Vol. 2 Issue 2
May 2010

IO Journal

A publication of the Information Operations Institute

EW and Cyberspace Convergence

Also in this issue:

China's Google Decision

Computers as Weapons of War

AOC
Association of Old Crows

An Important Debate

I won't suggest here what the "right/best" approach is, but I will suggest one that is the "wrong/worst" approach … one which fragments IO into several sovereign and independent tribes.

One of the many benefits of being a professor is the opportunity to learn from some very smart people: my students. I've always said that I learn far more from them than they learn directly from me, although this may be the result of the unique and exceptional people I have been, am, and will be fortunate to have as my students. Sometimes the discussions pertain directly to issues with which the Information Operations, Cyberspace, and Electronic Warfare community—note that I used the singular, not the plural—grapple and debate on a daily basis. That happened in class this week.

The issue in point is the relationship between IO, EW, and Cyber, and the discussion centered on a Venn diagram that depicted several ways of looking at these relationships. One had each of those "tribes" standing apart and separate from the others, and there are certainly some people from those fields who see the world that way. Another had EW nested within Cyber and that nested with IO, and there are some who have argued in support of that approach. A third had Cyber—as defined by the DOD—nested within what we called Electromagnetic Ops, and that in turn within IO. And a fourth that we explored in the class had those circles overlapping but not completely encased. I won't suggest here what the "right/best" approach is, but I will suggest one that is the "wrong/worst" approach, and that is the first one, which fragments IO into several sovereign and independent tribes.

I expect to see these kinds of debates and discussions all across the course of InfoWarCon 2010, which is precisely the kind of venue we—the IO community writ large—need to generate these kinds of discussions and to move our craft and discipline forward. Our attendance will include all of these diverse sets of expertise and experience, yet will also highlight the synergies between them. Last year's return of InfoWarCon was exceptional—all of you reading this at this year's meeting will make it even better …

Dan Kuehl

Dr Dan Kuehl *is a professor of IO at the iCollege of the National Defense University, an Editor of the IO Journal and member of the IO Institute.*

For more information about InfowarCon 2010 – www.InfowarCon.com or www.Crows.Org

IOI Call for Events

The IO Institute is soliciting input for an IO Community Event Calendar. Please send notifications for IO, SC, PD and related events to: IOI@crows.org. At a minimum, please include name of event, location, date and POC information.

Vol. 2, Issue 2 • May 2010

IO Journal

U.S. Navy Aviation Ordnanceman 1st Class Terrence Carr checks his Facebook page while an unknown assailant gains access to the same page on the other side of the screen at Pearl Harbor, Hawaii, January 11, 2010. The Navy urges Sailors and families to practice good operational security to prevent adversaries from discovering critical information. *(U.S. Navy photo by Mass Communication Specialist 2nd Class Mark Logico/Released)*

|o| Contents

On the cover: An air-to-air left front view of an F-4E Phantom II aircraft (top) and an F-4G Wild Weasel Phantom II aircraft (bottom). Note the open refueling port on the top of the F-4E. Both aircraft are equipped with AN/ALQ-119 electronic countermeasures pods.

EDITORIAL & PRODUCTION STAFF
Editors: Carson Checketts, Joel Harding, Dr. Dan Kuehl, Jon Pasierb, Catherine Theohary
Publisher: Elaine Richardson
Advertising: Jason Dolder, Shaun Greyling, Erik Henson, Chris Zabel, Melissa Zawada
Marketing: Allie Hansen
Design & Layout: Deb Churchill Basso
Advertising Art: Effie Monson

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@crows.org.

Computers as Weapons of War

"History teaches us that in asymmetric warfare the most heavily armed do not always win."[1]

—Ignacio Ramonet

By John Bumgarner

Most warfare throughout the two centuries of the industrial era centered on one principal strategic objective: the physical occupation of territory. The possibility of occupying territory, or the threat of becoming occupied, forced many nations to amass large standing armies, to maintain navies, and to build aircraft in hopes of achieving battlefield superiority against their adversaries.

Several pivotal events over the last three decades have been gradually changing that paradigm, shifting nation-states from the industrial era of warfare into the cyber defense era of warfare. One of these events was when cyberspace was classified by the United States government as being strategically important to national security.[2] With that classification, cyberspace became the fifth domain of war, comparable to the domains of land, sea, air, and space. The geopolitical events that were the tipping points that catapulted us from the industrial defense era to one of cyber defense, were the campaign-level cyber attacks launched against Estonia in 2007 and Georgia in 2008.[3] Global militaries are scrambling to understand their own capabilities, their adversaries' capabilities, and the new multidimensional, multidirectional and multilayered battlespace of cyberspace.

The U.S. armed forces have been grappling with these issues for years, but only recently established the U.S. Cyber Command (USCYBERCOM) to start addressing our national defense and economic survivability in cyberspace. The operational mission of the command is to coordinate U.S. operations in cyber network defense and cyber network attacks. The command is linked to the National Security Agency, which has a well established history of contributing to the nation's intelligence collection efforts (e.g. Signals intelligence (SIGINT) and technological advancements (e.g. cryptography) in the digital age.

The ever-increasing asymmetrical (e.g. Al-Qaeda) and peer-to-peer (e.g. Russia) threats posed within this new war-fighting domain are eclipsing current U.S. military doctrine, which outlines Information Operations (IO) capabilities. Current Joint Doctrine outlines five primary categories of IO capabilities, which are Computer Network Operations (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Psychological Operations (PSYOP), and Operations Security (OPSEC).[4]

Electronic warfare, military deception, psychological operations, and operations security have a long established history within the industrial defense era. Computer Network Operations[5] is the only IO capability conceived entirely in the cyber defense era. CNO has three operational missions. The first is to defend information systems from enemy attacks. The second is to gather intelligence from adversarial networks. The final CNO mission is to conduct offensive cyber attacks against enemy computer systems and other electronic assets.

Combining core IO capabilities with traditional military operations (e.g. strikes, noncombatant evacuation operations) has been a major challenge for classically trained commanders. Military leaders need to realize that the cyber component of information operations can support a broad spectrum of combat and noncombat operations, as well as the continual preparations needed for both. Within certain offensive engagements, the IO component can be a more effective option than the use of conventional forces.

U.S. Air Force Senior Airman Lauren Johnson, a 379th Expeditionary Communications Squadron network control center technician, maintains the base computer server for more than 10,000 users January 4, 2010, at an undisclosed location in Southwest Asia. *(U.S. Air Force photo by Senior Airman Kasey Zickmund/ Released)*

U.S. military and political leaders are still debating the rules of engagement and the legitimacy of using the latter capability as an offensive technique in future warfare. In early 2009, Pentagon officials said they were uncomfortable discussing the issue of offensive cyber operations.[6] Senior government officials from the United States and Russia met in November 2009 to discuss the possible creations of treaties that would limit offensive cyber operations and curtail the development of cyber munitions.[7]

As an offensive capability, CNO engagements have as much potential to inflict physical damage on adversaries' information systems as a multi-million dollar missile does. In chemical production facilities, for example, computers controlling reactions that take place at high pressures and temperatures could be used to cause explosions and fires. Operations targeting national critical infrastructure, such as electrical generation systems that service large metropolitan areas, have the potential to cause extreme[8] economic loss and even considerable loss of life. Understanding the full range of offensive engagement possibilities that CNO components can bring to the fight is one of the greatest challenges in the cyber battlespace.

For a number of years, military operations have used electro-magnetic attacks to disrupt enemy communications on the battlefield, but there are now many additional IO capabilities. The cyber campaign against Georgia in August 2008 is probably the best example of how to properly employ one of the newest IO capabilities, computer network attack on a modern battlefield. During that campaign, Russians and Russian sympathizers disrupted key Georgian media sites through the Internet using denial-of-service — a neo-electronic warfare jamming technique of the cyber defense era.

The speed of action and multidirectional nature of these cyber strikes adhered to a classical military swarming technique, overwhelming the cyber defenses of the Georgian targets. The attacking forces were highly decentralized, but were able to synchronize and concentrate their operations in a way that made any Georgian defensive response nearly impossible. The primary objective of this cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fit neatly into a military-style invasion plan. Many of these cyber strikes were clearly designed to make it harder for the Georgians to determine what was happening. The inability of the Georgians to keep these websites up and running was instantly damaging to national morale. These attacks also served to delay any international response to the kinetic conflict unfolding in the South Ossetia region.

Probably the most important strategic lesson learned from the cyber campaign against Georgia is that cyber attacks are a viable military option on the battlefield. Another lesson is that cyber attacks can be launched from a safe remote location. Yet another lesson is that these operations can be employed in certain cases (e.g. targeting civilian communication facilities) where limiting the physical damage to the target is a strategic concern for the theater commander.

Even though the cyber campaign against Georgia was tactically successful, there are several disadvantages to using offensive cyber attacks against an adversary's information systems in place of more traditional attacks such as air strikes or direct

Alexsi, an Israeli air force crew chief, conducts preflight checks at Nellis Air Force Base, Nev., before a training mission at Red Flag July 20, 2009. Red Flag is a highly realistic combat training exercise that pits U.S. and allied nation air forces against simulated enemy forces in a challenging air, ground, cyberspace and electronic threat environment. *(U.S. Air Force photo by Tech. Sgt. Michael R. Holzworth/ Released)*

action missions by special operations units. One of these disadvantages is that cyber attacks don't produce quantifiable results as consistently as their kinetic counterparts do. This is due to the fact that specific cyber attacks can often be rendered useless by routine modification (e.g. application-level patches) in the target system. In military engagements involving equals, the tactical advantage for most offensive cyber attacks goes to the defender, because it is easier and faster to implement defenses than it is to develop offensive cyber attack techniques.

Even with these technical and tactical limitations, computer network operations have great potential in future military conflicts. For example, during the industrial warfare era acts of industrial sabotage against critical targets were often conducted by physical means, thus requiring localized access. In the cyber defense era, the potential for the military to conduct acts of industrial "cybertoge"[9] are increasing exponentially. Key nation states already possess the capabilities to disrupt information systems used within civilian industries that have strategic military value to a nation's war effort. These critical infrastructures include airports, electric power plants, dams, gas and oil pipelines, oil refineries, maritime ports, railroads and manufacturing facilities. Historical warfare precedence shows that all these industries have been targets of sabotage attacks using conventional kinetic methods, such as direct action missions by special operations forces.

Although conventional forces are effective for sabotage, IO forces can conduct many of these operations without causing physical damage to the target or placing soldiers in harms way. There are several technical cybertoge techniques available to offensive IO forces including the use of weaponized computer viruses or worms. Probably the most effective technique available to offensive IO forces is the intentional insertion of a "logic bomb,"[10] into an information system that the target is dependent upon. These malicious programs can be introduced through a variety of means, months or even years before they need to be triggered for a specific operation.

One example that has not been publicized occurred during an unannounced training exercise conducted at a major corporation. During that exercise, I personally crafted some specialized code that was designed to simulate a hardware failure on a common UNIX platform. The warning messages generated by the code contained valid support phone numbers, e-mails addresses, and website addresses for the platform vendor. The technical contact within the corporation contacted the vendor concerning the hardware problems. Over a two-week period the vendor sent multiple technicians to replace various hardware components within their platform. When a replacement component failed to resolve the problem, the technician would escalate the issue to the next tier of support at the vendor. Eventually the exercise was terminated, because the internal support team or the vendor couldn't identify the problem. During the exercise hundreds of man-hours and thousands of dollars were expended to tackle an information system hardware failure that was fictitious.

Unclassified historical examples of logic bomb deployments by military forces do not exist, but we have examples from the civilian sector. One of these examples involves a disgruntled employee who planted a logic bomb within the computers of UBS PaineWebber.[11] When the code was detonated it erased critical files on approximately 2,000 UBS's computers. According to published reports surrounding this incident some of the computers affected were offline for several weeks, which hindered USB's daily business operations. In 2008, a similar incident was accidentally foiled by an employee at the United States mortgage corporation Fannie Mae.[12] The Fannie Mae logic bomb was designed to erase the hard drives for 4,000 servers on a preset date.

There is also a purported historical example of the Central Intelligence Agency using a logic bomb to cause physical damage to a Siberian pipeline. This revelation was highlighted in the book *"At the Abyss: An Insider's History of the Cold War,"* written by Thomas Reed, a former Secretary of the Air Force and former Director of the National Reconnaissance Office. According to Reed's account of the incident, the CIA inserted malicious instructions in pipeline control system software stolen by the Russians. When the software was deployed in the Siberian network, it triggered the logic bomb to activate instructions that were designed to destabilize components that controlled pressure within the pipeline. These pressure destabilizations triggered a failure of safety mechanisms at the pipeline, which eventually exploded. The resulting consequences associated with this alleged attack are an excellent example of how a strategic supply line can be disrupted without using conventional methods (e.g. explosives).

The modern battlefield is littered with military equipment, such as main battle tanks, satellite communication architecture, and UAV battlefield surveillance systems, that contain sophisticated electronic components that can be targeted by cybertoge forces. In the heat of battle, enemy equipment containing embedded malicious code could activate, which in turn could disable computerized targeting systems, global positioning systems, thermal imaging devices, communication components or internal power plants in mechanized weapon systems

(e.g. Russian T-95 main battle tank). When utilized properly, cybertoge attacks achieve the element of surprise, because of their stealthy delivery method. This capability for surprise prevents the adversary from receiving indications that an attack is approaching or already initiated. Under ideal conditions, the enemy may be forced to withdraw or surrender their forces.

Targeted cyber attacks can be just as destructive as operations using cybertoge techniques. Probably the best documented evidence of such an attack is a previously classified video produced by the Department of Energy's Idaho National Laboratory for a project code named "Aurora."[13] This video shows a remote cyber attack being launched against control systems that managed an electric generator hosted within DOE test range in Idaho. The attack was highly effective in causing the generator to fail, because of the mechanical effects caused by the cyber attackers. The attack made the generator wobble and go out of control, caused the rotor to hit the stator, shredded the windings, and made the generator catch fire. This sort of attack becomes more effective, the larger the generator. It could be automated, is scalable, and could be used to destroy large numbers of generators simultaneously.

This successful attack was an eye opener for those industries and government agencies responsible for the security and economic stability of the electric grid in the United States. One of most troubling lesson learned from the Aurora project is how a cyber attack could cause lasting physical damage to a mechanical component. Electrical power components (e.g. dams, power plants, transmission lines) have been viable military targets since their inceptions into the world. During the World Wars, Allied Forces destroyed electric systems with massive bombing campaigns. In 1999, U.S. Forces operating in Serbia under the umbrella of NATO disrupted the electrical power infrastructure using a non-lethal munition,[14] which contained carbon graphite filaments.

While these aerial campaigns have been an efficient method of incapacitating an adversary's electrical systems cyber attacks can be employed in similar ways. Offensive IO forces can launch precision attacks in a given operational area, which could disrupt electrical power prior to committing any conventional forces (e.g. infantry, air assets). In certain political scenarios, the use of IO forces instead of conventional forces maybe the more strategically acceptable option. IO forces can be used in these circumstances to provide a proportional response that disrupts an enemy's critical infrastructures (e.g. electrical power). Limiting physical damage in these cases would greatly reduce repair time and possibly limit any post-conflict restitution payments to replace the components.

This type of attack aligns with one of Clausewitz's nine Principles of War. That principle is economy of force, which calls for the judicious exploitation of combat power in relation to achieving mission objectives. Military-level cyber attacks against electrical power generation facilities increases the likelihood for externalities consequences in the operational area. Such tactical cyber strikes can also cause major disruptions in conventional land-line and Voice over Internet Protocol (VoIP) communications infrastructure, cellular networks, television and radio broadcasts. These secondary disruptions could sever command and control (C2) channels or possibly cripple air defense networks, which would benefit conventional forces operations.

U.S. Marine Sgt. Kermit Harrison, far right, teaches advanced computer networking to Iraqi army Maj. Abbas Ahmed, Communication Officer, 7th Iraqi Army Division, at Camp Mejid, Asad, Iraq. *(U.S. Marine Corps photo by Staff Sgt. Chad L. Simon/Released)*

Another probable IO attack for military forces was highlighted in the 60 Minutes segment entitled "Sabotaging the System."[15] Experts working for the Sandia National Laboratory demonstrated in that segment how to disrupt production at an oil refinery. The cyber attacks were designed to cause critical components to overheat, leading to a catastrophic failure at the refinery. The experts caused this failure by modifying the BTU settings for a heating element within the refinery and by disabling the recirculation pumps used to control increases in temperature. Cyber attacks similar to the one conducted by Sandia could be carried-out by IO forces against refineries that produce fuels, lubricants or petrochemical products used by enemy forces.

Similar IO attacks could be conducted against nation states that have violated international treaties in order to carry out as uranium enrichment for nuclear weapons. Most of the unauthorized enrichment facilities in these cases are constructed deep underground. Conventional munitions, including bunker busters, could have difficulty penetrating and damaging these hardened structures. Cyber munitions, however, could be used to destroy key equipment used in the enrichment process. One of the primary IO targets would be the gas centrifuges used to create weapons grade uranium. The rotors within these centrifuges operate at extremely high speeds (e.g. 50,000 RPM). A cyber attack that increased the RPMs beyond normal safely levels could result in a catastrophic failure of a single centrifuge. Implementing this IO attack across thousands of centrifuges has the potential to disrupt enrichment operations for considerable periods of time.

Offensive military operations targeting enemy supply lines have been conducted for centuries. Modern militaries have adopted just-in-time inventory practices that have greatly limited their on-hand strategic stockpiles of beans, bullets, and

bandages. Offensive IO forces could be used to disrupt these critical supply lines. One of the high-value IO targets would be the computerized inventory control systems used within this fragile supply chain. Once the IO force has penetrated this computerized system, they can identify critical supplies, insert disinformation about the inventory levels of these supplies and then reroute these critical supplies to remote locations. Another probable IO attack would be to reprogram the Radio Frequency Identification (RFID) used to either track individual components or pallets of supplies. Certain RFID tag designs utilized ultra high frequency (UHF), which makes them highly prone to IO attacks using traditional electronic warfare methods. IO forces could also be used to target individual components (e.g. shore-to-ship cranes) used within the shipping process. Many of the modern shore-to-ship cranes are highly computerized, which makes them vulnerable to a targeted cyber attacks. Some of the systems use embedded operating systems (e.g. Microsoft Windows XP), which have known security vulnerabilities. IO forces could exploit one of these vulnerabilities to disable or damage the crane.

The U.S. Armed Forces have sometimes been called on to conduct preemptive conventional strikes against strategic enemy targets. On today's battlefield, military commanders can conduct preemptive cyber strikes against critical infrastructure targets (e.g. oil refineries, electrical power plants, telecommunication nodes) to potentially cause so much destruction that the enemy would have limited ability to carry out combat operations. Such preemptive actions could potentially reduce the collateral damage and casualties normally associated with military conflicts. An adversary that exercises a strategic first cyber strike that successfully disrupts an opponent's critical infrastructures prior to battle could potentially reduce the opponent's capacity to wage war.

