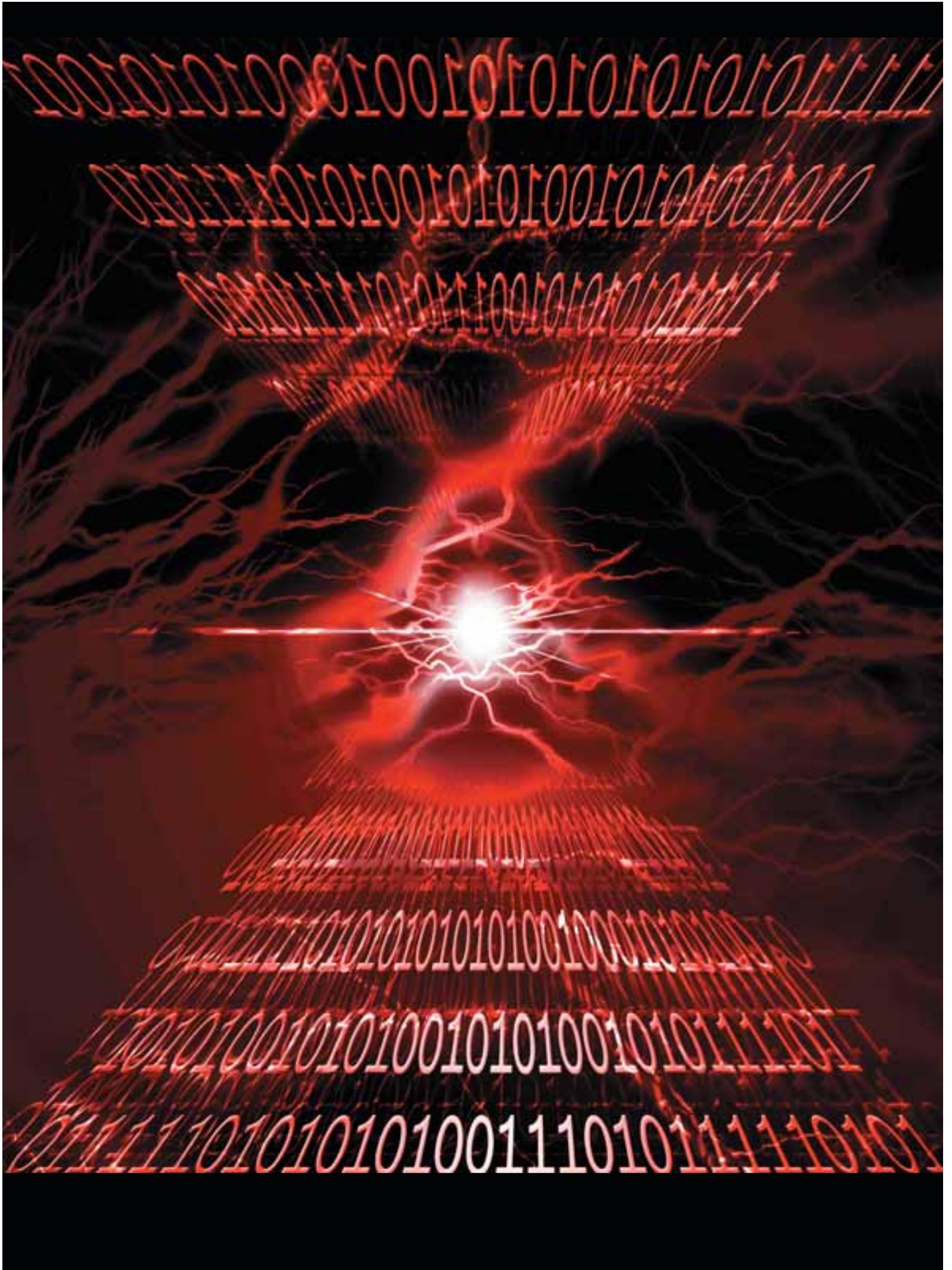
- 2) Chairman of the Joint Chiefs of Staff, “Joint Publication 3-13, Information Operations,” 13 February 2006, pp. ix, xii.
- 3) Ibid, p. I-1.
- 4) It’s worth noting that the definition of IO includes core capabilities for programmatic reasons, i.e. the listed capabilities have funding streams. Unfortunately, there are numerous examples of senior military leaders using the term “IO” when referring to a single, specific capability thus reinforcing the confusion.
- 5) The long history that, at least in perception, equates psychological operations to propaganda is outlined in “Propaganda: Can a Word Decide a War” by the author and James F. White, in the autumn, 2007 issue of *Parameters*.
- 6) James G. Stavridis, “Strategic Communication and National Security,” *Joint Force Quarterly*, 3rd Quarter, 2007, p. 4.
- 7) U.S. Department of Defense, “QDR Execution Roadmap for Strategic Communication,” September 2006, p. 3. The Deputy

Assistant Secretary of Defense for Joint Communication states that this is the only Department of Defense definition of strategic communication that should be in use.

- 8) Ibid, p 2.
- 9) The office of the Assistant Secretary of Defense for Public Affairs recently published “Principles of Strategic Communication.” Interestingly, and apropos to the complexity of the roadmap definition, this product simply refers to strategic communication as the orchestration and/or synchronization of words, images and actions to achieve a desired effect.
- 10) Vice Chairman of the Joint Chiefs of Staff, “Definition of Cyberspace Operations,” memorandum for the Deputy Secretary of Defense, September 29, 2008.
- 11) United States Joint Forces Command, “Commander’s Handbook for Strategic Communication,” September 1, 2008, p. i.
- 12) The Joint Staff, “Final Coordination (FC) Program Directive for Joint Publication 3-13, *Information Operations*,” received December 2008.



U.S. Soldiers from 315th Psychological Operations (PSYOP) Company and 2nd platoon Alpha Company 1st Battalion 6th Infantry Regiment, 1st Armored Division, Multi-National Division-Baghdad, and Iraqi soldiers patrol through The Peoples Market outside of Homidia, Iraq. (U.S. Army photo by Spc. Joshua E. Powell/Released)



POLITICAL AND TECHNICAL ROADBLOCKS TO CYBER ATTACK ATTRIBUTION

By Jeff Wozniak and Prof. Samuel Liles, Purdue University Calumet

Can novel approaches to using current techniques in the realm of network forensics be successfully applied to remedy the problem of attribution in cyber warfare? If not, what elements, technological or otherwise, must be further developed to combat the problem?

According to Susan W. Brenner:

“The task of identifying those who are responsible for an attack has been, and will remain, a constant. As we will see, identification of the attacker can play an integral role in ascertaining the nature of an attack; and ascertaining the nature of an attack is usually the first step in formulating a response to an attack, of whatever type. (2007)”

Obviously, if one is going to take countermeasures against an act of war or terrorism, the identity of the attacker must be known. Unfortunately, due to the topology of the Internet, the ability to reliably identify an attacker with any degree of certainty is difficult within the realm of cyber warfare and cyber terrorism. For these reasons, the ability to determine the true source of an attack, not just the physical location that launched the attack, is of great importance to any sort of response or counter-defense to a cyber attack.

This paper will examine whether or not the current capabilities, as they are currently applied or otherwise, of network forensics is capable of reliably attributing attacks to individuals, groups, or states. It will look at the techniques and tools used in traditional, non-political, or state-sponsored cases of cybercrime and examine the similarities and differences in ap-

plying these techniques to the different cases. This paper will also look at the potential flaws or shortcomings of these techniques as they relate to the attribution of acts of cyberwar rather than acts of cybercrime.

After these techniques are analyzed, their overall capability as they are currently exist will be examined to determine if the tools are adequate for the task of cyber warfare attribution. If the tools are found to be lacking, depending on the degree or areas in which the tools are found to be lacking, this paper will either examine non-traditional adaptations of current tools for this purpose and additional capabilities necessary for this task. Geopolitical considerations will also be considered in the development of these tools since they do not work in a vacuum and their results usually rely on international cooperation to be successful beyond a reasonable doubt.

In the very recent past, there have been two high profile incidents of cyber warfare in the media. Specifically, these events are the attacks that disabled various Estonian government and business websites and the attacks targeting similar Georgian websites before and during the Russian incursion into South Ossetia (Gee, 2008). Both of these incidents involved denial of service attacks against, and the defacement of, government and commerce sites in the two countries. In May of 2007, several Estonian websites were targeted by attacks aimed at overwhelming the connections providing service to websites, thereby preventing legitimate users from accessing them (Traynor , 2007). As early as July of 2008, almost two months before the beginning of its kinetic conflict with Russia, websites serving the Asian nation of Georgia began to experience similar denial of service attacks and defacement (Markoff, 2008).