The examples discussed in this paper are only a sampling of the possible offensive information operations that could be conducted by military forces within the Cyber Defense Era. These examples underline the importance of utilizing offensive IO forces in future military conflicts. The digital age has made cyber attacks a logical extension of projecting diplomatic and military power against our nation's adversaries.

In this new defense era, wars will not only be waged by high-tech conventional forces using bullets and bombs, but in concert with information operations forces using bits and bytes. Current U.S. military doctrine doesn't fully address these combined neo-warfighting capabilities. The doctrine also isn't designed to quickly adjust to rapid technological shifts that occurred in cyberspace, which could adversely affect military superiority. With the dawning of the Cyber Defense Era comes a pressing need to reassess traditional warfare doctrine to ensure that our armed forces meet the challenges that this new era brings to the 21st Century battlefield.

John Bumgarner *is the Research Director for Security Technology the U.S. Cyber Consequences Unit (US-CCU) and a Senior Research Fellow in International Security Studies at the Fletcher School of Law and Diplomacy of Tufts University. He was formerly a member of the Intelligence and Special Operations branches of the United States Army.*

Endnotes

1 Ignacio Ramonet, "Unjustified means." *Le Monde diplomatique*, November 1, 2001. Accessed at: http://mondediplo.com/2001/11/01unjustified

2 The National Military Strategy of the United States. Accessed at: http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf

3 John Bumgarner and Scott Borg, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, A US-CCU Special Report, August, 2009.

4 Information Operations, Joint Publication 3-13, February 13, 2006. Information Operations also include various supporting and related capabilities. Supporting capabilities include: Counterintelligence (CI), Combat Camera (COMCAM), Information Assurance (IA), physical attack and physical security. Related capabilities include: Civil-Military Operations (CMO), Defense Support to Public Diplomacy (DSPD) and Public Affairs (PA).

5 Information Operations, Joint Publication 3-13, February 13, 2006. Computer Network Operations (CNO) includes: Computer Network Attack (CNA), Computer Network Defense (CND) and Computer Network Exploitation (CNE).

6 David E. Sanger and Thom Shanker, "Pentagon Plans New Arm to Wage Cyberspace Wars." *New Yorok Times*, May 28, 2009. Accessed at: http://www.nytimes.com/2009/05/29/us/politics/29cyber.html

7 John Markoff and Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security." *New York Times*, December 12, 2009. Accessed at: http://www.nytimes.com/2009/12/13/science/13cyber.html? scp=2&sq=russia&st=cse

8 Milton Maltz, "Turning power lines into battle lines." *National Post,* October 21, 2009 Accessed at: http://www.financialpost.com/personal-finance/tax-centre/Story.html?id=2125907

9 The term cybertoge was coined by John Bumgarner, during a presentation entitled "Cybertoge Threats," which was presented at the National Defense Industrial Association Cyber Symposium in San Diego, California on October 27, 2009.

10 A "logic bomb" or "slag code" is a set of instructions that has been intentionally designed to execute (or 'explode') when a particular condition has been satisfied. Commonly these "bombs" delete or corrupt data, reset passwords, or have other harmful effects.

11 Sharon Gaudin, "Ex-UBS Systems Admin Sentenced To 97 Months In Jail." *Information Week,* December 13, 2006. Accessed at: http://www.informationweek.com/news/security/showArticle.jhtml?articleID=196603888

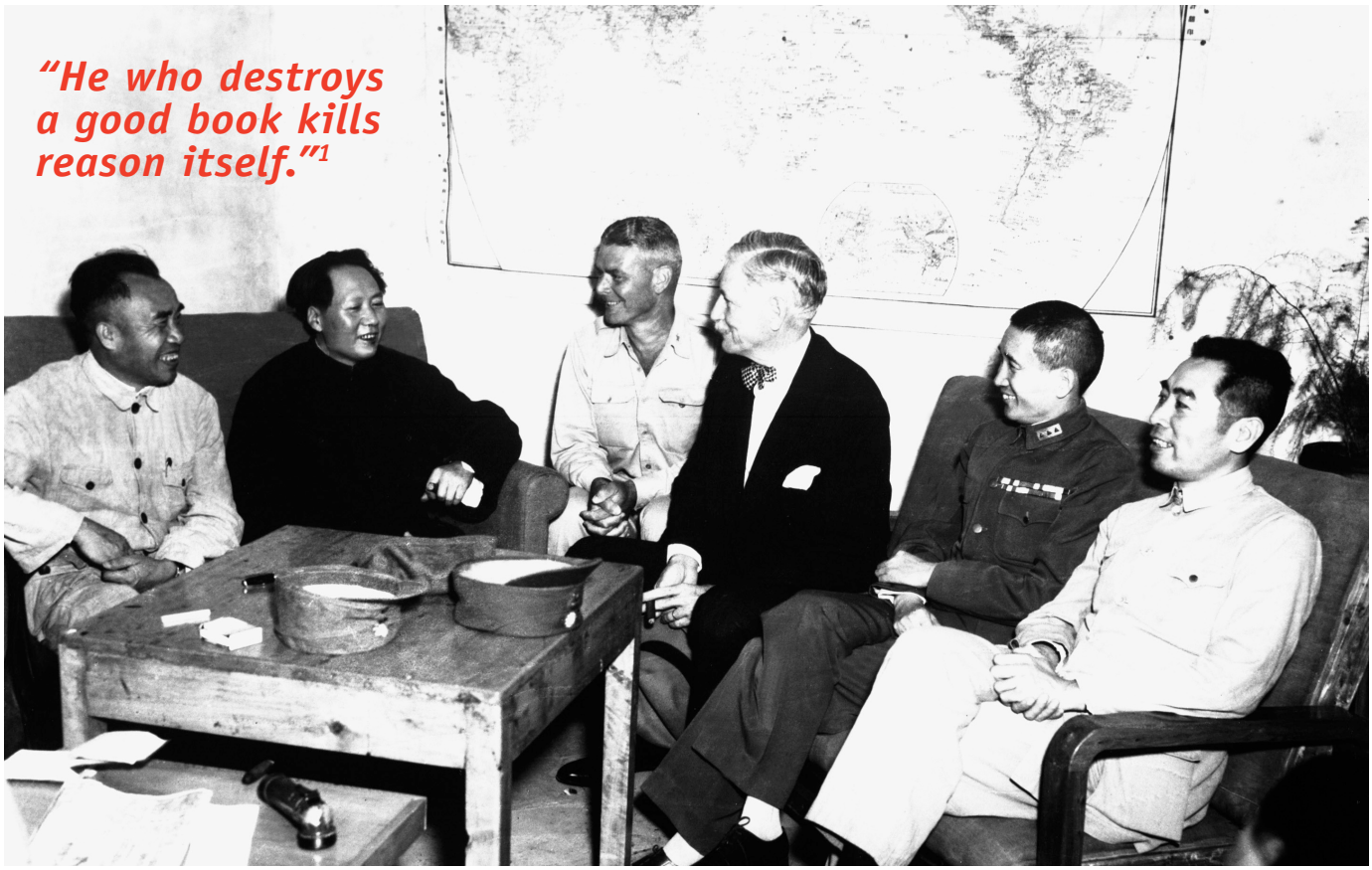
12 Thomas Claburn, "Fannie Mae Contractor Indicted For Logic Bomb." *Information Week*, January 29, 2009 Accessed at: http://www.informationweek.com/news/security/management/showArticle.jhtml? articleID=212903521

13 Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid." *CNN,* September 26, 2007. Accessed at: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

14 The BLU-114/B is a non-lethal munition used to disrupt electrical systems. The device is also known as the "soft bomb," "graphite bomb" and "blackout bomb."

15 60 Minutes "Sabotaging The System." *CBS*, November 8, 2009. Accessed at: http://www.cbsnews.com/video/watch/?id=5578986

Burn the Books:
What China's decision on Google reveals about the PRC



Conference at Yenan Communist Headquarters before Mao Tze Tung, chairman, left for Chungking meeting. Central figures are U.S. Ambassador Patrick J. Hurley, Col. I.V. Yeaton, U.S. Army Observer, and Mao Tze Tung. August 27, 1945. *T5c. Frayne. (Army)*

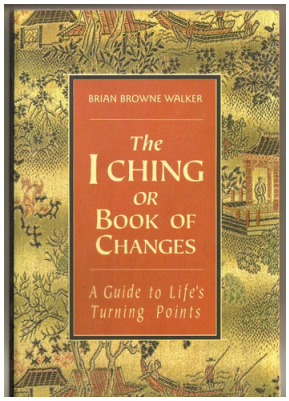
By Carson Thomas Checketts, J.D.

"Discipline that stifles creativity and initiative should be abolished. It is a dangerous policy to forbid people to meet face to face with false, ugly and antagonistic things, such a policy would lead to people being incapable of facing the outside world, and unable to meet the challenge of a rival."
—Mao

"When ideas fail, words come in very handy."
—Goethe

Something or someone in the PRC has failed. China's attempts to attack Google betray a deep discomfort with the PRC's own decision to ban the worlds leading technology leader from its shores. Perhaps, given Goethe's insight, it's fair to say that the PRC's "ideas" have failed so it is now resorting to all it has left: words. Despite a widely shared international consensus among academics[2] that an industrial revolution remains hollow without a transition to a services and information based economy, China has turned its back on its own modernization.

This change has many implications for the world, but perhaps the most significant is that the Google decision shows who really holds the cards in the PRC's inner circle. It would appear the less educated military may have moved from a position of moderate influence into the inner circle, where their paranoia has apparently convinced the PRC that technology is what ancients called



a "Greek gift," intended to harm rather than enlighten the recipient. It is too often forgotten that the catalyst for this conflict was a sophisticated hacking attack launched from within China. After NSA and Google teamed up for this investigation (both sought to make it clear this joint venture had only one purpose: identify the nation and or individuals/organizations behind the attempted corporate theft), it was concluded the attacks likely point of origin was the Chinese research universities that maintain the great firewall which may or may not have been tasked as a "proxy" attack by the PRC.[3] To make the attack on Google even more pugnacious, there are signs that the PRC may have "planted" or recruited a Google employee to amplify the sophistication of the attack from inside Google's headquarters. While it's difficult to put a dollar amount on the value of Google's Source Code, the code is by most estimation the distinguishing element that makes Google unique. In other words, if Google's software and search programming code were stolen whole cloth, there would be nothing preventing the PRC from creating its own "Google." While there are many political, legal and corporate ramifications for such a masterfully executed conspiracy of grand theft this paper will focus on the cultural, philosophical and ideological trends in China that may help the rest of the world understand why the PRC would plan such an egregious assault on a private corporation. This failure in competent leadership can only be explained by a change in the inner circle of China's highest ruling body, the politburo.

It has been observed that you can gauge the competence and virtue of a nations leaders by evaluating their ability to honor their nations best traditions. Every nation including the U.S. and China possess in their histories former citizens, presidents and leaders who represent the highest caliber of their nation's cumulative brain trust. These Sages of the past were able to speak the "truth." Not from a myopic perspective limited to their own time and culture, but as "galvanized rods" (Emerson) they spoke the truth of their generation and shed light on their nations past, present and future potential.

As China and Google grapple with the consequences of the PRC's attack, it occurred to me that the conflict may best be evaluated not by Western standards, but by the standards of China's great philosophers which laid out the etymology and cultural values in Chinese culture. However, as I worked my way from Confucius to Mao, it became clear that some of China's greatest philosophers and their works (Mao in particular) were informed and enlightened by some of Europe's greatest minds. As a result, this paper explores a wider angle on what both Chinese and European philosophers may say about the Google/China problem, with emphasis on China's most gifted minds.

China has produced a lion share of our world's collective wisdom; however, no great philosophers have emerged since the PRC came into power.[4] What can be made of this relative "dry spell" in China? After all, the mysticism, depth and power of China's religious and philosophical culture have long been the fascination of many western minds. People from all over the world travel to China for advanced acupuncture, herbal remedies and to have the worlds best I-Ching oracles lend some sage insight into their lives. Perhaps the PRC's political leadership has become too disconnected from the people it governs. The PRC appears increasingly disconnected and fearful of modern technology. This fear risks cutting China off from the development that has lifted modern nations from the filth of industrial factories to the height of intellectual and technological prowess. It was the great philosopher and play write Oscar Wilde who stated: "We are all in the gutter, but some of us are looking at the stars."[5] Perhaps it is not too far a stretch to observe that by banning the world's largest wealth of digital knowledge known to man, the PRC has decided the gutter of 20th century factories is good enough for its people. Such a decision defies not only the extraordinary capabilities of China's people and potential, but also disregards the prescient insights of its greatest philosophers. It was Chairman Mao himself who stated that there was "nothing to fear" from intellectuals; instead he warned, "Shall there be only peace and no trouble…it would lead to mental sluggishness."[6]

I. Philosophy in China: From Early Promise to Modern Decline

If there were a "Plato of Asia" it would probably be Confucius. Confucius (Kongfuzi/K'ung Fu-Tzu), like Plato, represents both the flexibility and stoic nature of his time. His work reflecting both a commitment to social norms and a desire to encourage citizens to educate themselves to attain the highest virtue possible. This dichotomy is replete throughout Confucius' work, which argues on one hand that the virtue of Li requires adaptability to each different situation that confronts an individual, while insisting on the other that "rectification of names" (zhengming, or cheng ming) by the wider society must be enforced in order to "enforce li." In other words, society should choose values, have a means to enforce (or encourage) those values and remain flexible to "jen" (human heartedness) which is the highest virtue any man can attain. This tension within Confucian philosophy between strict adherence to social norms and independently enlightened people can still be seen in some aspects of Chinese culture. Human-heartedness or jen (which is also expressed as "ren") has been interpreted by Professor Liang Sou-ming as spontaneous intuition, which results in moral decisions.[7] Confucius was known for his willingness to accept students who were at all stages of their intellectual and personal journeys. The "jen" which he taught was not reserved for a ruling elite, but was presented as something that should be a universal goal for all people. The more authoritarian aspects of Confucius are given less attention and space in his own written work than the broader themes of education and human progress.

In modern terms we would consider the strict elements of Confucius (zhengming) as a "state of emergency" that was issued by the government or military when the nation was threatened or chaotic. Confucius states that "if the society were not out of order, I would not bother to reform it."[8] Given China's decision regarding Google and this insight from Confucius, we may want to consider the degree to which the PRC perceives China as a nation as being "out of order." But there are other strands of Chinese thought that we must account for before drawing any overly broad conclusions.

U.S. Sailors aboard the dock landing ship USS Harpers Ferry (LSD 49) carry a fuel hose to a Marine Corps CH-46 Sea Stallion helicopter for refueling during flight operations March 20, 2010, in the South China Sea. *(U.S. Navy photo by Mass Communication Specialist 1st Class Geronimo Aquino/Released)*

Confucian's ideal of human heartedness was enhanced by one of China's more recent philosophers, Fung Yu-Lan who lived from 1895-1990. Yu-Lan used almost Hegelian divisions to describe four spheres of life (living). These four spheres include the innocent sphere, utilitarian sphere, moral sphere and the transcendent sphere. Yu-Lan believed that the process of education enabled men to move from one sphere to the next, ultimately reaching for the "transcendent" sphere. Yu-Lan's system of philosophy is one of the most sophisticated and comprehensive that China has produced. While it remains difficult to ascertain which European philosophers were most influential on Yu-Lan, it's hard to read Yu-Lan without viewing his fourth sphere as being related to Kant's transcendental turn. In fact, Yu-Lan has been quoted as referring to his own six major works as "the six books at the turning point."[9] Despite having worked on several Moaist and Marxist projects, Yu-Lan's self-acclaimed metaphysical turning point reads much more like a pre-Marxist expansion of Georg Hegel or Emmanual Kant than it does dialectic materialism. Were Yu-Lan actually persuaded by the Communist party, his four spheres theory would have to be inverted, much the way that Karl Marx inverted Hegel's phenomenology. In other words, the fourth sphere which represents Yu-Lan's ideal remains "transcendent." The only one of his four spheres which could be interpreted to be Marxist would be his second "utilitarian" sphere. This sphere could be seen as an endorsement of dialectic materialism and would probably support a communist form of government. However, in order to account for the hierarchy and propriety of Yu-Lan's work, this communist or utilitarian sphere of development must be seen as only the second of four steps toward progress. Yu-Lan's four spheres share an uncanny resemblance with Alain Badiou's unpublished manuscript, "La Logique des mondes." Badiou views the politics of revolution as following four steps and begins by citing ancient Chinese legalists. The four steps are: voluntarism, terror, egalitarian justice and concluding with trust in the people.[10]

The 21st century is the "virtual century" in a technological, economic, cultural and ideological sense. The difficulty China faces in banning Google in light of Yu-Lan's metaphysics is that Yu-Lan seems to adopt Hegel's preference for enlightened metaphysical philosophy that values man's quest for knowledge and enlightenment over his thirst for material objects.[11] It is of interest that Yu-Lan did serve (however briefly) as a "philosopher-adviser" to Chairman Mao's wife Jiang Qing (Chiang Ch'ing).[12] To the degree that Google and its digital resources could assist Chinese citizens in attaining Yu-Lan's transcendent fourth sphere of being, keeping Google from Chinese citizens may damage its hope of attaining super-power status. Uneducated and overly censored citizens cannot transform China from an industrial power to an information age economy. China's leaders would be wise to notice widespread enthusiasm in U.S. political parties when Google announced its likely departure. Americans and Europeans alike know something that has so far escaped the PRC's leadership: wisdom doesn't come without education and enlightened education cannot emerge without freedom. Chairman Mao made difficult decisions to ensure the unification of China's continental power; his advocacy and bold pursuit of truth exceeded all common wisdom. Those academics in the U.S. who downplay Mao's intelligence may not know that this man predicted the split of the atom before scientists had even considered weaponizing a nuclear bomb.[13] It is perhaps one of the cruel ironies of history that were Chairman Mao born in today's China he would have less intellectual freedom to write, speak and develop himself than he had over a hundred years ago. Such a reality does not bode well for China's future.

II. Heads without Bodies: What Lenin and Chinese Philosophers have in Common

While much attention is given to Mao's "Let a Hundred Flowers Bloom" speech, too little has been paid to the preceding events that made his speech necessary. In the years between 1950 and

Chinese army Gen. Xu Caihou, vice chairman of the Central Military Commission of the Chinese People's Liberation Army, presents a document from the Chinese military archives relating to the crash of a U.S. military aircraft to Secretary of Defense Robert M. Gates in October 2009 at the Pentagon. *(DoD photo by R. D. Ward/Released)*

1955, China was facing pressure to either mimic the Soviet form of communist step by step, or to forge its own path. Mao had a well-known dislike for Stalin and held only a slightly better opinion of Lenin.[14] Mao observed while speaking to the 8th Congress that the Soviet people "have abandoned Stalin and practically all of Lenin as well—with Lenin's feet gone, or perhaps with only his head left, or with one of his hands cut off."[15] Mao replied to Soviet pressure to follow the Soviet form of communism in part by cracking down on Chinese intellectuals.[16] It was only after Mao's "secret speech" deciding to take China on a different course from the Soviets, that he realized silencing critics of communism had left China with too few intellectuals. Mao's own mental sluggishness and delays in breaking from the Soviet communists left the PRC with a populous that Mao himself described as "poor and blank."[17] In stark contrast to the wisdom of past centuries the 1950s saw Chinese philosophers treated as a "black class."[18] Chinese philosophers and intellectuals have not recovered from Mao's wrath despite his own efforts to reverse himself.

Philosophical historians may wish (with the gift of hindsight) that Mao had read more Yu-Lan or Hegel and less Confucius and Marx. While it remains difficult to ascertain the depth of Yu-Lan's involvement in Mao's philosophy, certain components of both Yu-Lan's philosophy as well as Hegel can be seen in Mao's own thought. Perhaps one explanation of Mao's preference for certain philosophers is that Yu-Lan was a contemporary whose life-span covered a large portion of Mao's own life. Mao could be summarized as the first well-known Asian dialectic materialist. His early preference for Marx, Engels, Lenin and Stalin explains in part why he interpreted a cynical view of Hegel's work, which was the catalyst for Marx and Engel's project. Since many of the books available to Mao both as a young adult and later in life were provided by Russia, his preference for materialism is perhaps nothing but a historic contingency. Mao was born into a deeply divided and fractured China, while his philosophy espoused dialectic materialism from Russia and Germany, his own biography reads like a Hegelian or Nietszchean champion of national idealism triumphing over rote materialists. Mao was a gifted philosopher, and if he adopted the official line of Russian dialectics, he also amplified and altered important aspects of it to make substantial contributions to philosophical thought. Mao was more interested in the metaphysical component of dialectics and its implications for political and strategic leadership than he was in details about material production. One of Mao's most significant achievements was to interpret Russian dialectics through the perspective of Chinese Daoism. Marx believed that "everything divides into two" (yi fen wei er fen wei erh) but is re-unified in the "unity of opposites."[19] In this important sense Mao seems to hold metaphysics that resemble Yu-Lan, subordinating material matters to idealistic conceptualizations of

reality for pragmatic considerations. This preference is expressed in Mao's "Let a Hundred Flowers Bloom," speech and his preference for resolving contradictions by determining the dominant (as opposed to secondary) contradiction. Mao's evaluative form of critiquing each contradiction that arises implies a human sense of proprietary knowledge that enables distinguishing theories and contradictions correctly. In other words, Mao espouses Marx but walks Hegel. His theory of knowledge reveals his rather enlightened perspective: "Discover truth through practice, and again through practice verify and develop truth. Start from perceptual knowledge; then start from rational knowledge and actively guide revolutionary practice to change both the subjective and the objective world. Practice knowledge, again practice, and again knowledge. This form repeats itself in endless cycles, and with each cycle the content of practice and knowledge rises to a higher level. Such is the whole of dialectical-materialist theory of knowledge, and such is the dialectical-materialist theory of the unity of knowing and doing."[20]

It remains difficult to understand how Mao would espouse such loyalty to the materialists while his own theory of knowledge clearly surpasses it. Mao's working-class background can perhaps shed some light as to his preference for focusing on material conditions, but his theory of knowledge has an edge to it that seems to exceed the coordinates of materialism. To the degree that Mao valued materialism he may have more in common with Heidegger than with Marx, or perhaps his work like most great philosophers is a synthesis of both concluding with a Hegelian triumph. Heidegger described the history of the "west" (and in some sense the whole world) as a "gradual estrangement from being."[21]

Heidegger's insight allows us to perceive Mao from a slightly different angle where human experience determines the initial coordinates of a theory, but which "rise to a higher level" as Mao claims. With the aid of Heidegger, Mao appears closer to Fung Yu-Lan than he does Confucius. To the degree we are tempted to evaluate his political efforts towards Chinese unification we would be remiss if we didn't mention Hegel's theory of history marching towards enlightenment. In short, Mao may be demonstrating a principle acknowledged by the great French philosopher Albert Camus, who astutely noted that an individual is the "aggregate of the voices of our whole generation."[22]

One selection of Mao's theory of knowledge is both more relevant and more complex than it appears on first glance. Mao suggests we "start from perceptual knowledge; then start from rational knowledge and actively guide revolutionary practice to change both the subjective and the objective world." In order to better understand the depth of his observation I have broken it down to each step of what I term Mao's "active learning," below:

Start from perceptual knowledge. This first step seems to reference the empirical world that can be perceived by the human senses.

Then start from rational knowledge. This step implies any prior knowledge.

Actively guide revolutionary practice. This step acknowledges the role of the state in allowing and guiding the persistent revolutionary impulses of the society.

Change both the subjective and objective world. This is Mao's most profound insight where he highlights the need for dynamic internal change both within the individual and in the external society.

The fourth step of Mao's theory of knowledge implicitly incorporates Yu-Lan's and Confucian's conception of transcendent enlightenment. The spark of "wisdom" within ancient Chinese emperors was said to be so powerful as to change the weather when the Emperor would turn to face south. There is also a rather explicit temporal reference in Mao's fourth step, which implies the omni-directionality of knowledge. When transcendental knowledge emerges, wisdom "occurs" in both the past, present and future, lending the individual with access to "heavens will," or the power to make his subjective reality sufficiently virtuous to exude simultaneous correspondence in the external world. And here in the "mysterious path" (between the metal and water element in Chinese ontology and acupuncture[23]) lies one of the deepest similarities between Chinese mysticism and ancient mythology where Prometheus by stealing the fire of the Gods is said to have both created and enlightened man, all in one moment.[24] Mao's theory of knowledge and western conceptions of knowledge both share one strikingly common connection with the dominant theme of technological development: both build slowly and manifest in ways that alter our collective understanding of the past, present and future. Or as Slavoj Zizek states, "the past will be effected by discoveries we make in the future."

Such an observation makes outsiders wish that China had a few enlightened philosophers on hand to advise it on both Mao's philosophy and its recent Google decision. Up until this month, China demonstrated at least one "greatness" as defined by Pascal: "A man (nation) does not show his greatness by being at one extremity, but rather by touching both at once." If we are to look at Google as the embodiment of cutting edge 21st century technology, then it becomes clear that China has quite literally banned the most advanced future developments and has instead reverted to old Marxian materialism. Such a decision cuts against China's collective history represented by its own philosophers and shows a startling turn away from Mao's pragmatic philosophy of developing knowledge. However, since we are here in 2010 and the PRC has chosen to ignore the greatest insights of its former leaders, we may need to turn to one of Europe's most prolific philosophers to see why the PRC has been unable to accommodate Google. Slavoj Zizek observed in his seminal work the Parallax View that the grandest failure of all communist nations is their "narrative failure." "The narrative failure, the impossibility of constructing a 'good story', which indicates a more fundamental social failure."[25] In the present case it would appear that the PRC has failed its own people by demonstrating an unwillingness to connect them with the world's biggest knowledge base. The rather silly fear of pornography and a two decades old picture of a man in front of a tank are not enough to harm or undermine Chinese citizens who have advanced well beyond such mundane material. The PRC's hypervigilance in chopping its people off from wisdom is reminiscent of the worst parts of Confucius (later rejected by Fung Yu-Lan and Mao) who once sarcastically stated: "Men of integrity in my community are different. The father conceals for his son and the son for his father, therein integrity is found."[26]

From our modern philosophical coordinates it would be fair to observe that the PRC is attempting a Lacanian "short-circuit."

"I have frequently stated that if the culture of a nation is to advance, society must have considerable respect for the scholar, allowing him to make a living from his intellectual pursuit without fear..."[44]

—Liang Ch'i-ch'ao

With one hand it claims to be "shielding" its people, while what it really seeks to do is to put their populous into a deep intellectual slumber, to make them subject to material conditions and cut them off from the intellectual ideals that are the engine of any great culture. Poorly educated investors in London and New York are already betting on the "expanded revenue" of Baidu, Google's rival in China. As an individual who believes in certain historic trends, I am inclined to think these investors bet on the survival of 18th and 19th century dialectic materialism will ultimately wish they had invested elsewhere. Chairman Mao, Confucius, Georg Hegel and Fung Yu-Lan all advocated for the advancement of individual wisdom and knowledge. Google's departure and the PRC's suspicion of technology will undoubtedly make education more difficult. Were these philosophers to be investing in a company today, it is likely they would be buying Google's stock and chastising the PRC for fearing the only true engine of lasting economic growth: their own people.

III. 21st Century Internet: Soldier's Cyber-War or Public Square for Transnational Civil Society?

While it would be easy to criticize the PRC's censorship of information technology without reference to policy in our own country, understanding our nations challenges may help both nations better understand one another. 2010 was a watermark year for the U.S. and its position on information technology. The 1990s ushered in what is widely considered the "information age." As with every world changing phenomena the information age was (and in some senses still is) very much in need of intellectual and doctrinal exploration. Mapping the impact of the virtual century's depth and breadth fell first to the military. Who, despite all criticism, is often the first department in the U.S. government to appreciate the weight and value of new technology. In an effort to ensure the expansion of the military's relevance to the new century, the Air Force decided the information age exposed vulnerabilities that needed to be defended and not inconsequentially militarized. The concept of "cyber-war" emerged first from RAND who was paid by the Air Force, and spread from there.[27] Knowing that Congress and the American people don't go to war without provocation, the Air Force used its own discretionary funding to incite fear of a global cyber-arms race overseas. It is my *own* opinion that such mismanagement of American tax-dollars has not been seen since the epistemologically flawed "intelligence" used as justification to "preemptively" invade Iraq.

Until 2010 the U.S. military's response to the rapid advancement of technology has been informed primarily by 18th and 19th century perspectives on the advance of weapons technology. Military officers imitating the form (but not the insight or wisdom) of scholars wrote entire books comparing the evolution of the sword and crossbow to something as harmless as e-mail messages.[28] Perhaps the only wisdom in these books worth highlighting is the implicit acknowledgment among military leaders that the 21st century looks "too peaceful," to justify the scope of the U.S. military's present funding. In hindsight, these fears of a war in cyberspace appear to have only slightly greater validity than the fears of widespread computer failures in 1999 as we approached "Y2K." Since the end of the world did not accompany the arrival of the new century, ideologically motivated zealots thought they would plan a new war with similarly founded logic.[29] For complex political reasons (that include NSA's ill-informed political interference), there were substantial delays in President Obama choosing a White House Cyber-Czar to oversee U.S. cyber policy.

Mr. Rod Beckstrom, former Director of the National Cyber Security Center, noted that NSA also interfered with DHS civilian cybersecurity efforts. In Mr. Beckstrom's resignation letter in March of 2009 he stated: "NSA effectively controls DHS cyber efforts through detailees technology insertions, and the proposed move of NPPD and the NCSC to a Fort Meade NSA facility." Mr. Beckstrom also notes that "the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization (either directly or indirectly). During my time as director we have been unwilling to subjugate the NCSC underneath the NSA. Instead, we advocated a model where there is a credible civilian government cybersecurity capability which interfaces with, but is not controlled by, the NSA."

The militaries strangle-hold on U.S. cyber-policy officially ended the day President Obama chose his Cyber-Czar, who has since spoken a truth that well-informed leaders knew all along: "there is no war in cyberspace."[30] The U.S. position on information technology was further amplified and given legal weight on Jan. 21, 2010 by Secretary of State Hillary Clinton, who cited the universal right acknowledged by the United Nations to "seek, receive and impart information and ideas through any media and regardless of frontiers."[31]

While cyber-espionage and computer network attack (CNA) will likely become a standard component of national power, there is a robust diplomatic effort underway to ensure that we do not have a global cyber-arms race that would re-create the negative consequences of the Cold War. Senior military leadership in the U.S. has acknowledged that the military must resist the temptation to dominate U.S. foreign policy.[32] In this regard the U.S. military is moving closer towards a vision of the military as an enabler of civil society rather than a competitor with it. The international movement towards CIMIC (civil military cooperation) has been endorsed by leading intellectuals in Germany and India. The keystone of a peaceful 21st century will be allowing the peaceful progress of civil society and technology while resisting factions who desire to militarize every modern development at the expense of modern civil society. [33]

Perhaps the greatest risk China and the U.S. face over the next 100 years is determining the amount of weight to give the "insight" of military and intelligence leaders who having been trained and paid to be paranoid and xenophobic duly oblige the people who pay their salaries by seeking to scare them. This risk is amplified

by the hidden world of espionage and subversion where nations who are rightfully fearful of a grand alliance between China and the U.S. work to stoke the flames of war and suspicion. It was the great military philosopher Sun-Tzu who recommended carrying on "alliances with strong countries (so) your enemies won't dare plot against you," and to attack the alliances of your enemies so they will fall apart.[34] While China is rumored (with or without justification) to fear the excess influence of neo-conservatives and hawks in the United States, it provides the world plenty of reasons to fear the ideological and mundane influence of its own military and intelligence services. It is a historic and universal truth of every nation that "a foreign policy conducted by military men according to the rules of the military art can only end in war; 'for what we prepare for is what we shall get.'"[35]

If the two nations are to forge a 21st century filled with economic, intellectual and philosophical prosperity, it will be made possible by the intellectual, political and corporate relationships between the two behemoth nations. The ideological appropriation of U.S. and European actions by the PRC's military and intelligence services betray ignorance as to who the most valued citizens and leaders are in the United States. Every step China takes towards warfare with Taiwan, harassment in Hong Kong and the humiliation of Tibet strengthens European, American and Indian voices that believe a war with China to be inevitable. China's unwillingness to accommodate digital knowledge and connectivity embodied in Google sent shockwaves through the world's capitals, as every nation had to consider what it would mean should Leninist and Marxist military men govern China's emerging power and the inner circle of the politburo. If even the "keys" to knowledge and enlightenment (embodied in part in Google and international corporations) are barred from China's shores, the world cannot hope for a peaceful 21st century.

This leaves all supporters of a peaceful 21st century in a rather unenviable predicament. While Google is not closely related or connected with the U.S. Government, it has come to embody the "symbol" of independence of thought and free speech that modern cultures value. It is worth noting that the PRC is not the only government that Google has angered. Since 2001 Google has consistently refused to turn over all the data that the U.S. government requests on what the most popular internet searches are in the U.S. While outside observers believe U.S. corporations are often in collusion with the government, the political reality is quite different. Using political relationships with the U.S. Congress and Supreme Court, international corporations like Google are given wide latitude and immunity to behave with the full rights of a living human being. This reality led to a confrontation between President Obama and the U.S. Supreme Court during the President's State of the Union address. The President publicly challenged the wide latitude the Supreme Court gives corporations to spend money on campaigns and unduly influence politics. This corporate independence continues to cause the U.S. legal migraines, but gives the world access to something they would not otherwise have: access to the worlds most ingenious technological developments as they happen, often in real time.

IV. Building Knowledge To Maintain Peace[36]

"There is a historical vortex at the center of our thought which drags it (thought) out of true."[37]

As every nation around the world works to develop their policies regarding the profound power of information technology, they would be wise to remember that despite the ideologues in their own countries they are not capable of electing or even creating a "new people," but it is rather the people who choose whether to work in support or opposition to their government.[38] For all its failings, the PRC is not without cause for its concern for the influence of intellectuals. It was Mario Palmieri who noted in his *Philosophy of Fascism* "a religion or a philosophy lies at the base of every revolution." What Palmieri failed to account for is the middle path that lies between revolution and enlightenment. As both Nazi Germany and the former Soviet Union discovered, economic prosperity and the intellectual brilliance that fuels it cannot survive in a closed society.[39] Chairman Mao warned Chinese leaders that it was dangerous to squelch dissent, stating: "Fear is no solution. The more afraid you are, the more ghosts will come to visit you…I think that whoever wants to cause trouble should be allowed to so for as long as he wants."[40]

Mao's warning about restricting citizens' freedom sounds like an echo of Hegel's profound insight when he stated that that "there are in tragedy two standards of right, the daylight standards of Apollo and the underworld standards of the Furies."[41] The U.S. learned a painful lesson in the first year of the new century that China has yet to learn. There is nothing predictable about the 21st century. The biggest threats to China, the U.S. and all modern nations are not from other states but from radical, coercive and persuasive networks of ideologues. These zealots of every political stripe and in every nation prey upon the uneducated, the obsessive and those of weak intellect. The threat of domestic and transnational terrorist networks extends to every nation in the world. The most effective option modern nations have is to educate, liberate and care for their people or eventually become the target of their wrath. Nations would be wise to foster an international community where the synergies of enlightenment contain the furies of ignorance. China's ancient philosophy may be critically important to this effort.

One of China's more modern philosophers Liang Ch'i-ch'ao recognized the yet un-tapped potential of Chinese philosophy and left some rather enlightened insight behind for future generations of Chinese and international intellectuals. In the interest of being true to his insight and in acknowledgment that I have yet to have the time and space necessary to extract the wisdom of China's intellectual treasures, I have copied his recommendations below, first published in English in 1959.[42] As one final note it is perhaps worth noting that China's Renaissance in philosophy between 1736-1820 afforded well-compensated Chinese philosophers only a fraction of the time and support required to organize more than 3,000 years of Chinese philosophy. China's ancient works of philosophy remain one of the few gold mines left for modern intellectuals to explore. In a sincere effort by the author to be a catalyst for renewed efforts in a Sino-American exploration of Chinese philosophy and its applicability to the 21st century, I have launched a website and project titled *Chien* after the I-Ching hexagram that was the catalyst for this paper.[43]

This brief review of Chinese philosophers reveals a latent cultural and political tension within the PRC. On one hand, China's great philosophers have advocated for the education and enlight-

enment of their own citizens, a noble goal which coincides with all modern societies. On the other hand, the PRC still suffers from the corrosive unthought of Marxism, which values the material over the ideal and the coercive over the natural. If the Politburo had faith in its own citizens' creativity and scientific advancements it would not have felt compelled to plan and execute a cyber-attack against Google. This leaves us with a rather complex puzzle. If the Politburo has no faith in its own people's creative potential, why do international investors?

Perhaps the most important component of this puzzle is the PRC's quixotic relationship with Marxism. It is difficult for citizens living in a closed system to effectively critique and reach above the confines of a society so focused on squelching dissenting views. Engel's believed that there was no freedom outside of historically driven necessity. The PRC may feel compelled to seize control of technology in order to ensure that it cannot serve to undermine its authority. And here the PRC suffers from a related problem; the more the PRC engages in desperate acts to ensure its survival the more backwards and dysfunctional it appears to its own citizens and the world at large. In democratic nations the blame for national troubles is split at least once and often multiple times between culpable parties. In modern democratic nations, citizens dismay at corruption, excessive taxes or a lack of healthcare, invest time aligning themselves with political parties and can work to advocate for values that help society progress. In China, almost every problem citizens encounter can be traced back to only one place: the single party rule of the Communists. For this reason alone, the PRC's monopoly on political power is not likely to survive the 21st century. If China's leaders were to show a modicum of faith in their people, they would trust them with popular elections and even a two-party system. Whether this system featured a Socialist Party to compete with the Communist Party or a more liberal party could be chosen by the PRC. Splitting accountability and dividing ideologies would be in line with Mao's theory of knowledge. Mao sincerely believed that contradictions in politics, war and peace were best resolved by active dialectic debates by informed parties. Such a move would have the added benefit of freeing China's intellectuals to critique and improve something that is currently not allowed: the effectiveness of their own government.