In the case of Estonia, the attacks began after a Soviet war memorial was removed from its capital city, Tallinn, in April of 2007. The attackers targeted websites of government agencies, financial institutions, and news organizations. While the individual sources of the distributed attack came from throughout the world, cyber warfare and computer forensics experts believe that the attacks were perpetrated from within Russia; however, the anonymous nature of the Internet and the fact that users' computers could participate in such an attack without their knowledge make difficult the task of identifying who actually instigated the attack (Traynor, 2007).

In the case of the South Ossetian conflict, Georgian websites began experiencing low level distributed denial of service attacks in mid-July. When strained relations with Russia finally boiled over in early August, Georgian Internet services were crippled by an onslaught of attacks. As with the Estonian incident, despite attacks from multiple sources, Russian entities were determined to be behind the attack; however, as before, it was impossible to determine whether or not the attackers were agents of the government, parties acting with implicit government consent, or genuinely rogue groups acting out of national pride (Markoff, 2008). In both cases, the international media jumped on the digital attacks, aimed not at individuals but at sovereign entities, and declared them to be acts of cyberwar. While the attacks against Georgia coincided with actual physical violence between two nations, neither case demonstrated the use of digital attacks as part of a broader strategy or tactical objective. The attacks were of the same caliber and type as attacks commonly perpetrated against commercial websites all over the world (Manimaran & Muthuprasanna, 2008).

Additionally, the attacks could not, with any degree of certainty, be attributed to any specific entity, let alone a sovereign nation. These two facts immediately throw into question the media's declaration that the acts were acts of war and not simply acts of cybercrime or cyber terrorism. This demonstrates a very basic shortcoming in current perceptions of the task of attribution in terms of cyber conflict, namely the lack of legal or even generally agreed upon definitions of what constitutes cybercrime, cyber terrorism, and cyber warfare.

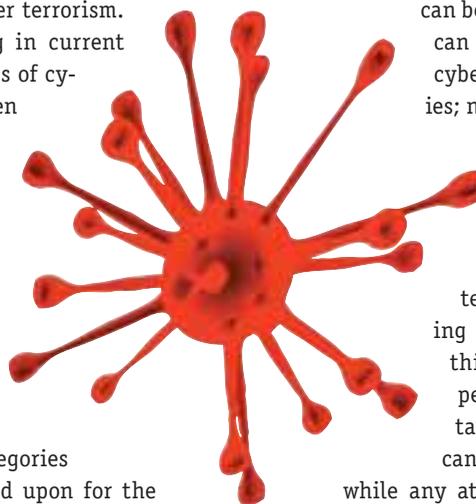
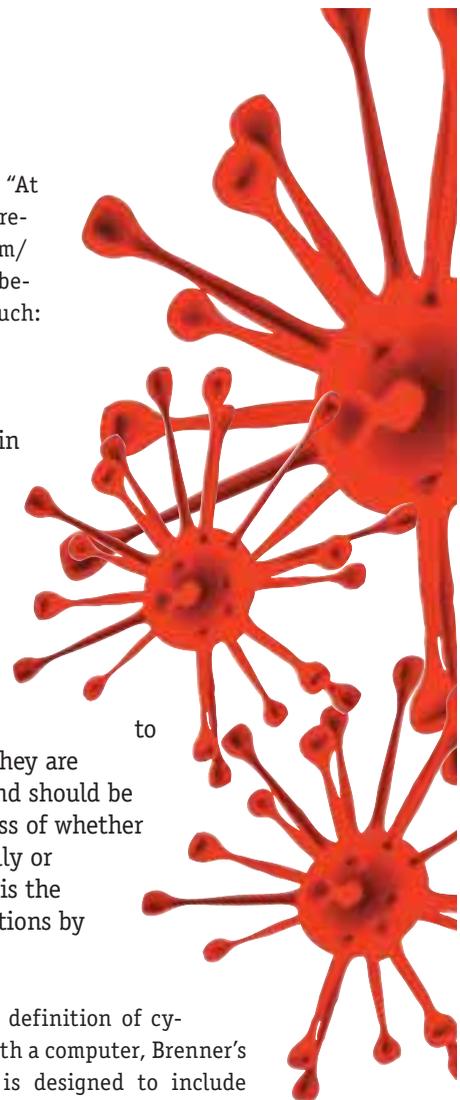
While, on its face, the task of clearly defining categories of digital attacks may seem to be purely academic in the face of overtly illegal acts, these distinctions become important when they must be discussed in terms of an international legal framework pertaining to the conduct of wars. For this reason, working definitions of the three categories mentioned above will be listed and expanded upon for the simple purpose of distinction within this paper, rather than proposed as a sort of "official" definition.

In Susan Brenner's article, "At light speed: Attribution and response to cybercrime/terrorism/warfare," she differentiates between the three categories as such:

"Cybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order.... The same should be true for [cyber] terrorism. Insofar as [cyber]terrorist acts are designed to undermine a society's ability to maintain internal order, they are indistinguishable from, and should be treated as, crime regardless of whether they are perpetrated locally or remotely.... Cyberwarfare is the conduct of military operations by virtual means. (2007)"

Rather than the traditional definition of cybercrime as crime committed with a computer, Brenner's addendum to that definition is designed to include purely digital crimes with no parallel in the real world, such as denial of service attacks. The other two definitions are fairly straightforward, branding cyber terrorism as a type of cybercrime and cyber warfare as military acts, whether or not those acts can be included as part of the latter two categories.

Based on these definitions, a few initial conclusions can be drawn. Specifically, differentiations can be made solely on the grounds that cyber warfare is conducted by militaries; namely that, although cyber criminals and terrorists could theoretically be just as organized and capable as a cyber military, the fact that militaries are agents of a nation precludes a non-state actor from technically being capable of perpetrating acts of cyber warfare. Essentially, this means that any digital attack, from petty vandalism to well-organized attacks, committed by a non-state entity cannot be considered an act of cyberwar, while any attack committed by a military, from petty vandalism to well-organized attacks should be covered under the umbrella of cyber warfare.





This distinction has certain implications for the task of attribution in terms of cyber warfare. First, and most obviously, it distinguishes between what is and is not considered an act of cyberwar ... in theory. Again, this seems purely academic in the face of attacks wherein the culpable party is so difficult to identify, but these distinctions come into play in cases where attribution is successful. Once a responsible party is identified, the distinction between state and non-state entities will come to determine whether an act is covered under the legal framework for crime or for war.

Defining and categorizing what is or is not an act of cyber crime/warfare/terrorism is moot, however, if one remains unable to determine the party responsible for an attack. For this reason, it is important to examine technical underpinnings of attack attribution. This includes the mechanisms for discerning the origin of attacks, modeling and quantifying attacks, and identifying attackers who attempt to conceal their affiliations. Accordingly, the technical capabilities and limitations of current technology in terms of those three areas will be examined next.

Traditionally, techniques for deciphering the origin of a cyber attack entail reconstructing and recreating a chain of events for the attack using digital forensic methods such as log inspection and reverse engineering (Enfinger et al., 2008). Such techniques are based on common digital forensic principles for examining attacked systems and using information on those systems to determine information about the attack that was perpetrated upon it.

In the case of remote, network-based attacks, comprising the majority of attacks classified by the media as cyber warfare, a large part of the investigation process revolves around examining the traffic logs of network devices. This includes network routers, firewalls, servers, and any other device responsible for moving traffic from the outside world to the device or network that was targeted. These logs provide information about what type of traffic was being generated at the time of the attack, the amount of traffic traversing the system during the attack, and, to a limited extent, the source and destination of packets entering and leaving the network during the attack (Enfinger et al., 2008).

The information contained in these logs provides a limited, static view of events that occurred on the network after an attack has taken place. This information can be used to gain insight into certain aspects of the attack such as identifying

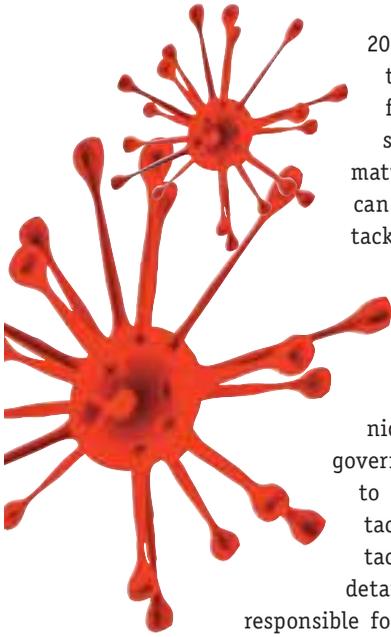
patterns, establishing a sequence of events, and generally providing a broad description of activity on the victim network (Enfinger et al., 2008). There also exist products for collecting the information contained within packets for further examination and reconstruction, but aside from the level of detail provided by these solutions, the basic principles and capabilities are essentially the same (Bokkeken et al., 2003). Unfortunately, this method of investigation is passive and occurs once an attack has ended; that is, log inspection and reverse engineering can only determine as much information about the origin of an attack as is provided to it from the outside world. Specifically, this means that such an investigation relies on the attacker to slip up and provide information about their origin and is incapable of actively seeking out and collecting information. This is akin to tracking the Unabomber without the ability to see past a phony return address. Any meaningful investigation, where simple methods of obfuscation are readily available, necessarily relies on the ability to reach out and pull more in-depth information about an attack. For this reason, more advanced and active techniques have been developed for modeling attacks in order to perform more accurate attack attribution.