"Poverty increases insofar as freedom retreats throughout the world, and vice versa. And if this cruel century has taught us anything at all, it has taught that the economic revolution must be free just as liberation must include the economic. The oppressed want to be liberated not only from their hunger but also from their masters. They are well aware that they will be effectively freed of hunger only when they hold their masters, all their masters, at bay." [45]

—Albert Camus

The PRC's effort to steal Google's technology has given the world an image of the PRC that will not soon be forgotten. One of China's more recent philosophers Liang Ch'i-ch'ao ended his seminal work by advising future Chinese generations to "absorb as much new culture from outside as possible," while warning that China should never sacrifice its own unique heritage. Liang Ch'i-ch'ao believed that China would allow the sciences of Europe and America to "flow steadily" into China in a way that would allow China to become a first-class scientific and cultural leader. Liang believed in the potential of a cooperative Sino-American culture that would become generative, enabling both societies to advance the development of knowledge. The PRC's attempted robbery of Google makes such cooperation less likely and raises serious questions about how the politburo could have made such an illegal and strategic miscalculation.

It is time for the leadership of the PRC to prove to its own people and the world that China's leadership is capable of honoring their highest traditions and begin evolving with the 21st century. To the degree the PRC still views the world from Engel's and Marx's disordered ontology, they will find themselves unable to keep up with the advancement of modern culture and the technology that accelerates it. If the joint US/China victory over the Soviet Union, the defeat of Hitler's Germany and the World War II defeat of Imperial Japan is not enough to demonstrate the futility of single party rule to China's leadership, it seems likely that the advancements of 21st century knowledge will.

ENDNOTES

1 See: "Areopagitica," by John Milton, Nov. 25 1644.
2 One of Europe's most widely respected philosophers Slavoj Zizek describes this transition this way: "The central event of the 20th century is the overthrow of matter. In technology, economics and the politics of nations, wealth in the form of physical resources is steadily declining in value and significance. The powers of mind are everywhere ascendant over the brute force of things." See: Parallax View p. 179.
3 The two universities reported were Shanghai Jiaotong University and the Lanxiang Vocational School. More recent supports suggest preparations for the attack may have started as early as April of 2009. Note that Google did not announce their knowledge (if any existed) of the attack(s) until January 12, 2010.
4 See: "Politics among Nations: The Struggle for Power and Peace," by Hans. J. Morgenthan, 1950. Specifically p. 409: "The Chinese people have a tradition of respect for learning superior to that of any other people, and they can look back upon a history of cultural attainments longer than any other and at least as creative. These high qualities of education and culture have made the Chinese look with contempt on the profession of the soldier as well as upon the members of all other nations, which at the beginning of the nineteenth century were still regarded as barbarian vassals of the Chinese emperor. Yet they have not made the Chinese people less nationalistic and more peaceful."
5 See: Oxford Dictionary of Quotations, Second edition 1953 quoting Oscar Wilde, p. 569.
6 See: "Mao a Life," by Phillip Short, p. 455-460.
7 See: "Eastern and Western Civilizations and Their Philosophies," by Professor Liang Sou-ming, 1922, and "Great Thinkers of the Eastern World," p. 4.
8 Id. at 7.
9 Id. At 149.
10 Parallax View, Slavoj Zizek, p. 379.

11 For a well reasoned critique of where Hegel's philosophy was inverted (and subverted) by Marx and Engels see: "Truth and Reality in Marx and Hegel a Reassessment," by Czeslaw Propkopczyk, 1980. The author notes that Engels rather dishonestly portrayed Feuerbach's interpretation of Hegel as supporting materialism while Feuerbach interpreted Hegel's more profound insights as being consistent with idealism. Yu-Lan's hierarchies between the four spheres signal his wisdom in seeing (and avoiding) Engel's intellectual and ideologically motivated trap.

12 Id. At 148. Note, it is also reported that Mr. Fung Yu-Lan was also a member of Chinese People's Political Consultative Conference when he died in 1990.

13 See: Slavoj Zizek.

14 See: "Mao a Life," by Phillip Short, p. 449.

15 Id. P. 452.

16 Id. P. 452.

17 Id. P. 488.

18 Id. P. 453.

19 Id. P. 143.

20 Id p. 144.

21 See: "Time of Need: Forms of Imagination in the Twentieth Century," William Barrett 1972. P. 53.

22 Id. p. 52.

23 See: "Nourishing Destiny," by Lonny S. Jarrett.

24 See: "Cosmos and Psyche," Richard Tarnas.

25 See: Parallax View, p. 315.

26 "Great Thinkers of the Eastern World," p. 4, also XIII, 18.

27 The RAND Corporation and its stratagems were also key to the expansion of the Vietnam War.

28 See: "Strategic Warfare in Cyberspace," by Mr. Greggory Rattray. It is worth noting that senior military leadership is rather astutely aware of uniformed service-members inability or unwillingness to think strategically. See: Joint Forces Quarterly, "Strategists and Strategy," Issue 55, 4th Quarter 2009 published by the National Defense University. See Also: Nietzsche who noted quite accurately over a century ago: "Uniform" one calls what they wear: would that what it conceals were not uniform! You should have eyes that always seek an enemy—your enemy. And some of you hate at first sight. Your enemy you shall seek, your war you shall wage—for your thoughts. To you I do not recommend work but struggle." See: "Thus Spoke Zarathustra," p. 159. Book not in author's possession, quoted using Google Books: http://books.google.com/. Nietzsche's point reveals the degree to which military men and women are forced in true Marxist fashion to subordinate their intellect to the material conditions of their labors. This feature of military service was observed in 1788 by one of America's founding fathers Thomas Jefferson, who observed: "Breaking men to military discipline, is breaking their spirits to principles of passive obedience." See: "The Clash of Political Ideals," by Albert R. Chandler, 1940 p. 52.

29 It is here worth noting that whether "cyber-weapons" are or do become a strategic threat to the U.S., we should not rely on cyber armaments for our security. It has been observed, "Complacency, derived from reliance on some presumably impregnable main weapons system or defensive line, is a fatal trap. If democracies have an inherent strategic weakness, it is a proclivity toward such complacency." See: "On Political War," by Paul A. Smith, Jr. published by the National Defense University, 1989. The author would like to remind readers that investment in kinetic armaments (even if working properly) have but one use, while investments in intellectual capital can be used towards any and all ends deemed worthy of pursuit. Such observations speak to the need for scholarship over weapons and objectivity without bias.

30 See: Wired Magazine: http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

31 See: http://www.state.gov/secretary/rm/2010/01/135519.htm

32 See: Admiral Mike Mullen, Speech at Kansas State University, March 3, 2010, stating: "My fear, quite frankly, is that we aren't moving fast enough in this regard. U.S. foreign policy is still too dominated by the military, too dependent upon the generals and admirals who lead our major overseas commands. It's one thing to be able and willing to serve as emergency responders; quite another to always have to be the fire chief."

33 See: "Building a Transnational Civil Society," specifically an essay by Gerhard J. Klose titled "The Role of the Military in a Changing World." See also: "Rescuing the Future," by Jagat S. Mehta who endorses a uniquely Indian view of enlightened internationalism where "socio-economic growth and political participation are more critical for national strength than military might." p. 127. Mr. Mehta believes the real challenge of the 21st century is to "find the alchemy of trust in the web of bilateral relations, which have got so vitiated because of a search for security."

34 See: "The Art of War," by Sun Tzu, p. 36-37 quoting Meng shi and Wang Xi.

35 See: "Politics among Nations: The Struggle for Power and Peace," by Hans. J. Morgenthan, 1950. P. 443.

36 Liang Ch'i-ch'ao noted that China has in past centuries lost part of its greatest thinkers wisdom by keeping them so secret that they could not be passed to the next generation. See: p. 121.

37 See: "After Theory," by Terry Eagleton, p. 7. To understand the weight and profound nature of Eagleton's insight it is worth quoting Carl Jung, himself a student of Chinese philosophy who stated, "consciousness is still in an experimental state."

38 See: "Violence," by Slavoj Zizek, quoting Michael Wood who stated: "In a famous poem, written in East Germany in 1953, Brecht quotes a contemporary as saying that the people have lost the trust of the government. Would it not therefore be easier, Brecht slyly asks, to dissolve the people and have the government elect another one? Saramago's novel is a parable of what happens when neither government nor people can be dissolved?" at p. 215.

39 See: "The Open Society and its Enemies," by Karl Popper.

40 "Mao a Life," by Phillip Short, p. 459.

41 Hegel, Phenomenology of Spirit, Book VII section 738. To fully understand Hegel's point one should also note sections 739-740: "Zeus is presented as the ultimate reconciler and unity of the two standards. Both forces are equally right and wrong, and their struggle ends in the death of the individual concerned, or his absolution from guilt. Both then vanish in the calm balance of the ethical order." Hegel's insight is helpful in that the objective position of "right" is one existing simultaneously in three perspectives, first that of Apollo, the god of law and the sun, second, as the night-time equalizers of the furies who stabilized or enforced oaths and promises with nefarious means, and finally in Zeus who represents the stabilizing actor who brings the balance. The brilliance of Hegel's context is that that each actor is necessary to bring about a stable international order. Apollo, representing logic, order and symbolization brings order to society, or light to darkness, through organization and legal structure. These could be seen as our legal system and international agreements. The furies bring balance to the system by enforcing the oaths taken on Apollo's watch and agreements made in the cover of night. The furies metaphysical position exists outside of the established order, yet maintains supportive of the system. The furies are best seen as the animus mundus (or passions) of the people, which must be allowed expression, or they will explode into the open, thus de-stabilizing nations and harmony. And finally, Zeus who orchestrates the instruments, which bring balance to universal order, completes the triangle by utilizing both. This symbolic triad is not intended to suggest or imply a subjectivist ethical order, but rather an expression of how the objective ethical order establishes itself through symbolization, free expression and leadership.

42 See: "Intellectual Trends in the Ch'ing Period," by Liang Ch'i-ch'ao and translated by Immanuel C.Y. HSU.

43 See: Hexagram #53, specifically line 6 (nine at the top) where the "wild goose" subordinates the mundane affairs of man and establishes correspondence and progress through effort in the "clouds." Website located at: http://chiendevelopment.typepad.com/chien-development/. Intellectuals in China, the U.S. and around the world are invited to use this website to further advance the study of Chinese philosophy. You may also email the author to post on the blog at: thechiendevelopment@gmail.com.

44 See: "Intellectual Trends in the Ch'ing Period," by Liang Ch'i-ch'ao and translated by Immanuel C.Y. HSU. P. 74.

45 Albert Camus was the intellectual leader of the French Resistance to Nazi occupied France. See: "Resistance, Rebellion and Death," p. 64.

Active Defense of Corporate Information Systems

By Mathew Borton and Samuel Liles, Purdue University Calumet

ABSTRACT

An aspect of network forensics is the detection of intrusions into the network. There is considerable amount of debate regarding the appropriate action once the responsible technician is alerted to the intrusion. Corporations will often simply shutdown the systems under attack in an effort to fail gracefully and mitigate further compromise of the system. There are some who advocate a more aggressive option. Immediate active defense in retaliation for network intrusion is a viable, though seemingly illegal option.

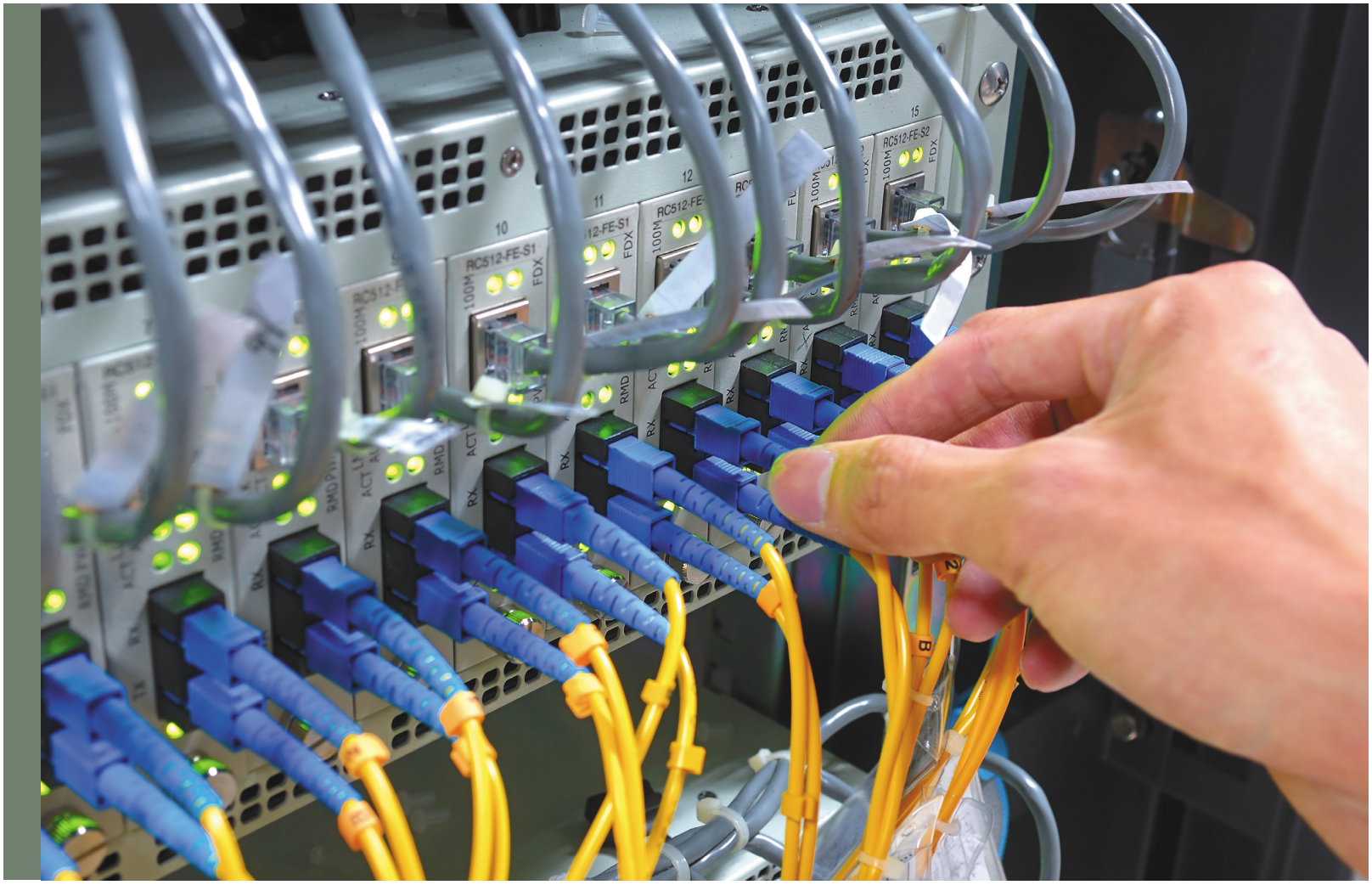
But is it illegal? The US constitution guarantees the right to self-defense, and each of the several states has their own definition of acting in self-defense. Do these rights extend to cyberspace? If so, does the precedent of corporate personhood allow a corporation to actively defend its information technology assets from cyber attack? This paper will attempt to answer these questions by reviewing US code and legal precedent.

This document is not a law review, but rather a policy recommendation directed toward corporate information technology professionals. The author hypothesizes that there is enough information to inform policy on this subject.

INTRODUCTION

Millions of dollars are spent on information technology security every year. Despite all of the firewalls, intrusion detection systems, despite the policy and training, someone with enough skill and motivation will succeed in accessing the system and stealing data or causing mayhem and destruction. Corporations currently have few legal options to respond to attacks on their information resources. It is generally held that the best practice is to mitigate as much loss and damage to the system as possible by failing gracefully. This process generally means shutting down services and systems to isolate the breach as much as possible and prevent further loss. This process also means loss of services to the corporation, which will impact the bottom line. These breaches are rarely reported to law enforcement because investigations often include the seizure and long-term impounding of hardware for forensic analysis, leaving businesses without necessary assets for long periods of time (Federal Bureau of Investigation, 2006).

The resulting loss of data costs millions of dollars annually (Federal Bureau of Investigation, 2006). Systems and services unavailable as the result of an attack cannot be used to generate revenue. Loss of reputation from the public disclosure of a successful attack translates to a loss of future business. It appears to be a lose/lose situation for those entrusted with the security of information. Cyber crime presents criminals with a relatively easy target, a potentially high payoff and a fairly low risk of consequences. In a world where information technology is ubiquitous and the flow of information drives commerce, the chance of this problem going away on its own is slim to none.



It appears that information security is a lost cause then, since it is a question of when and not if a corporation will be attacked, and an attacker need only be successful once to cause loss. It seems that passive defense of the system is the only way to resist. But is this really the case? Is the only alternative for corporations to turtle up and hope for the best, or is there another way? Can corporations fight back? The technology exists. Most information security professionals have the basic skills needed to perform the very intrusions they are charged with preventing.

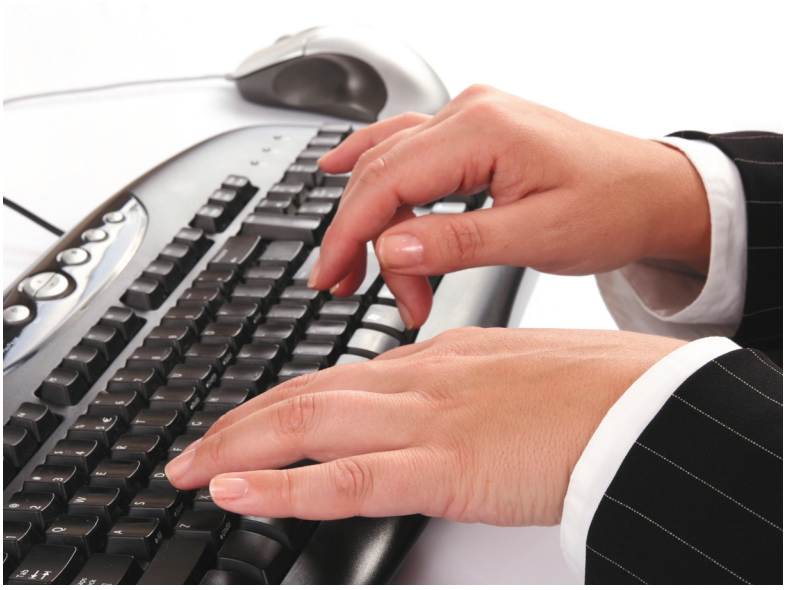
At first glance however there appears to be a huge legal roadblock to corporations actively defending their information assets. 18 USC 1030, commonly known as the computer fraud and abuse act, makes it a crime to access a computer without authorization with the intent to cause harm to the system (18 USC 1030, paragraph 5). But is this really the case, or do corporations have the right to actively defend themselves from attacks originating in cyberspace?

Since the antebellum period in the United States corporations have been given an ever-increasing number of constitutional protections normally only afforded to citizens (Million). Based on the 14th amendment, which states:

No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws (1787). The Supreme Court has at various times granted corporations protections under the first, fourth, fifth and seventh amendments (Graver, 1999, p.1, 2). If this corporate personhood grants companies these rights, then precedent indicates that it is legal for Corporations to act in self-defense as provided for by the second amendment Therefore corporations have the legal right to actively defend themselves and their assets in cyberspace.

This work assumes a United States perspective. The concept of corporate personhood as discussed in this paper is peculiar to the United States due to interpretation of the nation's constitution. The entire discussion assumes a corporation created under the laws of the United States, with assets inside the United States under attack by a criminal actor from within the United States. Further, this document assumes a corporation actively detecting an intrusion and responding immediately to the attack.

This paper concerns only companies fully incorporated under United States law. Partnerships, Limited Liability Companies and other forms of business arrangements are treated differently under the law and will not be addressed. While there are three commonly recognized theories of personhood, the nuances are irrelevant to the discussion of self defense. Related to these theories is the discussion of motives for the



creation of corporate personhood and the discussion of the intent of the fourteenth amendment. These discussions are moot, as legal precedent is the standard by which courts make decisions. Therefore the author is not concerned with the various arguments about the makeup of corporate personhood, and they will only be discussed where necessary. The discus will only consider self-defense from attacks originating from non-physical vectors. Corporate physical security, while similar in nature has a separate and better defined legal precedent. It is not necessary to discuss the issue in depth. The author appreciates the difficulty and the importance of attribution as well as proportionality of response in order to mitigate the risk of damage to innocent third parties. These issues, while problematic, have little bearing on the legal right to self-defense, and are beyond the scope of this discussion.

The author is a technologist, not an attorney. The paper is written not as legal opinion, but as a vehicle for information security professionals to discuss the active defense option as an alternative to passive loss mitigation strategies. Additionally, each of the states has its own legal code defining and limiting the use of force for self-defense. An exhaustive discussion of the nuances of each of the fifty states' laws is not possible here, though examples will be discussed.

Before the discussion continues, it is important that the idea of corporate personhood is understood. Corporate personhood is the concept that corporations are a distinct legal entity separate from the individual natural persons that have some interest or involvement in the company (Millon, 2001 p. 1). This corporate personhood is a legal fiction, a tool used by the courts to conveniently serve justice (Aljalian, 1999 p. 73). The concept then is that the corporation, despite being made up of several natural persons is treated as an individual person for legal purposes such as taxation, property ownership, contracts and tort law, criminal action and Constitutional rights. (Millon, 2001 p. 1).

Self-defense also needs to be clearly defined in order to clearly set the boundaries of this discussion. Self-defense is the use of force to prevent harm to one's self, one's property, or a third party (Neyland, 2008 p. 60). Such force, normally punishable under the individual states' legal codes, is deemed excusable if the individual has an honest and reasonable belief in the need to defend themselves.

PERSONHOOD

Much work has been done in the analysis of corporate personhood. Carl Mayer provides a detailed history of corporate personhood as it relates to the Bill of Rights. Mayer points out that while the issue of personhood started with the enactment of the fourteenth amendment, assertion of Constitutional rights by corporations was generally restricted to procedural provisions of the Bill of Rights, such as due process and double jeopardy (Mayer, 1990 p.3). It is not until the 1960s that intangible humanistic rights such as freedom of speech and right to privacy have been challenged. Mayer asserts that this is due to a change in federal regulatory standards and the way property rights were handled. During this time the public pushed for social responsibility from corporations. (Mayer, 1990 p.10, 11). While Mayer does not specifically disagree with the current trend, he fears abuse of the law beyond the original intent will raise corporations to the level of super-empowered beings with rights greater than the individual. Mayer calls for an amendment, stating that the law must favor the individual over the corporation (Mayer. 1990. P.23).

Perhaps the most important idea we get from Mayer is the idea that the desire for corporate responsibility is tied to application of constitutional rights.

Other authors have argued the same, for slightly different reasons. David Millon examines the evolution of the theories corporate personhood and discusses the debate among scholars as to which theory is correct, and how that theory applies. He looks at the corporate person from a social and economic as well as a perspective. Particularly relevant to the issue at hand is Millon's discussion of the corporate person as a citizen. Millon asserts that the corporation as a person has a social responsibility to act with the interests of society as a whole in mind. (2001, p.11, 17). Millon, quoting E. Merrick Dodd Jr., posits that while a corporation's goal is to make money for its shareholders, citizenship implies good conduct in the context of a community of others (Millon, 2001, p. 14). Since the corporation has the capacity, and it would appear the responsibility to act as a good citizen of society, it follows that it also has the legal right to defend its self from another's breach of that same social responsibility, and an interest in the well being of the society as a whole.

David Graver takes the idea a step further. Graver provides an excellent explanation of the various theories of personhood. He gives a detailed account of the three theories, fictiona,l real, and nexus or relational (1999 p. 2, 3). He goes on to point out that while the three theories of the corporate person exist, there is no standard. He calls for the development of a standard of personhood in order to more justly handle the application of rights (Graver, 1999. p 5). Graver goes on to suggest a fourth, corporeal theory of personhood. He explains that human existence, according to several schools of thought, is not based solely on identity or awareness but also on being embodied, and having both internal and external perceptions

(Graver, 1999. p. 5). He then defines the concept of the body. Graver explains corporations meet all the aspects of corporeality in that it is aware of its self; it has an outer image and can be held liable to the law. It has internal processes and functions that are not visible to the outside world (1999. p. 7). Holding to Graver's theory, a corporation is more closely related to a person then the earlier theories suggest. If this is the case, it should have the same rights as a natural person to defend its self and its property as one would defend themselves from bodily harm.

Several examples exist that demonstrate the application of the Bill of Rights to corporations Elizabeth Salisbury Warren provides an excellent discussion of the eighth amendment as it applies to corporations. She shows that each of the provisions in the amendment were meant to protect from harsh punishment regardless of the subject of the punishment (Salisbury Warren, 1996. p.5). Her example counters the issue that Mayer has with corporate personhood in that she demonstrates that the intent of the amendment was to limit the power of government rather than specifically empower the individual. She further points out that providing this right to individuals and corporations alike provides a sense of consistency and equity to the law (Salisbury Warren, 1996. p.7-9).

There are dissenting opinions. Natasha Aljalian calls into question the legal fictions that are the basis of corporate personhood. She claims that these fictions are a gross misinterpretation of the Constitution and are against the intent of the original framers (Aljalian, 1999 p. 1). She sees this process as "dangerous and alarming (Aljalian,1999 p. 2) and calls for an end to what she sees as the judiciary assuming powers it was not originally meant to have. (Aljalian, 1999 p. 10). Aljalian fails to consider any of the issues presented by the authors above however and instead sticks to a narrow, literal interpretation of the issue. She does this so much so in fact, that one begins to wonder if there is not an agenda to her paper beyond what is clearly stated. The whole work does eventually devolve into a thinly veiled pro-life opinion piece. However there is value in the questions she raises about the interpretation of the law and the use of conveniences in order to swiftly decide legal challenges rather than careful study of intent.

SELF-DEFENSE

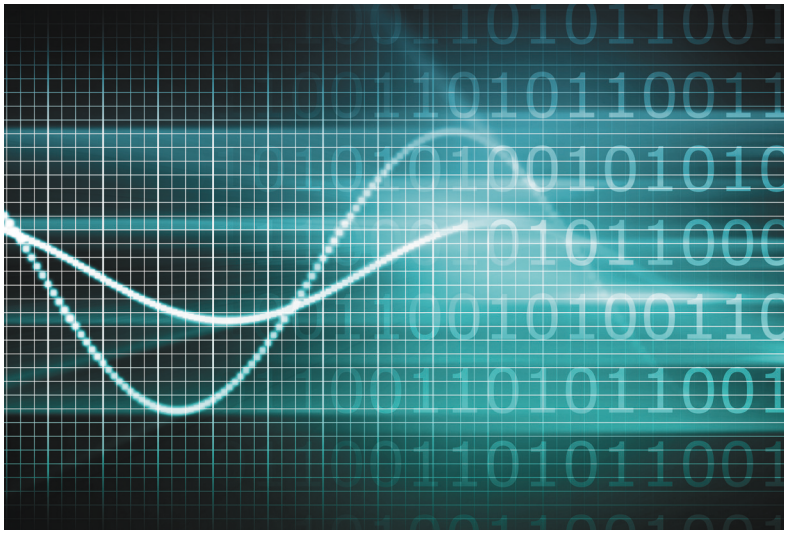
Beyond the discussion of corporate personhood, it is necessary to investigate the ideas behind and surrounding the principles of self defense. The second amendment is perhaps the most controversial and often debated part of the Bill of Rights. Many experts claim that the second amendment deals only with the militia, or in today's language, the National Guard, and has nothing to do with the rights of individual citizens or their entitlement to self defense. In his article titled "The Second Amendment in the Nineteenth Century" David B. Kopel reviews the written legal opinions of the experts at the time. He discusses the commentary of St. George Tucker, a lawyer from Virginia.

Tucker states:

The right of self defense is the first law of nature: in most governments it has been the study of rulers to confine this right within the narrowest limits possible. Wherever standing armies are kept up, and the right of the people to keep and bear arms is, under any colour or pretext whatsoever, prohibited, liberty, if not already annihilated, is on the brink of destruction. (1998 p. 1377).

Kopel cites the continuing quotation of Tucker's opinion in federal cases as the proof of the strength of Tucker's position (1998 p. 1377). This, along with the ninth amendment's guarantee of nonenumerated rights to the people provides the legal basis for self-defense. (Cornell 1787). This limitation of government power further strengthens the case made by Salisbury Warren discussed above. The difference here is that Tuckers comments, as quoted by Kopel do imply specific empowerment of the people.

With the basis for the right of self-defense explained, it is still important to review the necessary guidelines commonly associated with the use of force for self-defense. In her paper reviewing California's self-defense statute, Janet Grummer breaks down the elements of self-defense. Grummer explains that the beyond defending life or property, the individual must have an honest and reasonable belief that there is imminent harm, and the amount of force used in defense must



be proportional to the threat. (2003 p. 1575, 1576). She goes on to give several examples of how these standards are tested and applied in the California legal system. While the specifics are particular to the state of California, the general concepts are universal.

One concept that is not universal is the so-called castle doctrine. Some states provide for the right of the individual to stand their ground and defend their property. Others state in their statutes that citizens have a duty to attempt to flee a hostile situation and only use force in self-defense as a last resort. J.P. Neyland reviews the idea of castle doctrine and variations in its application in his document "A Man's Car is His Castle: The Expansion of Texas' "Castle Doctrine" Eliminating the Duty to Retreat in Areas Outside the Home". Neyland explains that the duty to retreat has its basis in English common law at a time when commoners had to retreat to the wall before turning to fight (2008 p. 2). He states that the majority of states are moving away from this idea (Neyland, 2008 p. 3). Neyland points out that the Supreme Court has been largely silent on this issue and has returned any cases involving it to the state courts to consider. While this is not a federal issue, it is still relevant to the discussion at hand, as the duty to retreat has strong implications when discussing self defense in cyberspace.

Though the right to self-defense is guaranteed by the Constitution the implementation and regulation of that right is left up to the individual states. As stated above, a detailed discussion of each state's individual laws is not possible within the scope of this document. However, some examples should be reviewed for commonalities.

Indiana's law, Indiana code, IC 35-41-3-2 states that a person can use reasonable force against anyone to protect themselves or a third person from imminent use of unlawful force. The individual does not have a duty to retreat, and may defend their home, property and vehicle. They may use force to prevent trespass and to protect property (State of Indiana, 1979).

Texas has similar provisions in Title 2 Chapter 9 of their Penal Code. Texas law states that the actor may use for if they believe it is immediately necessary to protect against someone else's use of force. Texas also has no duty to retreat, protection of third persons, and allows for the protection of property. Texas extends the use of force to prevent the commission of arson, robbery, burglary, and criminal mischief as well as to prevent someone from fleeing after the commission of those crimes (State of Texas, 2007).

New York State surprisingly has very similar laws to the state of Texas. Article 35 of the New York penal code lays out the justifications for use of force. The law is silent on the issue of duty to retreat. New York is however very strict on the use of deadly force and spells out specifically when it can be used (State of New York, 2009). Title 16 of Oregon state law also provides similar provisions though it is very general in explaining use of force. And the extent of use of force (State of Oregon, 1971).

Four state laws then all have very similar provisions, and all allow for the use of force for defense of the individual, or third party, and for defense of property. It is safe to say that though the wording may vary, the legal code in all states will be similar. While none of the four states reviewed had a duty to flee clause, the author acknowledges that they do exist and that the idea still needs to be taken into consideration.

CYBER-DEFENSE

The idea of self defense in cyberspace is not new, though the topic has not been widely discussed in academic circles. Jay Kesan and Ruperto Majuca have provided one of the most substantial discussions of the topic thus far. Using game theory, they analyze the benefit of active self defense in cyberspace. Kesan and Mejuca provide examples of companies who have engaged in counterattacks, but they also have found little legal precedent to demonstrate legality. (Kesan and Mejuca 2009, p.5, 6) They cite the common issues of attribution and proportionality of force in their work, but the pair's findings indicate that if these issues can be controlled there is an overall benefit to society to allow this type of self-defense (Kesan and Mejuca 2009, p.37).

DISCUSSION

As stated above, there is no existing case law on this subject. Any corporations currently actively engaging in active defense are likely to be reluctant to advertise, due to fear of legal retaliation. If one considers active defense of information technology systems to be analogous to physical self-defense, however, one can see many parallels.

Corporate personhood has been thoroughly defined and established in the court for years. However if the corporation is considered to have a body as proposed by Graver, the issue of defense quickly becomes much less convoluted. Additionally if, as asserted by Mayor and Millon, corporations are socially responsible to be good citizens of the community they may not only have the right to defend themselves, but also the responsibility.

The author has established the realities of corporate personhood and drawn specific attention to the ideas of corporate citizenship and the corporeal nature of the corporate person. Further, the author has shown that precedent applies constitutional right to corporations more often than not. Pursuant

[T]he corporation, despite being made up of several natural persons, is treated as an individual person for legal purposes such as taxation, property ownership, contracts and tort law, criminal action and constitutional rights.

to this idea, it has been established that the right of self defense has been granted by the second amendment and ninth amendments of the constitution. According to Kesan and Mejuca, where possible, the ability of the corporation to defend its self is good not only for the corporation but also for society (2009, p.37).

With all this information taken together, it is the opinion of this researcher that corporations have the legal right to actively defend themselves in cyberspace, provided the issues of attribution and proportionality are covered. The corporation as an entity with a body is entitled to defend its body as well as its property from harm. The unique nature of the corporation's body makes its information assets both part of the physical body and property. As we have seen above most if not all states provide for use of force in defense of both categories.

The duty to flee may hurt this stance however. If the analogy is to be followed through to completion, corporations with in an area with an obligation to flee may have no other recourse than to disable systems, unless they can prove that doing so causes irrevocable harm and they have no other choice but to fight back.

Finally, if a corporation has a duty to do right by the society in which it resides and Kesan and Mejuca are correct, a corporation may have an actual duty to defend its self. The corporation may prevent loss of revenue which would lead to loss of jobs. They may discourage criminals from attacking other corporations in the community. Lastly, by defending themselves, corporations remove the burden from law enforcement (assuming they would have been contacted in the first place).

The above is really just the beginning of a long discussion. The practicality of actually acting based on attribution and proportionality should be examined. These issues are extremely complex due to the anonymous and mutable nature of cyberspace. Further work will also need to be done for international and foreign corporations. These companies do business in the United States and have holdings and offices here, but may have systems that span continents. How will the law deal with these situations? Finally, some municipalities also have laws affecting the use of force. These laws will also need to be examined in order to ensure corporate compliance.

Samuel Liles *is an associate professor of computer information technology at Purdue University Calumet, where he researches cyber warfare and cyber terrorism. His research agenda follows the spectrum of information operations and how cyber warfare realistically impacts the various effects of conflict. He currently is researching cyber warfare as a form of low intensity conflict and insurgency.*

Mathew Borton *is a graduate student studying information security at Purdue University Calumet. His research interests are directed toward information security policy with a focus on cyber war policy.*

REFERENCES

Aljalian, N. N. (1999). Fourteenth Amendment Personhood: Fact or Fiction?. St. John's Law Review. Vol 496, No 73.

Cornell University Law School Legal Information Institute. (1997). 18 USC 1030 The Computer Abuse and Fraud Act Retrieved from http://www.law.cornell.edu/anncon/

Cornell University Law School Legal Information Institute. (1787). The annotated Constitution of the United States. Second amendment. Retrieved from http://www.law.cornell.edu/anncon/

Cornell University Law School Legal Information Institute. (1787). The annotated Constitution of the United States. Ninth amendment. Retrieved from http://www.law.cornell.edu/anncon/

Cornell University Law School Legal Information Institute. (1787). The annotated Constitution of the United States. Fourteenth Amendment. Retrieved from http://www.law.cornell.edu/anncon/

Federal Bureau of Investigation. (2006). FBI Computer Crime Survey. Retrieved from http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm

Graver, D. (1999). Personal Bodies: A Corporeal Theory of Corporate Personhood. The University of Chicago Law School Roundtable. Vol. 234 No 6.

Grummer, J. (2003). Self Defense. Loyola Law Review. Vol 36, No 4. 1575-1595.

Kesan, J.P., Majuca, R.P (2009). Hacking Back: Optimal Use of Self-Defense in Cyberspace. Illinois Public Law and Legal Papers Series. Research Papers Series 8, 20. 1575-1595.

Kopel, D.B. (1998). Second Amendment in the Nineteenth Century. BYU Law Review.

Mayer, C. J. (1990). Personalizing the Impersonal: Corporations and the Bill of Rights. Hastings Law Journal. Vol 41 No 3.

Millon, D. K. (2001) The Ambiguous Significance of Corporate Personhood Stanford Agora: An Online Journal of Legal Perspectives. Available at SSRN: http://ssrn.com/abstract=264141 or DOI: 10.2139/ssrn.264141

Neyland, J. P. (2008). A Man's Car is His Castle: The Expansion of Texas' "Castle Doctrine" Eliminating the Duty to Retreat in Areas Outside the Home. Baylor Law Review.

Salibury-Warren, E. (1996). The Case for Applying the Eighth Amendment to Corporations. Vanderbilt Law Review. Vol 1313 No 49.