Attack traceback is generally applied to distributed denial of service attacks and relies on mechanisms for marking and monitoring packets or modeling traffic patterns in order to gain insight into the origin of an attack. According to Manimaran & Muthuprasanna, "The three fundamental operations underlying any attack traceback mechanism are attack tree construction, attack path frequency detection, and packet to path association," (2008). Specifically, this entails developing a tree topology of the paths traversed by packets between the victim and sources of attack, determining the relative amount of traffic generated on each path within the tree, and the ability to track a packet through the tree to its source (Manimaran & Muthuprasanna, 2008).

The ultimate goal is to perform the functions above using distributed methods to gather and monitoring traffic, either by examining the relative frequency and paths taken by offending packets, or by actively marking packets traveling through the network, making them easily identifiable (Al-Duwairi & Daniels, 2004; Tang & Daniels, 2005). Unfortunately, this methodology possesses inherent limitations.

The prevalence of large groups of compromised computers in the hands of attackers, capable of generating enormous amounts of traffic without the knowledge of the computers' owners, means that techniques focused on identifying traffic sources do not necessarily meet the needs of attribution in the context of cyber warfare (Achido & Swartz,





2008). These methods are comparable to identifying the source of gunfire, but not the shooter or even the shooter's motivation. To complicate matters further, even if a specific botnet can be identified as responsible for attack, botnet operators have been known to rent out their services, further obfuscating the true instigator of the attack (Shachtman, N., 2008).

Consequently, while these techniques may prove useful for assisting government and other networks subject to a distributed denial of service attack in cutting off the source of an attack, the information provided is not detailed enough to determine the entity responsible for an attack. First, assuming a perfect scenario where every machine involved could be positively identified, these methods disclose only the machine, not the operator. This forces attribution efforts to reach beyond the digital realm in order to determine the physical entity with access to the offending piece of equipment. Second, even assuming that this method could positively identify the operator of the machine, knowing the identity of the user on the other end does not show that that user was responsible for, or even aware of the attack carried out by their hardware (Achoido & Swartz, 2008). Finally, even if the individual responsible for launching the attack could be identified, even further means would be required to determine whether or not they were acting with the explicit consent of a national government.

The general consequence of these limitations is that, while they may provide a certain degree of information pertaining to the origin of an attack, they do not provide enough resolution or nuance to be totally successful in the context of cyber warfare. Specifically, the purely technical approaches currently available are incapable of reaching beyond the digital realm and identifying the real world entity responsible for conceptualizing and executing an attack. Given this lack of certainty, especially in the context of actions that could elicit a response proportional to an act of war, methods extending beyond the cyberworld become necessary for successfully attributing acts that could constitute cyber warfare.

Consequently, the discussion of cyber warfare attribution moves from the digital world to the legal world. This includes aspects related to international law, conventions for conducting war, and the political considerations involved with events that place take across multiple boundaries. All three areas play a crucial role in determining whether or not achieving positive identification is a plausible expectation.

Currently, there is no uniform international framework for dealing with international acts of cybercrime, let alone

acts of cyber warfare. Dan Morrill of CityUniversity of Seattle points out that conducting cyber attacks, against individuals or organizations, is legal in some countries and illegal in others (2006). Without international agreements, possibilities are open for perpetrators to perpetrate attacks from countries where such activity is legal. Morrill goes on to note that, even in countries where hacking is illegal, lesser attacks not targeting large or governmental institutions go mostly unprosecuted (2006). While chances are good that an act of cyber warfare is likely to be of a scale that is readily noticeable or targeting a government organization and thus likely to be prosecuted, this inconsistency serves to demonstrate that even in the presence of laws concerning cyber attacks, enforcement is not uniform. (That is not to say that cyber warfare could not easily involve small, covert, and directed attacks, only that those incidents have lower potential for garnering the type of attention mentioned or even being noticed in the first place (Neil, M., 2007).)

As noted above, there is currently no international legal framework that deals specifically with cyber attacks. Current prosecutions and investigations, of cyber attacks rely on the legal framework designed for dealing with traditional crime (Strohm, C., 2008). Current prosecutions of attacks across international borders rely on cooperation between nations in order to gather evidence outside of a country's jurisdiction, and even once a perpetrator has been identified, their nation of residence has final say over whether or not they will be extradited (BBC, 2008). Even beyond the context of attacks carried out by individuals, this lack of enforcement mechanisms for aiding victim nations investigating attacks demonstrates the current weaknesses in international law pertaining to cyber warfare. The problem is compounded when nations are attacked from or through unfriendly nations, unwilling to cooperate, to any degree, with the victim nation.

While the international laws pertaining to cybercrime remain inconsistent, most countries abide by certain rules concerning the conduct of war; however, despite the fact that "nearly all authorities agree that international law does apply to cyber-warfare," the identity of the responsible party is required before a determination can be made as to whether or not an attack is an act of cyber warfare or simply a cybercrime (Rowe, N.C., 2007). An important aspect of the international guidelines for conducting war, and one that is key to the concept of attribution, is the prohibition of perfidy in conflict. For example, according to Hague IV 1907, Article 23, "it is especially forbidden ... to make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy..." This provision is designed to protect civilians and non-combatants from collateral damage by combatants unable to easily identify other combatants. Essentially, this principle of self-attribution renders moot, in terms of physical conflict, the various issues pertaining to attribution in cyber terrain (Rowe, N.C., 2007).



Based on all of the information presented above, one can see that there are obvious gaps in the technological and political capabilities related to attributing a cyber attack. It is also obvious that neither approach is sufficient, on its own, for the task. Consequently, one should examine possible combinations of the two areas, as they currently exist, for potential solutions to the problem.

In their paper "Attack patterns: A new forensic and design tool," Fernandez et al. propose that attacks are subject to being viewed as patterns (2007). Specifically, they state that "Many problems occur in similar ways in different contexts or environments. Generic solutions to these problems can be expressed as patterns," (Fernandez et al. 2007). According to their paper, this approach provides the ability to examine attacks, quantify them in standardized terms, and extrapolate this information in such a way that it can be used to increase the security designed into systems and provide the ability to quickly reverse engineer an attack if it occurs (Fernandez, et al., 2007). This approach provides many benefits in terms of cyber warfare beyond the two abilities described above.

First, as stated above, such attack patterns can be used to more quickly reverse engineer an attack and provide insight into an attacker's steps. Combined with the traceback capabilities already described, this provides a more powerful tool for winnowing the pool of potential attackers. By understanding the process an attacker would have to utilize in identifying and exploiting a vulnerability, groups of attackers can be eliminated based on capabilities and opportunity. If the generation of attack patterns is done diligently for a given system, one can quickly and easily identify the circumstances of a given attack and determine what was required for it to be successful.

Beyond the possibilities for attribution and prevention, the idea of attack patterns described could be used legally. Specifically, if ever an international legal framework were implemented for dealing with cyber attacks, a standardized and quantifiable description of attacks is almost certainly necessary for presenting evidence and descriptions of attacks within that framework. The template presented in the paper covers a great deal of information about an attack without also being overly broad. In a legal context, the template presented provides an effective and succinct format for identifying an attack's nature, the conditions required to execute it, what it affects, its consequences, and potential measures for preventing the attack (Fernandez et al., 2007). Such a standardized and dense description of an attack is almost a guaranteed necessity for any body that could ever hope to adequately deal with the broad topic of cybercrime.

Another alternative for supplementing existing technol-

ogies relies on the concept of open source information. The Intelfusion project is "a pure grass roots effort using only open source data pulled from the Web" that aims to successfully attribute the origin of the cyber attacks against Georgia during the South Ossetian conflict (Intelfusion, 2008). The project presents an innovative approach to attribution in that it relies neither on government intelligence sources nor professional intelligence operatives. Instead, it seeks to utilize publicly available information for the task of attribution. This information could include information regarding specific IP addresses involved in the attack based on publicly-available provider logs or even boasts made by particular groups claiming responsibility for attacks.