State of Indiana. (1979). Use of Force to Protect Person or Property. IC 35-41-3-2.

State of New York (2009). Defense of Justification. Article 35

State of Oregon (1971), Crimes and Punishments. Title 16.

State of Texas. (2007). Justification Excluding Criminal Responsibility. Texas Penal Code Title 2 Chapter 9, Subchapter C: Protection of Persons.

"Why do I need to understand Information Employment?"

By Jason Knowles, Major, USAF

"The Information Revolution has fundamentally changed the nature of combat. To win wars today, you must first win the information war."[1]

—Bruce Berkowitz, CIA analyst

The exploitation of the information environment to falsify, augment or reinterpret reality is not necessarily a new phenomenon in the annals of war. Deception has played a significant role in conflicts throughout history. However, the technology enabling the contemporary global information environment makes the manipulation of facts and advancement of alternative narratives much easier now. Consequently, our adversaries have found this non-kinetic asymmetric tactic of manipulating reality an attractive and useful means of confronting overwhelming conventional force. The capability to manufacture alternative "truths" and narratives is a device our adversaries have come to expertly employ to affect US national security deliberations and operations.

The purpose of this article is to foot-stomp the importance of recognizing this contemporary capability as a weapon of war. It is intended as a call-to-action to move the national debate from rhetoric to employment of information for effect by suggesting US military and civilian national security leaders aggressively integrate the informational element in *all* national security planning. To move from debate to verifiable effects-generating actions requires some modification in a historically nurtured military culture focused on kinetic effects.

It is now well understood strategic communication (though the term remains hard to define across the US government), information operations, influence operations, psychological operations, and public diplomacy are necessary communication tools to mitigate adversarial information operations. However, there is sufficient anecdotal evidence to suggest that the US has not made great strides integrating the information element of national power into its national security planning at all levels. Granted, there are statutory and policy constraints on the use of these communication tools in various situations. More importantly, the information environment is so pervasive it is now virtually impossible to conduct any of these operations without unintentionally reaching domestic audiences. This does not absolve us from planning and integrating such actions in response to an adversary's exploitation of the information environment.

"Plans are nothing; planning is everything."

—Dwight D. Eisenhower

Unfortunately, recognition and understanding of this imperative is virtually non-existent at the tactical and operational planning levels because of a preponderance of a kinetic effects focused US military culture (and possibly traditional US characteristics). Part of the situation that builds and maintains that cultural focus is an institutional reluctance or unwillingness to 'train to task' and 'educate to process' when it comes to the information element of national power.

Institutionally, the US military knows how to blow things up. The success the US has had exercising an increasingly precise and efficient kinetic capability has driven the requirement for the consideration of second and third order *informational* effects, and the unintended *informational* consequences associated with blowing things up, exponentially more important. Yet, the same success of the increasingly precise and efficient kinetic capabilities are either overshadowing or not being balanced with the effort to understand and manage the informational effects of those capabilities. This failure to recognize informa-

tional effects has, in various situations, marginalized the intended objective of kinetic actions. The tactical and operational planners must be familiar with the importance, applicability by friend and foe, and potential higher order impacts of employing information for tactical and operational effects. Even more importantly, commanders must be aware of this important element so they can direct their unit leaders and planners to incorporate information operations considerations into pre-deployment and or pre-operation execution. Current efforts to integrate information with traditional kinetic and tactical non-kinetic battlefield weapons employment[2] are not adequate for efficient or effective communication employment, or training, to achieve desired effects. Professor Dennis Murphy, at the US Army War College's observed that: "Each tour in a theater of war it took [the students at Army War College][3] on average, four months to emplace processes to proactively exploit [the information] environment."[4] Though the example reflects a US Army investigative approach, drawing from the author's experience[5], it could have significant application to US Air Force operations as well.

Engaging in the information environment and communicating for effect in response to adversarial information campaigns demands a purposeful approach that is fully integrated into a unit or agency because of the coordination-intense nature of planning and execution necessary to ensure themes and messages[6] are coherent, consistent, and timely delivered.

The primary information sources necessary to effectively counter adversarial information operations are resident in the tactical level unit's planned and executed Tactics Techniques and Procedures (TTPs).[7] The unit or agency designated to develop, coordinate, and implement communication for effect efforts are fortified, or rendered ineffective, by tactical operations executed by operational units. The integration level between the communication element and operational units' will directly reflect the level of impact the communication unit will be able to produce and or mitigate in their effort to further mission and operations objectives. In short, tactical operators' behavior will reinforce or contradict political and or informational strategies in manners that result in significant operational gains, but exponentially more importantly, possibly result in overarching strategic losses.

This directly drives the operational units' need to be aware of, and plan for these interrelations, data development, and information sharing methods, to provide the best opportunities for effect while denying and/or countering the enemy's efforts. Knowing and maintaining focus on over arching objectives is imperative, and operators must understand and internalize commander's intent and the rules of engagement prior to deployment. Now, in this global, speed-of-light, information saturated environment, operators must add the awareness of and exercise opportunities to integrate communication objective(s), theme(s), and potential message(s) development opportunities.[8] Operators must be able to understand how their actions impact the information environment, and integrate their operational actions, into communicating for effect efforts. These needs result in the operational unit's additional requirement for preparation and planning regarding information importance, application, and flows.

A computer instructor shows a student how to access a program during a computer class for instructors at the Regional Training Center on Camp Ur, Iraq, December 21, 2009. *(U.S. Army photo by Spc. Gavriel Bar-Tzur/Released)*

In his paper "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence" USAF Fellow Colonel Jeffery Smith observes that "operational bias has led military analyses to ignore the political objectives—the requirement to influence—in order to concentrate on kinetic effects and more concrete measures of effectiveness," and that "military leaders, by disposition, experience and training, may develop an operational bias—a tendency to

see war as requiring the use of overwhelming force to first and foremost prevail in combat and limit friendly casualties."[9] This may lead to friendly force stagnancy while the enemy remains dynamic, leading to greater potential for failure, effectively allowing the enemy to "achieve a position of advantage" in movement and maneuver.[10] Tactical and operational level planners are in a unique position to improve the potential battle space *effects* by providing operators the awareness and guidance to further the potential impacts of real time operator decisions. The push to be more *effective*, not just more deadly, by all levels of leadership will allow for US dominance to continue in the 21st century.[11] In this regard, it is imperative to understand that "… technologies will dramatically expand military capabilities. To benefit fully, planners and operators must avoid the trap of simply using new tools to do the same old things in better ways."[12]

"It is a fundamental mistake to see the enemy as a set of targets. The enemy in war is a group of people. Some of them will have to be killed. Others will have to be captured or driven into hiding. The overwhelming majority, however, have to be persuaded."

—Frederick Kagan[13]

"It would be up to the humans to train themselves and develop ways of evolving the system to suit them better. The humans and their technology would coevolve."[14] This quote was an observation about early (1960s) computer programmers, but is relevant now as well. Given the emergence of an increasingly powerful information environment and senior leadership transformational initiatives, tactical and operational leaders and planners must understand the necessity for, and when appropriate, integrate information employment planning with the intended effect of foiling the enemy's exploitive use of the information environment. But to put the horse before the cart, the services need to develop operational planners who are information environment-savvy, prepared to develop, test, assess and evolve innovative "information plans" in concert with operational plans.

The growing impact and employment of information for effects drives a need for a military culture change. Adam Brate's captured this imperative in *Technomanifestos* when he explained, "Technology shapes culture, and culture shapes technology."[15] That military culture change is the acceptance and employment of information as a weapon at the weapons employer levels of the military services – the author is certain that senior military leadership has accepted this. The idea that information is a weapon is not new. Sun Tzu states in *The Art of War* that "…to subdue the enemy without fighting is the acme of skill," and that "a victorious army wins its victories before seeking battle."[16]

"A weapon is a device for making your enemy change his mind."—Lois McMaster Bujold, "The Vor Game," 1990

"Weaponizing"[17] information has already been recognized as highly effective and has been effectively employed by our enemies. Examples of weaponized information are plentiful: The North Vietnamese bringing the war into American living rooms[18]; the Taliban's media feed regarding civilian deaths. The Taliban media feed resulted in US operations disruption and increases in US manpower and funding requirements that did not further US objectives[19], in essence provoking reactive and defensive damage control. One of the most noted Iraqi insurgents' successes was highlighted in the news report, *"Media Impact on Military Operations, Falluja in 2004"* which was aired 19 June 2007 on the Public Broadcasting System's *Frontline*, "The impression is portrayed [by the insurgents through information media] as if the Americans are going in and wantonly killing civilians along with the insurgents and it was unsustainable for the Iraqi leadership which at the time, wasn't elected, to continue. So, the American civilians in charge in Iraq appealed to the President [of the United States] to stop the Marines…This is a double loss. The Americans look indecisive, they look incompetent, and they also look inhumane to a wide number of people in the Middle East."[20] This effort has even been clearly communicated by our enemy's leadership. As noted in Lt Col Andrew Gebara's "Damage Control: Leveraging Crisis Communications for Operational Effect," "Ayman al-Zawahiri['s] strategic vision for IO attacks: '… despite all this, I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Umma. And that however far our capabilities reach, they will never be equal to one thousandth of the capabilities of the kingdom of Satan that is waging war on us.'"[21]

Communicating for effects[22] will continue as a significant battle space weapon at all levels of warfare. Designed communication efforts are also a shaping mechanism during peacetime. In *Technomanifestos*, Brate makes the observation in his discussion regarding Bill Joy's[23] fears regarding the future of the human race, "What makes the information age particularly dangerous is what also makes it so liberating: Information can circulate with unprecedented speed and scope."[24] In order for this ever-growing information weapon employment to be effectively used and developed, education must be provided on the

A U.S. Navy EA-18G Growler assigned to the "Vikings" with Electronic Attack Squadron 129, takes off from Naval Air Facility El Centro, Calif., during a training exercise. *(U.S. Navy photo by Mass Communication Specialist 3rd Class Rialyn Rodrigo/Released)*

importance of the weaponization of information and the organizational information element(s). For long-term impact, this education must be provided to those that will become the tactical and operational planners and employers. Tactical operators must recognize that kinetic operations communicate more than shock and awe. Therefore, those delivering kinetic effects must understand the informational consequences of those actions and integrate that understanding into their operational perspective. The USAF, other DoD branches, and allied militaries, must "breed-in"[25] this understanding and education. However, first, the individuals already established as field or weapons systems subject matter experts (SMEs) must receive this training. This group of SMEs typically would not be field grade officers, but Captains (O-3s) provided with oversight and guidance from the field grade officers. Once education methods are developed, these efforts could be employed and trained to by our allies, furthering building partnership capacity efforts. As with any new capability development, the field requires understandable terminology, TTPs, and education to facilitate understanding and effort integration. However, enough details, existing concepts, and communication operators are currently available for tactical and operational planners to start integrating tactical operations into Information Operations (IO), Public Affairs (PA), Psychological Operations (PSYOPS), Strategic Communications (SC), and Public Diplomacy (PD) efforts.[26]

Communicating for effects efforts span the range from tactical to strategic, civilian and military, but the differences between the types and intended uses are not well communicated to USAF officers during their development. In 2005, two US Army Captains commented that the "[US] Army has begun to emphasize information operations (IO) in every deployment."[27] This emphasis, though perhaps late to task, should eventually lead to a US Army wide understanding, not just limited to officers, as the entire force plays a part in information employment's effectiveness. The USAF officer corps lack of understanding in the types and intended uses of information results in operational planners that are not aware of how information may affect the operations they are planning. However, more importantly, the author's opinion is that operational planners as a group do not know how, or are not as interested in information employment as they should be. In the Joint Forces Quarterly, 3rd Quarter edition of 2007, US Navy Admiral James Stavridis advised commanders to "organize at the operational level to enable at the tactical. For a combatant commander, the place to 'organize' strategic communication is at the operational level."[28] Operational and tactical level leaders must step forward and seek out these opportunities, ask the culturally unpopular question, and demand honesty in pursuit of objectives and desired effects.

Blogging recently, US Army Lieutenant General William Caldwell references US Navy Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff, *Joint Forces Quarterly* article, pointing out Admiral Mullen's argument that "… the United Sates military's biggest problem is credibility – words matching deeds to establish trust with the local populaces."[29] In response to General Caldwell's call for discussion blog, US Army Major Enrique Vasquez suggests that breakdowns are not limited to credibility, but include interference and bias instilled through military hierarchy, ignorance of the information age, inconsistency of message development through the different levels of command, input of the wrong message or omission of an important event, or ignorance by those put in front of the media providing inconsistent or out of sync information.[30] Chuck de Caro, president of S.A.G.E.[31] and developer of the Softwar concept[32], lauded Major Vasquez and recommended the military prepare for media engagements as

they would for terrain and weather. Military units prepare for deployment by simulating the heat of a desert or mountainous terrain, but do not always train or equip themselves with the tools for the media interactions they may face. Any military member can create information effects ranging from tactical to strategic. It is common to banter about the effects the "strategic corporal"[33] can create, intended or unintended, due to the nature of the information environment. Anyone can engage, and many do. US Army Lieutenant Colonel Bart Stovicek succinctly comments, "In today's information environment every word, action, or event has potential strategic impact."[34]

A number of monikers have been assigned to exploitive engagements in the global information environment, *strategic communication* (SC) being fashionable over the past several years. But strategic communication is essentially one of the most misused buzzwords to denote *communicating for effect* within the military. SC is the orchestration of actions, images, and words to achieve objectives and/or desired effects.[35] SC is not something that only occurs in Washington D.C., at the strategic level of warfare, or the same thing as PD, IO, or PA.[36] SC is not a capability, a career field, crisis-driven, and does not just happen.[37] Nevertheless, since all levels of warfare impact the effort, all military personnel, but especially commanders, and operational and tactical planners must understand the associated communication objectives, themes, and how individuals can influence those objectives. No matter the source, friend or foe, planners must plan and integrate information effects for all contingencies. The enemy gets a vote and warfighters are human, meaning the enemy, friendly 'mistakes', and the ever-present Murphy's Law will play their part in the battle space. Plans can, and should, be designed to attempt to minimize their potential negative impacts.

In August 2008, Mr. Robert Hastings, Principal Deputy Assistant Secretary of Defense for Public Affairs signed and distributed "DoD Principles of Strategic Communication Guide". These principles are not new, but are very much worth review, reflection, and incorporation into daily operations. Mr. Hastings notes in his cover letter, "The Department [of Defense] held the first Strategic Communication Education Summit in March 2008" where the principles were developed "until policy and doctrine are published." The nine principles of SC are described in detail in the guide.[38] The SC guide is recognized and stated that it is just a beginning in Mr. Hastings' cover letter.

The criticalness of, and the ability to employ information to effect the battle space as a weapon will only become more imperative for military operations success. This is because information is vastly more accessible, employable, and influential across multiple audiences. Worldwide conventional and kinetic focused military warfare, such as those that won World Wars I, II, and the Cold War are now believed to be obsolete. The US military must accept and employ the innovative and unconventional methods available today to mitigate threats to US national security. In order to do this, it will take more than senior leader leadership. It will take leadership from all levels of the organization to effectively and efficiently employ any weapon, kinetic or non-kinetic such as the information element, to achieve national, strategic, operational, and tactical objectives and effects.

Jason Knowles *is an active duty USAF Major Air Battle Manager Weapons Officer and student at Air Command and Staff College. Major Knowles has been an Air Weapons Officer and Interface Control Officer assigned to 621st Air Control Squadron, Osan AB, Republic of Korea with duties including weapons control activities and execution of military datalink operations for 7th AF. While assigned to the 552nd Air Control Wing, Tinker AFB, Oklahoma and at the 961st Airborne Air Control Squadron, Kadena AB, Japan, Major Knowles was an E-3B/C Sentry instructor and evaluator Air Surveillance Officer, Mission Crew Commander, and squadron Weapons Officer.*

BIBLIOGRAPHY

Berkowitz, Bruce, The New Face of War: How War Will Be Fought in the 21st Century, New York NY: The Free Press, 2003.

Brate, Adam, Technomanifestos, New York / London: Texere Publishing LLC, 2002.

Caldwell, LTG, USA, Reflections by Frontier 6: Strategic Communication and National Security, September 2009, 2009, accessed November 9, 2009, http://usacac.army.mil/blog/blogs/why_i_serve/archive/2009/09/02

US Joint Warfighting Center, Commander's Handbook for Strategic Communications: Establishing Policy and Guidance, Washington D.C.: US Joint Forces Command, 1 Septembery 2008.

Karns, Christopher, Major, USAF, "Strategy and Communication: The Need for a Fused and Synchronized Strategic Capability", Air Force Fellows, Air University, Maxwell AFB, AL, April 2008.

Cook, Martin, "The Proper Role of Professional Military Advice in Contemporary Uses of Force", Paramerters: US Army War College Quarterly XXXII, No. 4 XXXII, No. 4 (Winter 2002-03).

US Department of Defense, Joint Publication 3-0: Joint Operations with incorporated change , Final Coordination 2 October 2008.

Edward Mann III, Gary Endersby, Thomas Searle, "Thinking Effects Efects-Based Methodology for Joint Operations", Vol. CADRE Paper No. 15. Maxwell AFB, AL: College of Aerospace Doctrine, Research and Education (CADRE), Air University Press, October 2002.

Gebara, Andrew, "Damage Control: Leveraging Crisis Communications for Operational Effect", Air and Space Power Journal Fall 2009 (September 2009).

Griffith, Samuel, Sun Tzu, The Art of War, Trans.l. London, Oxford, New York: Oxford University Press, 1963.

Lind, William, et al, FMFM 1-A, Draft 4.2 18 June 2007, Formatted 30 October 2007, http://ics.leeds.ac.uk/papers/pmt/exhibits/3007/fmfm_1-a.pdf, accessed 29 January 2010.

Loney, Timothy, Colonel, USA, "Drafting a New Strategy for Public Diplomacy and Strategic Communication", Carlisle Barracks, PA: US Army War College, 2009.

McLuhan, Marshall, Understanding Media: The Extensions of Man. Cambridge, MA: MIT Press, 1999, 1964.

Murphy, Dennis, "Forcing Cultural Change: The Information Endstate." September 4, 2009, http://www.carlisle.army.mil/dime/blog/archivedArticle.cfm?blog=dime&id=22 (accessed December 9, 2009).

Potter, Robert, Col, USAF (Ret.), Communication Analyst/Researcher and carrer USAF Public Affairs Officer, Air Force Research Institute, Air University, Maxwell AFB, AL, interviews by and other coorespondences with Jason Knowles, Major, USAF, (November 23, 2009 –January 29, 2010).

Smith, Jeffery, Colonel, USAF, "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence", Air Force Fellows, Air University, Maxwell AFB, AL, April 2008.

Stavridis, James, Admiral, USN, "Strategic Communication and National Security", Joint Forces Quarterly, 2007, 3d Quarter ed.