The Intelfusion project provides a novel look at the problem of attribution that could be used to reinforce current technical options. For instance, large groups of volunteer users can quickly search the vast resources of the Internet, turning up possible information about an attack. From this information, certain conclusions could be made regarding the source of the attack. In the case of parties actively claiming responsibility for an attack, if the boasts can be verified as true, attribution takes care of itself. However, despite popular belief, everything read on the Internet is not always true, making such investigations the equivalent of digital hearsay. For this reason, information from a technical investigation can be compared to and supplemented by information from a "social" investigation in order to gain a more complete understanding of the attack and the parties involved. If scientific methods can be used to verify hunches or other non-scientific information generated by open source volunteers, slower technical methods can be more efficiently guided by collective reasoning.

Unfortunately, even these solutions are lacking, demonstrating the need for future improvements in capabilities both technically and politically. As part of a technical solution to provide more precise attack attribution, governments and service providers could look at technology allowing for packet tracebacks to be conducted with the coordinated support of higher-level devices within the architecture of the Internet. By allowing devices with high-level views of the network to participate in tracebacks, much more accurate information can be derived, including the ability to determine the source of smaller, targeted attacks that do not generate nearly as much traffic as distributed denial of service attacks. Unfortunately, this solution poses serious privacy issues which would have to be addressed politically and legally.

According to N.C. Rowe, nations participating in cyber warfare could opt to voluntarily identify themselves using a number mechanisms that are described in his article. While seemingly counter-intuitive, nations have certain incentives to clearly identify themselves in cases of cyberwar. For instance, the ability to discern between



state entities helps to prevent civilian targets from being attacked. Self-identification also reduces the likelihood that a nation, with only murky evidence as in the case of the Russian "cyberwars," will be blamed for attacks carried out by rogues agents (Rowe, N.C., 2007).

In the political/legal arena, some sort of international framework, legally-binding or otherwise, is almost an absolute requirement for any meaningful steps toward true cyber warfare attribution. Without mechanisms for creating and enforcing laws or agreements, non-cooperation between diplomatically tense nations makes the entire concept a non-starter. As long as an entity can hide behind the figurative firewall of a nation that will absolutely not cooperate with another, the chances of somehow determining, with any definite accuracy, the true identity and nature of an attacker, are practically non-existent. For this reason, some mechanism must be in place to force compliance within the confines of acceptable cyberwar, or otherwise castigate non-cooperative nations.

Similarly, a general set of rules for engagement in cyber warfare should be discussed and adopted by participating nations. While not absolutely necessary, such guidelines would provide nations with an idea of what types of attacks are acceptable and which are not. They will also aid in the identification of non-state participants acting outside the rules of engagement. Similarly, they can help to establish what constitutes a cyber war crime, paving the way for prosecution of such offenses in international courts (Rowe, N.C., 2007).

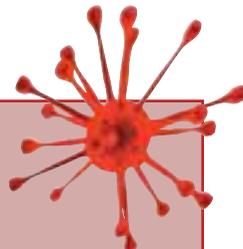
In conclusion, no solution proposed above, utilizing only current technology, is especially robust or complete. As a result, one can see that further developments must be made both technically and legally in order to sufficiently address the problem of attributing an attack. In order to come remotely close to accomplishing this goal, any solution must consist of multiple solutions, spanning all of the areas discussed and developed in conjunction with one another.

Technologically, the issue at hand is positive identification of an individual or organization ultimately responsible for carrying out an attack, while real world solutions are required to determine an attacker's motivation and administer some sort of response. Consequently, the respective solutions developed in each category should work toward meeting these individual goals in a complementary fashion.

Jeffrey Wozniak is a student at Purdue University Calumet studying information assurance and security. He is specifically interested in control mechanisms and technologies of security. After graduating he plans to seek employment in the United States' intelligence community.

Samuel Liles, as an associate professor of computer information technology at Purdue University Calumet, researches cyber warfare and cyber terrorism. His research agenda follows the spectrum of information operations and how cyber warfare realistically impacts the kinetic effects of conflict.

WORKS CITED

- 
- Acohido, B. & Swartz, J. (March 16, 2008). Bot-net scams are exploding. *USAToday*. Retrieved December 5, 2008. from http://www.usatoday.com/money/industries/technology/2008-03-16-computer-botnets_N.htm
- Al-Duwairi, B., Daniels, T.E. (2004). Topology based packet marking. *Computer Communications and Networks*. 11, 146-151.
- BBC. (December 5, 2008) Brown urged to keep hacker in UK. *BBC News*. Retrieved December 6, 2008. from <http://news.bbc.co.uk/1/hi/technology/7768394.stm>
- Bokkelen, J., Corey, V., Greenberg, M. S., Peterman, C., & Shearin, S. (2003). Network forensic analysis. *IEEE Internet Computing*, December 2003, 60-66.
- Brenner, S. (2007). At light speed": Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology*, 97, 97.
- Enfinger, F., Nelson, B., Phillips, A., & Steuart, C. (2008). *Guide to computer forensics and investigation third edition*. Boston, Massachusetts: Course Technology.
- Fernandez, E., Pelaez, J., Larrondo-Petrie, M. (2007). Attack Patterns: A New Forensic and Design Tool. *Advances in Digital Forensics*. 242/2007, 345-357.
- Gee, A. (November, 2008). The dark art of cyberwar. *Foreign Policy*. Retrieved December 5, 2008. from http://www.foreignpolicy.com/story/cms.php?story_id=4553
- Intelfusion. (2008, August). Social Network Analysis and Cyber Warfare: An Open Source Project. Retrieved October 5, 2008, from Intelfusion Web site: <http://intelfusion.net/wordpress/?p=398>
- Manimaran, G., Muthuprasanna, M. (2008). Distributed Divide-and-Conquer Techniques for Effective DDoS Attack Defenses. *The 28th International Conference on Distributed Computing Systems*. 2008, 93-102.
- Markoff, J. (August 13, 2008). Cyberwar and real war collide in Georgia. *International Herald Tribune*. Retrieved December 5, 2008. from <http://www.iht.com/articles/2008/08/13/europe/cyber.php>
- Morrill, D (2006, September 08). Cyber conflict attribution and the law. Retrieved October 15, 2008, from Managing Intellectual Property & IT Security Web site: <http://it.toolbox.com/blogs/managing-infosec/cyber-conflict-attribution-and-the-law-10949>
- Neil, M. (September 24, 2007). Lawmaker: Fed didn't sport cyber-attack. *ABA Journal*. Retrieved December 5, 2008. from http://abajournal.com/news/lawmaker_feds_didnt_spot_cyber_attack/
- Rowe, N. C. (2007). War Crimes from Cyber-weapons. *Journal of Information Warfare*. 6, 15-25.
- Shachtman, N. (2008, August 12). U.S. embassy in Russian hackers' crosshairs? *Wired*, Retrieved September 30, 2008, from <http://blog.wired.com/defense/2008/08/investigators-a.html>
- Strohm, C. (November 24, 2008). Officials lack policy for taking cyber war offensive. *NextGov*. Retrieved December 5, 2008. from http://www.nextgov.com/nextgov/ng_20081124_1148.php
- Tang, Y., & Daniels, T., E. . (2005). *A Simple framework for distributed forensics*. Paper presented at the Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05).
- Traynor, I. (May 17, 2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved December 5, 2008. from <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>



PSYOP

in the Age of

Inter-Consciousness

U.S. Army Staff Sgt. Nicholas Palmer of 13th Battalion, 2nd Psychological Operations Group, drops leaflets from a UH-60 Blackhawk helicopter over Amarah, Iraq. (U.S. Army Photo by Spc. Donte Baltimore/Released)

By Clay Wilson, PhD, CISSP

OVERVIEW

The term military psychological operations (PSYOP) often generates images of Japan's "Tokyo Rose", North Vietnam's "Hanoi Hannah", and more recently, Iraq's "Baghdad Betty" of Desert Storm. However, in the future, PSYOP will be conducted using modified strategies as U.S. and NATO forces place added emphasis on influencing local consensus to win the hearts and minds of populations abroad. Events such as the planned withdrawal of U.S. troops from Iraq, and the recent warning by a British military official that

the war in Afghanistan in unwinnable, both indicate that guns alone will not be the deciding factor in the ongoing war against terrorism. (1) This paper argues that for PSYOP to be successful and effective, future strategies must also adapt to the new ways populations now share information.

We are entering an age where a new type of consciousness is emerging; where Internet technology, social network sites, text and video messages, wikis, and blogs allow us to easily share our individual experiences, and some day, even the perceptions of all our five senses. It is a type of consciousness that we cannot yet call a collective consciousness, but it is becoming something much more than individual consciousness, and it is being enabled globally by growth in portable communications devices and the Internet. For now, we can call it "Inter-Consciousness", where our awareness of events in the world is expanded through immediate and increasing exposure to the ideas and opinions of others.