Stovicek, Bart, "Strategic Communication: A Department of Defense Approach", US Army War College, 30 March 2007.
Trent, Stony, Captain, USA and Doty III, James, Captain, USA, "Marketing: An Overlooked Aspect of Information Operations", Military Review, July-August 2005.

ENDNOTES

1 Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century*, xi.
2 Traditional kinetic and understood tactical non-kinetic battlefield weapons employment reflects operations such as Exercise RED FLAG/VIRTUAL FLAG or USAF Weapons School Integration and Mission Employment Phases activities.
3 "Students at the U.S. Army War College are senior leaders with about 20 years of military or government experience. Most have had multiple tours of duty in Iraq and/or Afghanistan. And so anecdotally, when I ask these students whether they "get it" regarding the importance of information as a significant warfighting enabler they almost unanimously state that they understand that the information environment is critically important. But when I drill down to the next level of detail I find that with each tour in a theater of war it took them on average, four months to emplace processes to proactively exploit that environment. That tells me that that the military leadership has not culturally inculcated information as a critical warfighting function…and so a forcing function needs to occur until that happens within a common planning process embraced by all." Murphy, "Forcing Cultural Change: The Information Endstate".
4 Ibid.
5 Tactical and operational execution and planning while assigned to 621st Air Control Squadron at Osan AB, Republic of Korea, 552nd Air Control Wing at Tinker AFB and 961st Airborne Air Control Squadron, Kadena AB, Japan. Wide range of live and simulation exercises with involvement from operator, planner, tester, instructor, and evaluator. Participation as operator and/or supplemental planner in Operations NORTHERN WATCH, SOUTHERN WATCH, NOBLE EAGLE, ENDURING FREEDOM, IRAQI FREEDOM, and others.
6 A theme is an overarching concept or intention, designed for broad application, while a message is a narrowly focused communication directed at a specific audience. U.S. Joint Forces Command, Joint Warfighting Center, "Established Policy and Guidance" in Commander's Handbook for Strategic Communication, 12 and Loney, "Drafting a New Strategy for Public Diplomacy and Strategic Communication."
7 Robert "Bob" Potter, Col, USAF (Ret.), electronic correspondence 15 December 2009.
8 "…focused Air Force efforts to understand and build strategic relationships with key audiences to create, strengthen, or preserve conditions favorable for the advancement of USAF strategic interests, policies, and objectives through the use of coordinated and integrated programs, plans, themes, messages, and synchronized products." Karns, "Strategy and Communication: The Need for a Fused and Synchronized Strategic Capability," 16.
9 Smith, "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence", 5 and Cook, "The Proper Role of Professional Military Advice in Contemporary Uses of Force," 24-28.
10 Joint Publication 3-0: Joint Operations, 17 Sep 2006, Incorporating Change 2, Final Coordination 02 Oct 2008, xviii.
11 As reflected in Effects Based Operations (EBO) concept. Mann, Endersby, Searle, "Thinking Effects Effects-Based Methodology for Joint Operations, CADRE Paper No. 15".
12 Ibid., 11-12.
13 "War and Aftermath," *Policy Review*, Aug. 2003.
14 Adam Brate, *Technomanifestos*, 128.
15 Ibid., 113.
16 Griffith, *Sun Tzu, The Art of War*, 77, 87.
17 mith, "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence", 7.
18 Gebara, "Damage Control: Leveraging Crisis Communications for Operational Effect".
19 Ibid.
20 *"Media Impact on Military Operations, Falluja in 2004"* aired 19 June 2007 on the Public Broadcasting System's *Frontline*.
21 Gebara, "Damage Control: Leveraging Crisis Communications for Operational Effect".
22 Phrase first learned by author during interview with Robert "Bob" Potter, Col, USAF (Ret.) 23 November 2009. Phrase also found in Smith's "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence".
23 Brate, *Technomanifestos*, 317-318. Excerpted: Bill Joy, co-founder and chief scientist of Sun Microsystems. Identified by Brate as a technologist and prominent leader of the Information Revolution. A wild-haired and brilliant hacker. Put together software version of Unix operating system that eventually enabled computers to be networked worldwide. Designed company's advanced networking architecture, which escalated the company to fame and fortune. Co-developed Java and Jini, two of the most powerful programming languages to date (2002). In 1997, President Clinton appointed Joy co-chairman of the Presidential Information Technology Advisory Committee.
24 Ibid., 320.
25 Robert "Bob" Potter, Col, USAF (Ret.), electronic correspondence 15 December 2009.
26 Smith's paper, "Communicating for Effect: Operationalizing and Analyzing Weapons of Mass Influence", provides definitions and assessments of the different kinds of communication types/categories.
27 Trent and Doty, "Marketing: An Overlooked Aspect of Information Operations".
28 Stavridis, "Strategic Communication and National Security", 6. (Admiral James G. Stavridis, USN , at the time of publishing was Commander, U.S. Southern Command and is Supreme Allied Commander, Europe at the time of this paper.)
29 Caldwell, "Reflections by Frontier 6: What's the Hubbub About Strategic Communication?", blog accessed 9Novemeber 2009. (LTG Caldwell currently serves as the commander of the Combined Arms Center at Ft Leavenworth, Kansas. The command oversees the Command and General Staff College and 17 other schools, centers, and training programs. US Army equivalent to US Air Force Air University.)
30 Ibid.
31 Sea Aerospace Ground Evaluations (S.A.G.E.) Corporation
32 Chuck de Caro, Lecture/Presentation, "Killing Al Q'aida", www.dodccrp.org/events/12th_ICCRTS/CD/html/presentations/031.pdf.
33 Lind, et al, FMFM 1-A, Draft 4.2 18 June 2007, Formatted 30 October 2007, 6.
34 Stovicek, "Strategic Communication: A Department of Defense Approach", 14.
35 Unsourceable Strategic Communication conference/presentation material that provided concise summary statements regarding authors learnings.
36 Ibid.
37 Ibid.
38 The nine principles are, in no order of precedence: Leadership-driven communication process; Credible: Perception of truthfulness and respect; Understanding: Deep comprehension of others; Dialogue: Multi-faceted exchange of ideas; Pervasive: Every action sends a message; Unity of Effort: Integrated and coordinated; Results-based: Tied to desired end state; Responsive: Right audience, message, time and place; Continuous: Analysis, planning, execution, and assessment.

Some Misconceptions Regarding Information Operations

By COL Michael J. Dominique, USA

A U.S. Soldier assigned to Charlie Company, 82nd Airborne Division, searches an orchard for improvised explosive devices and weapons caches during Operation Mesmar near a village in southern Afghanistan February 5, 2010. *(U.S. Air Force photo by Senior Airman Kenny Holston/ Released)*

The importance of information superiority is widely recognized throughout the Department of Defense and other agencies, but in the rush to learn this magical solution to all our problems, some misconceptions about Information Operations (IO) have evolved. The importance of information and what we now refer to as strategic communication materialized with the Committee on Public Information and its mission to promote U.S. policy goals to foreign audiences, counter foreign propaganda and rally American public opinion during World War I.[1]

The development of communication technology and the importance of media prompted the U.S. Army's formalization of Information Operations as a career field. Just as any emerging capability, the excitement of something new resulted in much attention and an influx of suggestions. In 1999, the Army's newly designated Functional Area 30s (Information Operations Officer) were sent out to do "great and wonderful things" armed with the 1999 version of Field Manual 100-6, *Information Operations,* in draft form and without formal IO training. It is no wonder that the definition of IO continued to change in those first several years and it was up to the practitioners and forward thinking leaders to take what little training and doctrine was available and develop their own interpretation of IO and how to best employ it. With this beginning and all the attention that IO has received it is not surprising that the military community and others outside the community have developed their own misconceptions about IO.

A common misconception is that IO is the "cure all" for information problems. Joint Publication 3-13 describes information operations as "the integrated employment of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), military deception (MILDEC) and operations security (OPSEC) in concert with specific supporting and relating capabilities to influence, disrupt, or usurp adversarial human and automated decision making while protecting our own."[2] The fact that it is a process is sometimes forgotten and many see IO as the primary means of addressing bad news or of informing target audiences. Others see IO as the means to prevent bad deeds or actions from becoming bad news. Just informing an audience is not enough; the words need to be supported by action. Information serves as a multiplier that gives credibility to "words, images, and actions" but information without the support of actions is merely words of no consequence.[3] The IO product is not a handbill or a news release but rather a synchronization matrix or a tool that ensures that the information capabilities or various elements related to IO are synchronized to achieve the commander's desired effects.

Another misunderstanding is confusing IO with PSYOP. IO is an integrated process that should synchronize PSYOP and the other capabilities, not replace them.

Much of the confusion is due to the critical role that PSYOP plays within the overall IO effort but there needs to be a clear distinction between the two. The use of PSYOP measures of performance for IO is a common technique due to its quantitative nature, but IO must concentrate on the overall measure of effectiveness for all the information tasks. A challenge always confronting the IO officer is how to brief the integration process when it is the quantitative results that get the attention. IO staff officers must learn to integrate the other information elements into the planning efforts and reports to provide leadership with all the information not just that information that is easily documented.

A new misconception that recently surfaced is the role of the Information Engagement (IE) officer. Since there is not yet a formal IE subject matter expert, many see the IO officer as the subject matter expert in regards to engagements. Experience in the Balkans showed the effective role that the IO officer had regarding IE but it places the IO officer in the role of an executor rather than an integrator. Anticipated changes within the Army IO doctrine reinforces perception that the IO officer's focus will be strictly on IE. This could lead many to the assumption that it is no longer the responsibility of the IO officer to integrate all the information elements for the commander. If the IO officer becomes an IE officer, by the definition of information engagement, he becomes responsible for "the integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communications and defense support to public diplomacy...."[4] If the IO Army officer focuses only on IE how will this affect the interoperability with Joint and Coalition IO efforts?

With the focus on influencing, the tasks of disrupting and usurping decision making at times becomes secondary. OPSEC remains a continuous challenge that normally does not get the attention it deserves unless there is a failure. MILDEC and computer operations are addressed but normally in classified channels so their lack of visibility can give the misconception of nonparticipation in the overall effort. The technical aspects of information, be it computers or EW, have increased the interest in their capabilities but the second and third order of effects require some limitation due to the potential strategic impacts. Ensuring a well integrated, full spectrum approach to achieve information superiority does not necessarily require employment of all capabilities, but consideration of all the capabilities is a must. Regardless of the environment, influencing is not the only task of the IO practitioner - just because it is not visible does not mean it is not in use.

Just as any messaging product, this article attempted to highlight some of the misconceptions that continue to plague IO and to prompt dialogue. Most IO practitioners will comment that this information is not new but the best way to counter the harmful impact of these misconceptions is through education and professional discussion. For those who did not see these as misconceptions then it at least should prompt some reassessment regardless of the outcome. Until these misconceptions are addressed or proven to be false, the IO community will continue to face challenges from doctrine writers, external organizations, leadership and from within.

A U.S. Air Force C-17 Globemaster III aircraft crew from the 21st Airlift Squadron out of Travis Air Force Base (AFB), Calif., loads Army equipment and personnel from the 4th Psychological Operations (PSYOP) Group, 9th PSYOP Battalion out of Fort Bragg, N.C., Jan. 27, 2010, at Pope AFB, N.C. *(U.S. Air Force photo by Staff Sgt. Joshua L. DeMotts/Released)*

Colonel Michael J. Dominique *received a commission as an Infantry officer in 1986 and became an Information Operations Officer in 1999. He has served in multiple IO positions to include the Commander of 1st Battalion, 1st Information Operations Command and the Corps IO officer for III (US) Corps, Ft. Hood, TX. He is a graduate of the U.S. Army War College and serves as the Director of the Information Proponent Office, Ft. Leavenworth, KS.*

ENDNOTES

1 Brian McKiernan, "Information Operations Roadmap: One Right Turn and We're There, *Information as Power: An Anthology of Selected United States Army War College Student Papers, Volume 2* eds. Jeffrey Groh et al (Carlisle, PA: US Army War College n.d.), 29.

2 Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (February 13, 2006), ix.

3 Dennis Murphy, "Strategic Communication Wielding the Information Element of Power" in *U.S. Army War College Guide to National Security Issues, Vol 1: Theory of War and Strategy*, ed. J. Boone Bathomees, Jr., 3rd Edition. (Carlisle, PA: Strategic Studies Institute, June 2008), 180.

4 U.S. Department of the Army, *Operations*, Field Manual 3-0 (Washington, DC: U.S. Department of the Army, February 27, 2008), 7-3.

Electronic Warfare and Cyberspace Operations: Where is the Convergence?

By COL Laurie M. Buckhout, USA

Introduction

The wars in Iraq and Afghanistan have challenged operational commanders with new and emerging cyberspace (Cyber) and Electromagnetic Spectrum (EMS) threats. Insurgent forces, for instance, commonly operate within cyberspace by using the Internet to promulgate their messages, while at the same time, insurgents physically threaten Soldiers by employing weapons enabled by the EMS, such as command and control of direct and indirect fires and Radio Controlled Improvised Explosive Devices (RCIEDs). The Department of Defense (DoD) and Service components, as a result, have identified and taken measures to address significant capability gaps for both areas. Services, including the Army, are currently struggling to determine how doctrinal relationships, warfighting functions and resourcing should occur for these two overlapping, yet distinct, capabilities. Within academic circles, discussions on the relationship between Cyber and Electronic Warfare (EW) have been dominated by a theory that their waveforms converge. Operational practitioners, on the other hand, view the capabilities as complementary but distinct. Convergence of the Cyber domain with EMS operations requires careful evaluation, in-depth discussion and final validation by senior leaders before the Army implements a holistic, single solution-set for Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Costs (DOTMLPF-C).

An EW Officer's Perspective on Convergence

The Army must explore convergence between EW and Cyber. To maximize capabilities available for operational commanders, the Army should look at Cyber and EW separately and identify requirements with a thorough threat analysis.

Army Solution Must Nest with DoD, Joint and Allied Doctrine

How the Army defines and creates DOTMLPF-C for Cyber and EW has a profound impact on the Service's ability to

support Joint and Coalition operations. For this reason, the Army's solution must nest with DoD, Joint, Service and Allied Doctrine. Currently, doctrine at these levels clearly distinguishes between Cyber and EW.

Cyber definitions at the strategic levels characterize cyberspace by computers and networks. For instance, National Security Policy 54 defines cyberspace as the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. The 2008 National Defense Strategy illustrates the strategic nature of Cyber. It states the cyberspace threat can disrupt commerce and daily life in the United States, causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks. Department of Defense Directive (DODD) 3600.01 defines Computer Network Attack as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Finally, in a 10 July 2008 memo, the Chairman Joint Chiefs of Staff (CJCS) defined cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Clearly, Cyber's center of gravity is the network. Cyber is strategic in nature due to the far reaching effects of the network.

Strategic definitions of EW, on the other hand, demonstrate its military nature. According to DODD 3600.0, EW is "any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or attack the enemy." Joint Publication 3-13.1 defines EW with exactly the same verbiage. These definitions validate that EW has militarily relevant targets not considered Cyber based. Examples of this include radar and communications receivers, laser designators and range finders, Signals Intelligence receivers, and night vision systems. A significant portion of the EMS used for military purposes operates along the Radio Frequency (RF) spectrum. Cyber operations, by contrast, primarily center on computer network operations and programming solutions and only occasionally involve the RF portion of the EMS spectrum in an information exchange function.

An E/A-6B Prowler aircraft from Electronic Attack Squadron (VAQ) 140 performs an arrested landing on the flight deck of Nimitz-class aircraft carrier USS Dwight D. Eisenhower (CVN 69), under way in the North Arabian Sea, March 7, 2010. *(U.S. Navy photo by Mass Communication Specialist 3rd Class Bradley Evans/Released)*

AOC 47th Annual Symposium and Convention

October 3-7, 2010
Atlanta, Georgia

AOC 2010

Get ready for the 2010 convention which will focus on the Electro-Magnetic Spectrum.

Exhibit space is extremely limited in Atlanta. Don't miss your chance to exhibit, sign up for your booth space today! Contact Stew Taylor at **taylor@crows.org**.

AOC WASHINGTON D.C. 2009

46th Annual Convention Wrap-Up Now Available

See what you missed at the 46th Annual Symposium! Watch a sampling of keynote addresses and sessions on the post convention Web page along with an exhibitor product demonstration by Anatech Electronics. Briefings and Show Daily editions are also available!

*Visit **www.crows.org** for more details.*

Joint Interoperability and unity of effort are key to the Army's ability to support the Joint Warfight, as required in the June 2008 National Defense Strategy. Any definition outside DoD, Joint, Service and Allied doctrine will lead to confusion within the institutional and operational Army and have profound impacts on development of Cyber and EW capabilities. Army doctrine not clearly nested with DoD, Joint, Service and Allied constructs will negatively impact resourcing and fielding of new systems and technologies.

Complete Assessment and Determination Required

Before the Army commits to resourcing Cyber and EW holistically, it must identify areas of overlap and divergence. To do this, Cyber and EW require separate Capabilities Based Assessments (CBAs) to identify materiel and non-materiel gaps. Once CBAs for both areas are completed, convergence between the two can be analyzed, evaluated and determined.

Since 2008, three EW CBAs have been completed (Army, Joint and Special Operations Command), and all identified nearly identical EW materiel and non-materiel gaps. The Army is currently addressing these identified gaps across DOTMLPF-C. For example, 1,664 personnel have been approved for initial resourcing into the EW career field. Training facilities have been built at Fort Sill, Okla. and EW courses have been developed and validated. Material solutions, to include Airborne Electronic Attack and Integrated EW systems, are in the pre-Material Development Decision stages for acquisition. In contrast, no Cyber CBAs have been conducted to date.

To accurately evaluate convergence across DOTMLPF-C, both capabilities must be viewed separately. A finding of similar capability gaps and requirements will either authenticate or invalidate convergence theory.

Conclusion

The relationship between cyber and EW must be carefully considered. Cyber and the EMS are different physically, doctrinally and technologically, yet simultaneously interdependent. How the Army defines Cyber, EW and their relationship with one another will have a lasting impact on its ability to support the joint war effort. Look for a series of future articles examining doctrinal relationships and warfighting functions, and exploring how the Army should man, train and equip future Army forces for the Cyber and EW fight in the April, July and October 2010 editions of the AOC *IO Journal*.

Colonel Buckhout *was assigned as the Chief, Electronic Warfare Division, Department of the Army, Washington, DC in June 2006.*

Colonel Laurie G. Moe Buckhout was commissioned in 1984 from James Madison University with a Bachelor's Degree in English. She is the daughter of a retired Infantry Colonel and a former Army Air Corps Lieutenant. She was commissioned as a Signal Officer and has served at echelons from a tactical platoon leader to a Presidential Communications Officer at the White House. She also served for two years as a Battalion Commander, leading an 800-Soldier Communications Task Force throughout Iraq from 2003-2004. Following command, she was assigned to the Joint Staff, J6. COL Buckhout was then selected by the Vice Chief of Staff of the Army to lead the Army's Electronic Warfare efforts, which she still leads today.