Today the world is experienced quite differently than it was by individuals five years ago or perhaps as recently as two years ago. In that time, new technologies, including Web methods which enable viewers to post their own content, have enabled information to be accumulated and more knowledge to be acquired through collective activity. New information is made more immediately available, and increased understanding is enabled through multiple channels of communication where topics are continually being created, updated, and debated. Knowledge of a local community, or of the world, is increasingly being shaped by ideas and comments shared between numerous individuals. Those ideas either reinforce or temper each other, and each individual is influenced in new ways through this increasingly collective capability.

However, one result from the increasing realization of inter-consciousness may be a reduced effectiveness for current PSYOP strategies, where attempts to influence local consensus can possibly be ignored or negated, simply through the

mass of interactions among natural participants who may collectively overpower PSYOP influence. Consensus by masses of individuals, who communicate online and collectively gravitate toward what appears evident, or true, or valid, may carry more influence than other messages that might appear as outliers.

This paper examines the emergence of inter-consciousness, and provides examples that illustrate its characteristics. The added PSYOP emphasis on winning hearts and minds is described, along with examples and proposed methods for measuring the effectiveness of a PSYOP campaign. The paper lists lessons from the private sector advertising industry that can be applied to military PSYOP for influencing local consensus, and describes policy issues that are related to PSYOP and inter-consciousness.

INTER-CONSCIOUSNESS DEFINED

"A mass of ideas has no social meaning unless there is what may be called an 'inter-consciousness' of each other's existence" – Michael Davis, Columbia University, 1909. (2)

Inter-Consciousness is different from what is commonly called "collective consciousness". Collective consciousness involves the transfer of thoughts throughout a group without active or deliberate effort on the part of individuals. Inter-consciousness is a state of social awareness that individuals experience as they actively connect to participate in a global community of ideas, sights, and sounds that are openly available through communication devices. Technology for multi-channel communication gives individuals this ability to simultaneously view what masses of people are thinking, and interact and exchange to gradually move toward consensus.

As technology changes, and the volume of online information continues to expand, individuals may some day also be attracted to experience what others actually touch (haptics), smell (olfaction), or taste (gustation), as well.

For now, inter-consciousness attracts individuals through the exchange of ideas, opinions, and comments, as well as through the experience of video and sound. Part of what gives the experience of inter-consciousness the power to resist outlier influence is the size of the collective exchange that can involve individuals from cultures located all around the world – individuals exchange ideas based on different cultural values, and those ideas reinforce or temper the opinions of other individuals in different cultures. Many exchanges from a variety of individuals can gradually strengthen a global understanding and tolerance, similar to the exchange of ideas encountered as one travels through foreign lands. The experience adds to maturity, and increases resistance to ideas that may appear uninformed. Inter-consciousness also derives from another type of power; the spontaneity and unpredictability of ideas, and near-instantaneous speed of communications. It is possible that this power from collective debate, and rapid exchange might eventually drive humanity towards a more global and less-local consensus on issues, reducing barriers and leading to more mutual understanding.

New Internet methods allow individuals to post their own content on web sites, and comment on the opinions of others, sometimes adding eyewitness accounts and posting video clips of events as they unfold. Automatic notifications alert individuals when topics in which they have a special interest are being discussed online. Participants in exchanges can include any age, race, or gender and can be located in any geographic area. Information updates can occur instantly and continuously, often outpacing the news media. In acknowledgement of this increasing capability to access events and relay information quickly, the TV news media has moved to incorporate blogs into their reporting process, and to seek more eyewitness video input. Concurrently, circulation of many newspapers is dropping, and traditional TV news broadcasts are losing revenue because of the Internet. (3)

Internet and cell text messages and video services are increasingly available globally, even in what some would call third-world countries. Automatic online language translators reduce barriers between languages, and illiteracy is less a factor since the communication of ideas can gradually rely more on video images and less on writing. In addition, as portable devices become more sophisticated, the underlying technical complexity is masked by simpler, easier-to-use controls.

Cell phones and laptops allow us to carry our global connectedness everywhere we go. Now, anyone can take on the role of on-the-scene reporter, and through cell phone videos allow history to unfold right before the eyes of a community of viewers, without the filtering and interpretation usually provided by the news media. One result is that media outlets, such as TV and newspapers, are losing viewers and subscribers to new, rapid, and varied sources of information that collectively manifest as inter-consciousness.

HARNESSING THE POWER OF INTER-CONSCIOUSNESS

A notable example of the effects of inter-consciousness can be found in the Democratic Party's campaign leading to the 2008 election of Barack Obama. The Obama campaign made extensive use of the Internet to broadcast its messages directly into the homes and offices of American people. The campaign web sites invited viewers to also input their own thoughts and comments and debate the views of others through blogs, which informed both the campaign staff as well as other viewers. Viewers became bloggers and information contributors themselves, and their ideas were placed on display for all to see, amplify or debate. Information was picked up from these blogs and carried beyond the Obama web site.

The Obama website provided space for an emerging inter-consciousness, where participants added to a collective knowledge base, and reacted to or modified each other's opinions on a global scale



U.S. Army Staff Sgt. Nicholas Palmer of 13th Battalion, 2nd Psychological Operations Group, drops leaflets from a UH-60 Blackhawk helicopter over Amarah, Iraq. (U.S. Army Photo by Spc. Donte Baltimore/Released)

that was never possible before the advent of networks to support world-wide instant public communications.

Some blogs took directions that were impossible to predict. These included debates between supporters and detractors, prayers of hope, complaints about credit card companies, questions about the rise of China, and numerous other topics. Comments and participation in online debates were not limited only to those residing in America. Many citizens of other countries were able to add their own thoughts and opinions to the blogs, and participated in this campaign in ways never before possible on such a large, publicly open, and global scale. According to a Newsweek article, the Obama campaign raised over \$458 million, largely through donations of less than \$25, and including some funds from foreign sources (which reportedly were returned). (4) It can be imagined how the thoughts and comments of citizens from other countries must have influenced Americans in online debates, and how they added directly to the inter-consciousness that emerged to both support and criticize the Democratic candidate. As time passed for the campaign, it appeared that a majority of

people in other countries viewed Obama favorably, and after the election results were posted, there were reports of celebrations and dancing in the streets of several countries.

The Obama transition team has continued using the Internet through a new web site, <http://change.gov/>, where viewers are now invited to become participants in discussions about health care, the environment, and opportunities for individual service to the country. And since there are no apparent rules to block participation from a variety of sources, once again, citizens from other countries may join in these discussions. In addition, Steve Grove, head of news and politics at YouTube, reportedly stated that, "Obama told us in a YouTube interview last year that he plans to have 'fireside chats' on video, and we expect his administration will launch a White House YouTube channel very soon after taking office." (5)

OTHER EXAMPLES OF INTER-CONSCIOUSNESS

Newer generations are abandoning newspapers and the regular nightly TV news broadcast, and prefer instead the speed and currency of online news feeds

and podcasts. Local communities and governments create blogs to invite increased user exchange and continuous feedback on community issues. Online viewers can easily become authors who share their comments with other viewers and authors.

Through an increasingly global collection of experiences, we are individually able to temper each others judgments about what is true and untrue for current events in a larger world. Sometimes those collected experiences can bypass, outpace, or even conflict with lagging reports from a bureaucratic government agency or the news media. This view is supported by yet another example of inter-consciousness that emerged during the 2008 terrorist attacks in Mumbai, India. There, the trapped hostages, plus outside friends and relatives, used cell phones to keep each other and distant family members updated on rapidly-changing circumstances, by sending videos and text messages to each other about the ongoing police action. In many cases, these cell-phone communications among relatives preceded the news reports broadcast on local TV stations. Eventually, as law enforcement officials began their final assault on the occupied buildings, local TV stations were forced by the government to suspend their broadcast in order to prevent the terrorists from watching the plans unfold on hotel TV sets. That left only continuous cell-phone videos as the remaining link to which the community of concerned relatives could turn. The cell messages were rapid, from a variety of primary sources, and often relied upon more by the citizens of Mumbai than news reports from the TV media.

The emergence of inter-consciousness may hold a message for any group or organization that wants to guide or influence perceptions, or shape local consensus. The expanding manifestations of inter-consciousness (blogs, social web sites, cell text messages and videos) may present new challenges for PSYOP proponents, similar to the challenges now affecting the news media. In the future, PSYOP

may be forced to adapt to the characteristics that describe inter-consciousness, including speed, variety for sourcing, spontaneity, and unpredictability. The questions that arise are: will adaptation to these characteristics by PSYOP proponents be enough to overwhelm inter-consciousness that manifests naturally, such as in blogs by local individuals, text messages and video clips from a variety of observers, and social web sites attended by large groups; will PSYOP campaigns be more or less effective in the future; and, will planning be adequate to overcome rapid and spontaneous global communications and other manifestations of inter-consciousness?