COL Buckhout holds Master's Degrees in Information Systems Management and in Military Arts and Sciences with a concentration in Military History. She has earned the Bronze Star, Defense Meritorious Service Medal (twice), the Army MSM (four times), the Joint Commendation Medal and multiple other service and Joint medals as well as the Army Meritorious Unit Citation, Army Superior Unit Award and the Presidential Unit Citation. She also wears the Joint Staff Badge, Presidential Service Badge, Army Staff Badge and Parachutist's Badge.

Chief of Naval Operations Adm. Gary Roughead delivers remarks during the Center for Strategic & International Studies' "Information Dominance: the Navy's Initiative to Maintain the Competitive Advantage in the Information Age" event October 1, 2009, in Washington, D.C. *(U.S. Navy photo by Mass Communication Specialist 1st Class Tiffini Jones Vanderwyst/ Released)*

DIME is for Integration:

Strategic Communications as an Integrator of National Power

By MAJ's Beau Hendricks, Randall Wenner, and Warren Weaver

"If I were grading, I would say we probably deserve a D, or a D plus as a country as to how well we're doing in the battle of ideas that's taking place in the world today. ... We have not found the formula as a country."

—Donald Rumsfeld, Army War College, March 2006

Introduction

Information as an element of national power is regularly discussed, interpreted, and reinterpreted by various government agencies and organizations. Information represents technical capabilities and infrastructure, as well as cognitive aspects of values, beliefs, and attitudes. Another aspect of Information is its role as a synchronizer of information capabilities, conduits and audiences in conjunction with diplomatic, military and economic elements of national power. This article asks the question, "what role does Strategic Communication play in the application of national power, and how are the efforts of U.S. Government agencies synchronized at the national level?" The authors propose that Strategic Communications (STRATCOM) should be the United Stated Government version of the Department of Defense's Information Operations (IO) concept. This will ensure that all elements of our government are saying and doing the right things, at the right time, through the right mediums, and to the right audiences to have the greatest impact in support of our national policies and objectives. By establishing a working definition of STRATCOM, utilizing the Department of Defense's concepts for STRATCOM and IO, and by applying the conceptual understanding of a communications model, this article proposes a method for understanding the context and delivery methods necessary to synchronize the narratives between the different elements of national power.

Working Definition of STRATCOM

The term "STRATCOM" is often used out of context. For the purpose of this discussion it is necessary to establish a common working definition of STRATCOM. Despite the lack of a common definition within the United States Government (USG), the Department of Defense (DoD) offers a vision for STRATCOM in the 2006 Quadrennial Defense Review (QDR)[1].

Jeffrey Jones, former Director for Strategic Communications and Information on the National Security Council defines STRATCOM as:

> *"The synchronized coordination of statecraft, public affairs, public diplomacy, military information operations, and other activities, reinforced by political, economic, military and other actions, to advance U.S. foreign policy objectives." In an effort to establish a common reference for members of the Interagency Strategic Communication Fusion Team in a presentation on STRATCOM and PSYOP a simple definition was provided: "the directed transmission of USG "intent" through a supporting architecture to an audience for a reason that supports U.S. goals or objectives."*[2]

To further demonstrate that we are speaking the same language, but not listening to each other, the Strategic Communication Advisor for the DoS, Dr. Emily Goldman defined STRATCOM as the "managing of information, ideas, and actions to influence attitudes and behaviors of target audiences in support of our policy objectives," by "the synchronized promulgation of information, ideas, and actions overtime through means and content that are tailored for multiple and diverse audiences." She goes on to write that, "Strategic Communication is an influence strategy. The goal is to influence attitudes and behaviors, not to make others like us."[3]

For the purpose of this article we will use the definition found in Joint Publication 3-13, Information Operations, 13 February 2006:

> *"STRATCOM is the focused USG processes and efforts to understand and engage audiences 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."*[4]

This definition recognizes the necessity to synchronize STRATCOM at the federal level, to ensure that there is a common understanding of national interests across the elements of national power. Lieutenant Colonel Bart E. Stovicek, USAR, wrote in a 2007 study:

"All STRATCOM in this context, are USG activities. The contributions made by the various USG departments and agencies (including DoD) are not, by themselves STRATCOM, Rather, STRATCOM is the synchronized, and integrated coordination…of these contributions in order to achieve the broader USG STRATCOM objectives. The distinction is very simple. DoD, DoS and other USG departments and agencies support STRATCOM by conducting various communication activities such as Public Diplomacy (PD), Public Affairs (PA) or Psychological Operations (PSYOP)."[5]

The point is that according to the DoD definition, STRATCOM is a USG activity that the DoD supports. The DoD's creation of the IO concept is a representative construct of how to integrate various capabilities more effectively at the national level.

The DoD Supports STRATCOM

There is an opposing opinion that suggests the DoD is doing STRATCOM every day, through every action and word. The nuanced difference is that the DoD is a conductor of Information Operations and not STRATCOM. Then why does the DoD discuss STRATCOM and why put together an image of STRATCOM as an orchestra illustrated in **Figure 1-1**? This is a good question. The answer is outside the scope of this paper, but it is likely because the DoD is acting as a forcing function for the whole of government. In short the orchestral concept was described by Matt Armstrong by saying that,

"The analogy of STRATCOM as an orchestra has at its middle, the conductor representing the collection of senior leaders, a music score as the STRATCOM plan, and an orchestra made up of various STRATCOM communities of practice and/or lines of operation."[6]

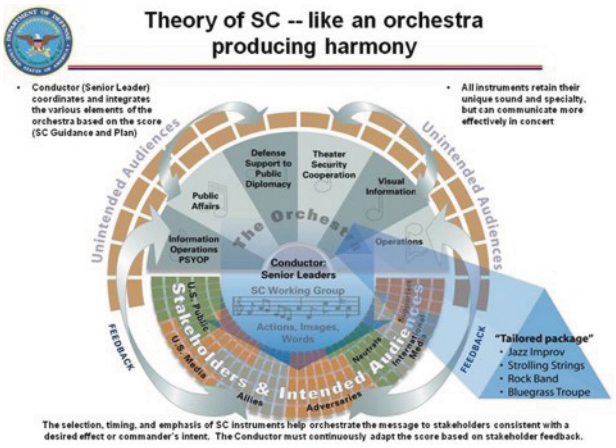


Figure 1-1. DOD STRATCOM Orchestra Concept

This orchestral concept may be too stringent. The comparison to a jazz improvisation is a better representation of what this model would look like. This would allow for the flexibility and mistakes without drawing an unacceptable amount of criticism when an agency gets off message temporarily.

An August 2008 STRATCOM Principles paper signed by the Assistant Secretary of Sefense for Public Affairs listed nine principles of STRATCOM. The principles are not listed in any particular order.

Leadership-Driven - Leaders must decisively engage and drive the STRATCOM process.

Credible - Perception of truthfulness and respect between all parties.

Understanding - Deep comprehension of attitudes, cultures, identities, behavior, history, perspectives and social systems. What we say, do, or show, may not be what others hear or see.

Dialogue - Multifaceted exchange of ideas to promote understanding and build relationships.

Pervasive - Every action, image, and word sends a message.

Unity of Effort - Integrated and coordinated, vertically and horizontally.

Results Based - Actions to achieve specific outcomes in pursuit of a well-articulated end state.

Responsive - Right audience, right message, right place, and right time.

Continuous - Diligent, ongoing research, analysis, planning, execution, and assessment that feeds planning and action.

These principles serve as guidelines for the integration of Information Capabilities is support of national Strategic Communications. If adopted by the USG, they may also serve as guideline for the integration of the elements of national power.

DoD IO Concept

The DoD concept can be utilized as an initial framework from which to more effectively synchronize the elements of national power. To begin facilitating this process it is necessary to understand the capabilities of DoD Information Operations (IO). IO are the planning and integrated employment of Information Capabilities (IC) in the Information Environment (IE) across the spectrum of military operations. They include activities to affect human decision-making and behavior; whether individuals or groups, for the purpose of obtaining a military advantage. They are conducted with the intent to effect and protect cognition, cognitive processes, information, the connectivity and processing systems necessary to create and exchange information.

Current Joint Doctrine identifies the five core IO capabilities as Psychological Operations (PSYOP), Military Deception (MILDEC), Computer Network Operations (CNO), Operations Security (OPSEC), Electronic Warfare (EW), and their associated or supporting capabilities. These supporting or related capabilities include Public Affairs (PA), Joint Combat Camera (COMCAM), Civil Military Operations (CMO), Defense Support to Public Diplomacy (DSPD), and Physical Attack (PHYS ATK). These are either directly or indirectly involved in the information environment and contribute to effective execution of IO. They should be integrated and coordinated with the core capabilities, but also serve other wider purposes in support of STRATCOM. The United States Army has created Information Tasks to bridge the gap between Joint Doctrine and the application of IO capabilities.

The current Department of the Army "Information Tasks" in **Figure 1-2**, are insufficient for discussing and understanding the complexity of the Global Information Environment and the Army's role in supporting STRATCOM. In the process of deconstructing IO and reconstructing it within the limitations

Task	Information Engagement	Command and Control Warfare	Information Protection	Operations Security	Military Deception
Intended Effects	-Inform and educate internal and external publics -Influence the behavior of target audiences	-Degrade, disrupt, destroy and exploit enemy command and control	-Protect friendly computer networks and communication means	-Deny vital intelligence on friendly forces to hostile collection	-Confuse enemy decision makers
Capabilities	-Leader and Soldier engagement -Public affairs -Psychological operations -Combat camera -Strategic Communicatio nand Defense Support to Public Diplomacy	-Pysical attack -Electronic attack -Electronic warfare support -Computer network attack -Computer network exploitation	-Information assurance -Computer network defense -Electronic protection	-Operations security -Physical security -Counterintelligence	-Military deception

Figure 1-2. Table 7.1. Army information tasks[7]

of tactical and operational authorities, doctrine writers have narrowed their understanding of the scope of military IO to five information tasks associated with specific information capabilities. FM 3-0, Operations, aligns STRATCOM under the information task of Information Engagement as an Information Capability, diluting STRATCOM's definition as USG processes to integrate the elements of national power.

While this framework simplifies the training, equipping, and application of military information operations, it artificially bounds capabilities that can be used to achieve other desired effects, and fails to recognize the difference between information capabilities by echelon. It also ignores the difference between information capabilities and the mediums that are used to communicate with target audiences to achieve desired effects in support of stated objectives. To address these short falls we propose a model that incorporates DoD IO capabilities, communications mediums and theories that can be applied to USG STRATCOM efforts.

IO Communications Model

Despite efforts to understand the role of information in military operations, there has been little effort to understand the relationships between IO capabilities and information conduits. Dr. Emily Goldman identified several communications mediums listed in **Figure 1-3**, that become information conduits when used to communicate themes and messages that support policy goals to various audiences.[8] While these mediums are neither inclusive, nor exclusive, they increase our understanding of the information environment and its complexity.

The IO Communications Model (**Figure 1-4**) is an attempt to visualize the holistic role that Military Information Operations has in engaging key audiences by synchronizing IO capabilities and conduits in order to achieve desired effects and support STRATCOM objectives. It is based on a combination of Laswell's and Berlo's communications models. Political scientist Harold Laswell posed the question, "Who says what in which channel with what effect?" His model includes considerations of a variety of factors (communicators, messages, mediums, and audiences) and their relationships to determine the impact of communication. Instead of focusing on these relationships, Berlo created a menu of ingredients for each factor or element of communication.[9] By mixing and matching these ingredients it is possible to generate a wide variety of communication options to gain the greatest impact against any audience. A feature unique to the IO Communications Model is that Information Conduits facilitate two way communications. They provide several means of delivering a message synchronized through the various capabilities, as well as providing multiple methods for the collection of information from key audiences to assess their effectiveness.

Information Domain	**Physical Domain**
• Radio	• Exercises
• Terrestrial TV & Cable	• Force Posture
• Satellite TV	• Visits / Person to Person
• Print	• Reconstruction
• Internet	• Trade and Aid
• Streaming Video	• Etcetera
• Cellular Phones	
• Tribal Councils	
• Word of Mouth; Rumors	
• Etcetera	

Figure 1-3. Communication Mediums

IO spans the full range of activities in human interaction from person-to-person through complex, multistate, intercultural, and international competitions. It is innately joint, and not limited to force-on-force military applications. The intent of conducting IO is to affect the outcome of *military* operations; whether to prevent the possibility of combat, undermine the ability of potential competitors to muster effective combat forces, enable the defeat of an opponent, or to ease the transi-

tion to peace. IO uses any or all means, in an integrated and coordinated fashion, to attain tactical, operational, or strategic objectives.

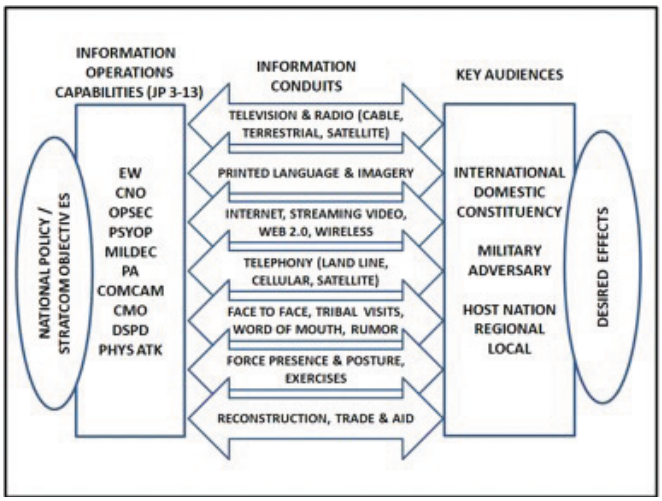


Figure 1-4. IO Communications Model

Conclusion and Recommendation

While the authors have recommended a DoD STRATCOM concept in conjunction with the IO Communications Model as a more effective tool for synchronizing the elements of national power the USG should remain the lead actor for the implementation of the aforementioned DoD construct. Secretary Gates appropriately stated on April 7, 2009 during a PBS News Hour interview:

> *"STRATCOM is basically under the auspices of the State Department. Although we do a fair amount and our commanders have the capability to do some strategic communication, fundamentally it is a State Department responsibility."*

Our nation exists in an environment of simultaneous competition, collaboration, and conflict with other actors. As described in the QDR, the United States will not win the war on terrorism or achieve other crucial national security objectives by military means alone. Instead, the application of unified statecraft, at the federal level and in concert with allies and international partners, is critical.[10] The responsibility for conducting activities in support of national objectives is government wide. Since IO is a tool for integrating and synchronizing Information capabilities in a military environment, STRATCOM should be used to fulfill its role as a focused synchronizer of national power at the federal level. Much like the DoD's orchestral metaphor, a holistically planned and flexibly executed federal communications strategy will ensure that all elements of our government are saying and doing the right things, at the right time, through the right mediums, and to the right audiences to have the greatest impact in support of our national policies and objectives.

The authors attend the School of Advanced Military Studies (SAMS) at the Command and General Staff College, Fort Leavenworth, Kansas.

Major Randy Wenner *is a Special Forces Officer (18A) with over 12 years of active federal service. Prior to joining Special Forces, MAJ Wenner served in various duty positions in the Light Infantry community. MAJ Wenner's most recent duty positions include Operational Detachment - Alpha (ODA) Commander; Assistant Operations Officer and Special Forces Battalion Future Operations/ Plans Officer during multiple combat deployments to Afghanistan in support of Operation ENDURING FREEDOM and other OCONUS missions.*

Major Beau Hendricks *is an Infantry Officer with 14 years of active federal service. MAJ Hendricks has served with the 10th MTN Division, 2nd Battalion, 58th Infantry Training Brigade and U.S. Army Pacific. MAJ Hendricks' most recent assignment was with 2nd Battalion, 27th Infantry Regiment, 3rd Infantry Brigade Combat Team, 25th ID as a company commander, deploying to OIF V.*

Major W. Scott Weaver *is an Information Operations Officer (FA30) with over 20 years of active federal service. MAJ Weaver served 15 years as an Infantryman in duty positions from rifleman to company commander, in airborne, mechanized and light organizations, including operational deployments to Bosnia (SFOR 6) and Afghanistan (OEF 1). MAJ Weaver's recent experiences as a Division Information Operations Officer in the 10th Mountain Division include operations in Afghanistan (CJTF-76) in 2006, and Iraq (MND-C) in 2008.*

ENDNOTES

1. Department of Defense, *Quadrennial Defense Review Report,* (Washington, DC: Department of Defense, 2006), 91-92.
2. Jeffrey B. Jones, *Strategic Communication: A Mandate for the United States,* Joint Forces Quarterly, Issue 39 (4th Quarter 2005), 108.
3. Dr. Emily Goldman, *Strategic Communication Theory and Application,* June 2008, http://www.ndu.edu/CTNSP/Strat_Com/Goldman_Plenary.pdf (accessed December 10, 2009), 5.
4. Headquarters Department of Defense, *JP 3-13, Information Operation,* (Washington DC: Department of Defense, 2006), I-10.
5. Lieutenant Colonel Bart E. Stovicek, *Strategic Communication: A Department of Defense Approach*, USAWC Strategy Research Project, U.S. Army War College, Carlisle Barracks, PA,(30 Mar 2007,g 4, (Accessed 30 Nov 09).
6. Matt Armstrong, A Theory of Strategic Communication: Like an orchestra producing harmony, September 29, 2008, http://mountainrummer.us/2008/09/sc_is_like_an_orchestra.html (assessed December 14, 2009)
7. Headquarters Department of the Army, *FM 3-0 Operations,* (Washington, DC: Department of the Army, 2008), 7-3.
8. Dr. Emily Goldman, *Strategic Communication Theory and Application,* June 2008, http://www.ndu.edu/CTNSP/Strat_Com/Goldman_Plenary.pdf (accessed December 10, 2009), 14.
9. Richard S. Croft, *Communication Theory.* 2004. http://www2.eou.edu/~rcroft/MM350/CommModels.pdf (accessed December 10, 2009).
10. Department of Defense, *Quadrennial Defense Review Report,* (Washington, DC: Department of Defense, 2006), 92.

Join the AOC's IO Institute

Benefits of IOI and AOC Individual Membership:

- *The IO Journal* – the premier professional journal of Information Operations.
- Through our worldwide chapters, access to an extensive network of government and industry professionals in the fields of Information Operations and related and supporting fields.
- Excellent networking opportunities:
  - Through chapter and regional activities tailored to meet local professional development needs.
  - Through world-renowned national/international conventions, exhibitions, conferences and symposia sponsored by the IOI and AOC.
- Career strategy assistance:
  - Access to job postings by IOI and AOC corporate members.
  - Access to the IOI and AOC's Professional Development Center – advanced education and training in communications, intelligence and information systems disciplines.
- Awards and scholarship programs for recognition of professional and academic accomplishments.

Visit www.crows.org and click "Join the AOC IO Institute" for an application.

AOC
Association of Old Crows