ADDED EMPHASIS ON PSYOP

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. PSYOP is also part of what DOD calls Information Operations (IO). DOD IO are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives.

In the past, PSYOP was identified by most as a tool for propaganda, used frequently during times of conflict to demoralize an adversary, or disrupt their decision-making process. However, DOD now emphasizes that PSYOP strategy must be fashioned to influence local consensus, and sometimes used outside times of conflict. For example, to reduce the popular support base for adversaries, the target audience for PSYOP may become the civilian populations that form a group of local villages. In a new effort that emphasizes winning hearts and minds, products created for PSYOP must also be based on in-depth knowledge of the culture that forms the framework for an audience's decision-making processes. Using this knowledge, the products intended for PSYOP must be produced rapidly, and disseminated di-

rectly to targeted audiences throughout the area of operations.

However, studies reviewed in a 2005 report by the National Defense University (NDU) found that U.S. PSYOP forces could not effectively disseminate materials over the Internet, or via commercial broadcast satellites, and that in some cases competitor civilian news organizations, such as Al Jazeera, were found to be better funded and freer of restrictive policies. In addition, U.S. personnel were not adequately trained in civilian marketing, polling, and media production skills. The NDU report also stated that Army PSYOP forces have a Cold War-oriented structure, often antiquated equipment, and limited financial support, even though PSYOP units were inundated with requests for support from the geographic combatant commanders to get information to foreign target audiences – audiences that are being served by an ever expanding array of information dissemination options. The report concluded that the Internet is a major new information transition method that should be exploited by using new systems and approaches. (6)

EXAMPLES OF PSYOP

Some observers say that military PSYOP has always been as much art as science. During the Revolutionary War of the colonies, leaflets were passed out to British soldiers at the battle of Bunker Hill promising free land if they defected. Prior to the 1994 U.S. invasion of Haiti, overhead aircraft reportedly beamed pro-Jean-Bertrand Aristide radio and TV spots into Haiti to prepare people for his return. However, a Defense Science Board study found that during NATO's 1999 air war over Kosovo, broadcasts from overhead aircraft were largely ineffective.

During the 1991 Desert Storm War, millions of leaflets were air dropped on Iraqi troops occupying Kuwait urging them to surrender. The PSYOP units broadcast accurate news to Iraqi soldiers along a two-way frequency, enabling them to call with their field radios and receive instructions from an Arabic-speaking of-

ficer who could explain how to give up safely. Many DOD officials believe that this Desert Storm PSYOP campaign encouraged thousands of Iraqi troops to surrender when U.S ground forces entered Kuwait. In 2001, Air Force planes over Afghanistan dropped hundreds of thousands of leaflets with a fairly simple message. The leaflets show an American soldier shaking hands with an Afghan in front of a mountain range. Printed in Afghanistan's two most common languages (Da ri on one side and Pashtu on the other) was one simple sentence: "The Partnership of Nations is here to Help." (7)

However, experts disagree over how to create an effective PSYOP strategy in Afghanistan, a country where much of the population is very isolated. The Taliban regime is unpopular among large segments of the population, and perhaps Afghans are starved for other outside information. But the Taliban has had an iron grip on what Afghans see and hear - and therefore a long lead in the PSYOP war. (8)

MEASURING EFFECTIVENESS OF PSYOP

Observers report that Army PSYOP specialists have sometimes found that the most effective method for influence is the truth. However, different cultural values, or differing interpretations of an observed event, may lead to disagreements, however unintentional, about what a target audience may call 'true'. In addition, what is viewed as 'true' may sometimes not offer a clear path toward a desired PSYOP goal.

Some Measures of Effectiveness (MOE) mistakenly quantify performance rather than effectiveness; an example is simply counting the number of leaflets dropped over an area. The effects of PSYOP are usually measured after being aggregated over long periods of time. Qualitative techniques such as focus groups are used to complement quantitative measures, and can be used to delve into why trends exist. However, such qualitative measures sometimes have biases such as cultural or language barriers, personality conflicts, or the trepidation of the respondents - for example, if the administrator is wearing a uniform and carrying a gun. (9)

Other proposed methods for PSYOP evaluation rely heavily on information from situation reports (SITREPs) and opinion polls. However, observers argue that there are a number of problems with this approach. For example, SITREPs often provide only subjective information about events, based upon anecdotal observations of the personnel reporting. Polls are designed to represent the opinions of a population by conducting a series of questions



**The face of IO is changing ...
SOSi is lighting the way !**

SOS International –
20 years of understanding,
engaging and shaping
information operations and
strategic communications
for clients
around the world.



www.sosiltd.com

and then extrapolating generalities. While they provide valuable insight, ultimately, these other approaches do not yield the systematic, behavior-focused information necessary for evaluating the effectiveness of PSYOP in achieving its objectives. (10)

MADISON AVENUE TECHNIQUES

Advertising specialists in the private sector (Madison Avenue) can measure the effectiveness of one of their product advertising campaigns by simply observing over time when, where, and on what a target population spends its money. Obviously, the same is not true for military PSYOP. However, a recent study by the RAND Corporation examined how successes from the commercial marketing industry might be used to assist U.S. military PSYOP strategy for Iraq and Afghanistan. (11)

The study found that, in the private sector, "Branding" plays an important role in developing influence with a population. Brands are the associations that people make with a product name. Branding principles suggest that every action, decision, and message of a military force can shape the local population. This indicates that it is important to present a unified message to the target audience, in both word and deed. In addition, it is important to first learn the wants and needs of the target audience. This is what empowers private sector businesses to deliver products or services that satisfy their customers. Therefore, local perspectives should be incorporated into the decision-making processes to create PSYOP designs that are effective. Finally, the U.S. military should also empower local government employees, and indigenous soldiers, with Internet tools, such as blogs, so that they can also advocate on behalf of NATO objectives.

ISSUES FOR PSYOP AND INTER-CONSCIOUSNESS

Characteristics of inter-consciousness include 1) spontaneity and immediacy, 2) the involvement of a variety of sources (often international), and 3) the use of

a variety of transmission methods (cells, social networks, blogs, podcasts), 4) sometimes leading to unpredictable consensus for a community of common interests. In the future, PSYOP campaigns must adapt to these same characteristics in order to remain effective to influence local consensus and decision-making.

However, while the Internet has exposed us all to a new style for thinking, there may also be something deeply troubling issues associated with the immediacy of inter-consciousness. While we come into contact with more ideas from more sources on a daily basis than ever before, some observers argue that less thought now goes into ideas before they're exchanged, accuracy suffers at the expense of time, sources aren't double-checked, and legend becomes truth. And, simultaneously, the concept of authoritative sourcing may be in flux. (12) However, just as other swarms in biology have ways of becoming self-organizing, future local and global communities may find ways to change their response to Internet information in ways that lessen the effects of chaos.

PSYOP THAT AFFECTS AMERICAN AUDIENCES

DOD policy prohibits the use of PSYOP for targeting American audiences. However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these targeted messages, and replay them back to the U.S. domestic audience. Therefore, a sharp distinction between foreign and domestic audiences cannot be maintained.

TERRORIST INFLUENCE THROUGH THE INTERNET

Reportedly, Taliban militants in Afghanistan, use their websites, send text messages, and make frequent calls to reporters to gain ground in the information war. (13) Insurgents also detonate roadside bombs and afterwards transmit video images of successful attacks against U.S. troops for broadcast on the

local news or the Internet, to influence public opinion about the future outcome of the War. In some cases, populations may have these video broadcasts or local TV news stories in their native language as their only source of information. These actions may indicate that the primary terrorist objective is to use and manipulate information, while the violence is actually secondary.

In addition, the civilian Al Jazeera news network, based in Qatar, now beams its messages to well over 35 million viewers in the Middle East, and is considered by many to be a "market competitor" for U.S. PSYOP. DOD officials have expressed concern that U.S. forces are being outmaneuvered on the Internet, and that we should invest more resources in creating our own effective Internet messages. Some observers have stated that the U.S. will continue to lose ground in the global media wars until it develops a coordinated strategic communications strategy to counter both terrorist groups and competitive civilian news media, such as Al Jazeera.

COMBINING PSYOP AND PUBLIC AFFAIRS

NATO military officials normally consider the Public Affairs function as separate from the military Information Operations function. However, recent news reports show that the commander of NATO's forces in Afghanistan has ordered a merger of the NATO Public Affairs Office (PAO) and the Information Operations and Psy Ops (PSYOP) office. Officials of several NATO nations reportedly stated that such a change could undermine the credibility of information released to the public. (14)

CONCLUSION

Methods for PSYOP now emphasize influencing local consensus to help reduce popular support for terrorist groups and other adversaries. However, communication and Internet technology enable near-instantaneous sharing and exchange of ideas, and enable individuals to experience a new collective awareness,

or inter-consciousness. Newer generations are also abandoning past methods of mass communication and embracing this new experience, which means they are receiving extra information and viewpoints from others in cultures around the world. Through new technology, inter-consciousness will evolve to include even faster communication, and many more shared perceptions and ideas from individuals. The emerging consensus on any topic that is experienced with inter-consciousness will be more global and less local, less predictable, and perhaps increasingly difficult for PSYOP to deliberately influence. As communities become less isolated, consensus will form more rapidly and outlier positions will be noticed more readily. PSYOP methods and messages must adapt to the characteristics of inter-consciousness, or else experience a gradual loss of effectiveness, similar to the fading newspaper and news broadcast industries.



U.S. Army Staff Sgt. Bruce Johnson, left, and Sgt. Tyler Wheaton use digital recorders near Baghdad, Iraq, to broadcast a message to residents on how to cooperate during a cordon and search operation. Johnson is with Tactical Psyop Team 1635, and Wheaton is with Alpha Company, 5th Battalion, 20th Infantry Regiment. (DOD photo by Mass Communication Specialist 2nd Class Kitt Amaritnant, U.S. Navy/Released)

ENDNOTES

- 1) Carlton Smith, senior commander of British forces in Afghanistan, reportedly stated, "We are not going to win this war..." and that the insurgency should be "reduced to a manageable level..." Christina Helmand, War on Taliban cannot be won, says Army chief, Times online, Oct 5, 2008, [http://www.timesonline.co.uk/tol/news/uk/article4882597.ece].
- 2) Michael Davis, Psychological Interpretations of Society, Studies in History, Economics and Public Law, vol. 33, no.2, 1909, Columbia University.
- 3) "...evidence suggests that the Internet is redistributing the news audience in a way that is pressuring some traditional news organizations. Product substitution through the Web is particularly threatening to the print media, whose initial advantage as a "first mover" has all but disappeared." Thomas Patterson, John Kennedy, Creative Destruction: An Exploratory Look at News on the Internet, the Joan Shorenstein Center on the Press, Politics and Public Policy, Harvard University, Aug 2007.
- 4) Michael Isikoff, Obama's 'Good Will' Hunting, Newsweek, Oct 4, 2008, [http://www.newsweek.com/id/162403].
- 5) Jose Antonio Vargas, The YouTube Presidency, Washington Post, Nov 14, 2008, [http://voices.washingtonpost.com/theadail/2008/11/14/the_youtube_presidency.html].
- 6) Christopher Lamb, Review of Psychological Operations Lessons Learned from Recent Operational Experience, National Defense University Press, Sep 2005, [http://www.ndu.edu/inss/Occasional_Papers/Lamb_OP_092005_Psyop.pdf].
- 7) Douglas Waller, Opening Up the Psyop War in Afghanistan, Time magazine, Oct 16, 2001. Leaflets Dropped Over Afghanistan: Operation Enduring Freedom, [http://www.psywarrior.com/Afghanleaflinks.html]. Commando Solo Radio Broadcast Scripts: War on Terrorism in Afghanistan, [http://www.psywarrior.com/radioscripts.html].
- 8) Douglas Waller, Opening Up the Psyop War: The U.S. goes on the offensive for the hearts and minds of Afghans, Time Magazine, Oct 16, 2001, [http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=64&paper=342].
- 9) Ryan Clow, Psychological Operations: The Need to Understand the Psychological Plane of Warfare, Canadian Military Journal, Aug 27, 2008, [http://www.journal.forces.gc.ca/Vo9/vo9/05-clow-eng.asp].
- 10) Gregory Seese and Paul Smith, Measuring PSYOP Effectiveness, Special Warfare, Dec 2008, Vol. 21, No. 6, [http://www.soc.mil/swcs/swmag/Articles_Page5.htm].
- 11) RAND National Defense Research Institute, Applying Madison Avenue Principles and Recent Operational Experience to Counterinsurgency and Stability Operations, 2007, [http://www.rand.org/pubs/research_briefs/2007/RAND_RB9268.pdf].
- 12) Dan McCreary, The Internet as Shared Consciousness, Effect, Winter 2001, p.31, [http://www.larsonallen.com/effect/win2001/internet.pdf].
- 13) Reuters, Press and "Psy Ops" to merge at NATO Afghan HQ: sources, Yahoo News, Nov 29, 2008, [http://news.yahoo.com/s/nm/20081129/wl_nm/us_afghan_nato_1].
- 14) Reuters, Press And "Psy Ops" To Merge at NATO Afghan HQ: sources, Yahoo News, Nov 29, 2008, [http://news.yahoo.com/s/nm/20081129/wl_nm/us_afghan_nato_1].

Information Related

TERMS, TRENDS & MYTHS

By Garry J. Beavers and F. H. "Skip" Allison

Marketing is an attempt to sell through persuasion.

Mass marketing is a market coverage strategy in which a firm decides to ignore market segment differences and go after the whole market with one offer. (1)

TERMS

In the "military information" market we have "firms" that are attempting to market information warfare, information operations, cyberspace operations, strategic communication, information engagement, influence operations, network centric warfare, and other "products" associated with the power of information. When bombarded with the time honored marketing claims of "NEW" and "IMPROVED", we (the military information customer) must turn a critical eye and ear to these claims to be sure we are not just getting replacement terms and concepts that are actually repackaging of existing information related terms and concepts. Much of the recent mass marketing generates confusion, distrust, and myths about the potential power of information and might actually mislead political and military leaders.

The United States, along with most other nation states and non-state actors, understands and appreciates that information is one of the elements of power that enables achievement of organizational objectives. But, certain trends promote the mass marketing of different terms and creation of myths about information.

TRENDS

First, the incessant drive to earn the next promotion, bonus, rainmaker status, control of resources, or star-power name recognition can become the dominant force behind the next great idea for the application of the power of information. This almost always generates new terminology to support, describe, and market the new idea.

Second, advocates that firmly believe in the power of information, but subscribe to the primacy of an individual information capability, may initiate a marketing campaign as a means to achieve their individual goals at the expense of a more cohesive and holistic strategy for the application of the power of information.

Third, implementation is not as sexy as inspiration. Even well researched and developed concepts require modification and fine tuning to succeed. The mundane tasks of writing policy and doctrine, creating programs of instruction, designing exercises and developing equipment test plans to nurture and grow a concept are demanding and do not provide much recognition or gratification in the short run. It is very tempting to switch horses to an emerging concept with its vibrant intellectual discussion, big-picture concept, and lexicon development and abandon the previous concepts as unworkable or outdated.

Savvy “digital natives” and “digital immigrants” (2) understand the power of information and some can recognize disinformation, misinformation, propaganda, public affairs, and other information related techniques when they are used in the mass marketing of information related terms and myths. Despite this level of awareness, leaders, their subordinates and the supporting information community of practice can be confused by competing information terms and the myths that are associated with those terms.

MYTHS

First information term and associated myth: There is no Information Environment.

Information is a basic feature of the natural environment that man has adapted to over time. As society developed, man also developed and refined capabilities to acquire, process, store, distribute, control, use, and protect information. As nations developed, they relied on increasingly specialized capabilities to project power throughout the militarily relevant portion of the natural environment – the operational environment. This operational environment is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the military commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment. (3)

Military operations occur in, on, or through these five components of the operational environment. All military operations and their supporting functions rely on information. Leaders use specific information to harness and direct functions that in turn generate combat and military power throughout the entire natural and operational environments. Many leaders have come to accept the Infor-



U.S. Army Soldiers with Detachment 1080, 318th Psychological Operations Company distribute “Baghdad Now,” a periodical put together by the 318th in the East Rashid region of Baghdad, Iraq. (U.S. Navy photo by Mass Communication Specialist 3rd Class David Quillen/Released).



A civilian interpreter with the Tactical Psychological Operations Team (PSYOPS), asks a local Iraqi civilian for directions to the nearest fish farm in Haswah, Iraq. PSYOPS collects economic data for the future benefit of the Iraqi people. (U.S. Army photo by Spc. Tiffany Dusterhoft/Released)

mation Environment as a concept that encompasses all the aspects of information that generate and sustain power. Officially defined as “the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information” (4), the Information Environment is also a “warfighting domain”. The history of armed conflict includes endless examples of military engagements and campaigns that centered on the fight for and with information. Since all military functions and operations rely on it, the Information Environment does not naturally fall within the purview of any one Defense Department or Component.

Second information term and associated myth: Cyberspace is a new warfighting domain.

Cyberspace does exist. However, it is a “domain within the information environment” and it is not new. After two years of debate, recently approved definitions clearly identify that cyberspace encompasses “the interdependent

network of information technology, infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" and cyberspace operations are "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." Cyberspace, as this man-made, interdependent network, is not the military operational equivalent of the four physical domains and the information environment. Cyberspace exists with other information systems and networks within the Information Environment in the same manner that other systems (tanks, ships, and missiles) exist within the physical domains.

Cyberspace is not new. Some cyberspace advocates use that term (a "product improved definition") as a replacement for a previous mass marketing effort touted as network centric warfare. Network centric warfare attempted to combine networked

communications, intelligence, surveillance, and reconnaissance, computer network operations, network warfare, and electronic warfare into a new warfighting "domain".

Cyberspace advocates that view it as the product improved version of network centric warfare ignore the fact that each of the individual components evolved initially to support other warfighting functions and operations. Cyberspace as a system of interdependent networked information systems existed well before wireless communications, the Internet, and the proliferation of computers. Use of interdependent networked information systems for warfighting began with the telegraph and continued with the radio and satellites. The modern version of cyberspace now relies on digital networks linked to computers instead of telegraphs, teletypes, radios, and other systems to provide information and support information related functions.

Cyberspace has been part of warfighting since the American civil war. Computers at the end of extended digital networks are merely the latest tools that can attack, defend, and exploit information on a networked information system. The introduction of each successive information system introduced new capabilities and vulnerabilities for military operations. Computers and computer networks also introduce new capabilities and vulnerabilities that impact on military operations. The networked information systems that comprise cyberspace today present a more lucrative target for adversaries simply because they carry more information and support more of the common military information functions than any of the other preceding information systems.

However, adversary interest in networked information systems is not a new development brought on with the advent of computers. Adversary interest in networks simply is an extension of the desire to find and exploit information. When computers and networks are replaced at some future date with a more advanced information system, adversaries will shift their efforts to the new system and mass marketing efforts will follow to emphasize the importance of fighting and winning within a new "domain" created for the next new information system.

Third information term and associated myth: Information Operations are replaced with five new information tasks.

Five "information tasks" were introduced into Army doctrine with the revision of Field Manual 3-0 (FM 3-0), Operations, in early 2008. However, FM 3-0 recognizes that "every engagement, battle, and major operation requires complementary information operations" and that Information Operations includes "associated Army information tasks." There are those that hold that the five information tasks (Information Engagement, Command & Control Warfare, Military Deception, Operations Security, and Information Protection) replace Information Operations. Others contend that this is just a reorganization of the core, supporting and related Information Operations capabilities defined in DoD policy and in Joint doctrine and policy. The capabilities that enable the accomplishment of the information tasks are the same capabilities that are synchronized and coordinated as Information Operations under Joint doctrine.

WHITE WOLF SECURITY

Large scale cyber-exercises

Turnkey solutions	On-site, multi-site or remote	Full reporting Central IDS
----------------------	-------------------------------------	----------------------------------



Traffic generation VoIP/GSM	Flexible environment
--------------------------------	-------------------------

www.whitewolfsecurity.com
 1052 New Holland Ave
 Lancaster, PA 17601
 717-295-6201 (o)

The task currently identified as “Information Engagement” is a re-branded term for the non-lethal Information Operations conducted in Bosnia and Kosovo as “Information Campaigns” as early as 1996. The Information Operations capabilities identified in FM 3-0 as supporting the “Information Engagement” task were first integrated with additional capabilities as “Information Campaigns” in Bosnia and later in Kosovo. “Information Campaigns” used all non-lethal information related capabilities to provide carefully selected audiences with accurate and reliable information to counter the propaganda and decision-making cycles used by each of the warring factions to promote violence. “Information Campaigns” were essential to disrupting the cycle of violence that threatened to undermine stability operations in the Balkans.

The same Information Operations and information related capabilities are used today to support stability operations in Iraq and Afghanistan. Fortunately, the rules of engagement in Iraq and Afghanistan permit the use of other Information Operations and related information capabilities that were prohibited under the Balkans rules of engagement. Coalition forces can integrate Electronic Warfare capabilities with other Information Operations capabilities to achieve both lethal and non-lethal effects.

“Information Campaigns” or the product improved term for the same thing, “Information Engagement”, may not be the primary or lead Information Operations task at the tactical through operational levels during major combat operations or during an electronic attack on our military or national information systems. Information Operations capabilities and tasks such as Electronic Warfare, Computer Network Operations, Operations Security, Military Deception, and Psychological Operations combined creatively with other related information capabilities and integrated as Information Operations support the full spectrum of conflict (stable peace, unstable peace, insurgency, and general war).

The integration of IO capabilities to accomplish information tasks, as described in FM 3-0, provides commanders the ability to “direct information tasks to hamper their opponents’ decision-making ability, protect their own, gain the trust and confidence of the people, and win the support of the diverse audiences throughout their operational environment”. This concept is very congruent with the DoD and Joint definition of IO as “the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting [Counterintelligence, Physical Attack, Physical Security, Information Assurance, and Combat Camera] and related [Public Affairs, Civil-Military operations, and Defense Support to Public Diplomacy] capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.”

CONCLUSION

No single department, Service, command, unit, or agency single-handedly possesses or controls all the capabilities and processes that support information related tasks and Information Operations. Thus, Information Operations are conducted by integrating and synchronizing capabilities from multiple agencies, departments, and military services to affect the In-

formation Environment in support of the Commander’s objectives. US military forces conduct Information Operations with the assets on hand, or the assets that are available through coordination, to support their current missions and operational requirements.

The Joint Commander must be able to integrate Information Operations capabilities effectively into his overall planning and execution, regardless of which Service or Agency provides the support. As long as the Commander has confidence in the resultant effect, the individual Service nuances or organization providing the effect should be irrelevant to him. Commanders should not need a Rosetta stone to determine what term a particular Service uses to describe an Information Operations capability or what command and control structure a particular agency uses to provide support for his operations.

Our leaders do not have the time to sort out the mass marketing barrage of confusing information terminology and myths. The replacement of a system or tool with a more capable version is not a warrant for endless, mass-marketed hyperbole. As information related concepts continue to be examined and discussed, we owe it to our leaders, and the great supporting cast of people and organizations that develop and provide capabilities in the Information Environment, to honestly and critically evaluate whether we have truly conceived something original that requires a new lane in the road or whether we have a valid enhancement of existing concepts that will allow us to proceed with greater speed, reduced cost or increased efficiency in the current lanes.

Mr. Garry Beavers has supported Army Information Operations for 14 years as an Army officer and contractor supporting the 1st IO Command, Army National Guard, and the DCS, G-3/5/7.

Mr. Forrest H. “Skip” Allison, has directly supported DoD Information Operations for 8 years as a Navy officer and contractor supporting the Assistant Secretary of Defense for Reserve Affairs and as a contractor supporting the Army Deputy Chief of Staff, G-3/5/7. Mr. Allison served as an Army intelligence officer on active duty, as a Civil Affairs officer in the Army Reserve, and as an intelligence officer in the Navy Reserve.

ENDNOTES

- 1) Wikipedia definition; available from: http://en.wikipedia.org/wiki/Mass_marketing; Internet; accessed 12 December 2008.
- 2) “...today’s students think and process information fundamentally differently from their predecessors. ... their thinking patterns have changed. ... But the most useful designation I have found for them is **Digital Natives**. Our students today are all “native speakers” of the digital language of computers, video games and the Internet. ... Those of us who were not born into the digital world but have, at some later point in our lives, become fascinated by and adopted many or most aspects of the new technology are, and always will be compared to them, **Digital Immigrants**.” Prensky, Marc, “Digital Natives, Digital Immigrants”. MCB University Press, Vol. 9 No. 5, October 2001, P. 1
- 3) “JP 3-0, Operations”. Department of Defense, 13 February 2008, Chapter II, Para. 6.a., p. II-20 – II-21.
- 4) Ibid, p.GL-15.

assure. support. defend.



Honeywell Information Assurance Services

For thirty years, Honeywell has designed, operated, maintained, analyzed and defended IT networks and systems for the U.S. government and Department of Defense. Honeywell Security Engineering and Information Assurance programs currently support the U.S. Navy, U.S. Joint Forces Command and NASA.

As part of your full spectrum Information Operations program, Honeywell's Security Engineering, C&A, Computer Network Operations and Computer Network Defense Services will help your IT networks and systems stay compliant and protected.

Honeywell

Find out more at www.honeywell.com/ia