Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**
US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

ARSTRAT IO Newsletter Online

ARSTRAT IO Newsletter at Joint Training Integration Group for Information Operations (JTIG-IO) - Information Operations (IO) Training Portal

Table of Contents

Vol. 13, no. 04 (January 2013)

1. 10th Annual Army Global Information Operations Conference
2. China's Space Activities Raising U.S. Satellite Security Concerns
3. 'Red October' Cyber-Attack Found By Russian Researchers
4. Influence Operations and the Internet: A 21st Century Issue
5. When the Network Dies
6. Cyber Operations: Bridging from Concept to Cyber Superiority
7. Army Electronic Warfare Goes On The Offensive: New Tech Awaits Approval
8. Army Manual Highlights Role of “Inform and Influence Activities”
9. DoD Looking to ‘Jump the Gap’ Into Adversaries’ Closed Networks
10. President Putin orders FSB to protect media sites from cyber attack

10th Annual Army Global Information Operations Conference Cancelled

Due to the current fiscal constraints, and the most recent Army guidance outlined in the SA and CSA Risk Mitigation Memo, we cancelled the 10th Annual Army Global Information Operations Conference this year. We will look at dates for the conference next year and announce those later.

More information will be provided later once we complete the approval process. Points of contact are Scott Janzen scott.c.janzen.civ@mail.mil, 719-554-8890; or Jose Carrington, jose.carrington.civ@mail.mil, 719-554-8880.

Table of Contents

China's Space Activities Raising U.S. Satellite Security Concerns

By Andrea Shalal-Esa, Reuters, 14 January 2013

WASHINGTON (Reuters) - The United States is concerned about China's expanding ability to disrupt the most sensitive U.S. military and intelligence satellites, as Beijing pursues its expanded ambitions in space, according to multiple sources in the U.S. government and outside space experts.

A classified U.S. intelligence assessment completed late last year analyzed China's increasing activities in space and mapped out the growing vulnerability of U.S. satellites that provide secure military communications, warn about enemy missile launches and provide precise targeting coordinates, said the sources, who were not authorized to speak publicly.

"It was a very credible and sobering assessment that is now provoking a lot of activities in different quarters," said one former government official who is familiar with U.S. national security satellite programs.

The intelligence report raised red flags about Beijing's ability to disrupt satellites in higher orbits, which could put the most sensitive U.S. spacecraft at risk, according to the sources. China has already conducted several anti-satellite tests at lower orbital levels in recent years.

Given the heightened concerns, Washington is keeping a watchful eye on Chinese activities that could be used to disrupt U.S. satellites. It is also urging Beijing to avoid a repeat of its January 2007 test that created an enormous amount of "space junk," said one senior defense official.

Details of the latest Chinese moves that have raised U.S. concerns remain classified.

U.S. officials charge that China's anti-satellite activities are part of a major military modernization that has seen Beijing test two new stealth fighters; step up cyber attacks on foreign computer networks; and launch more commercial and military satellites in 2012 than the United States.

China still lags behind the United States in most military fields.

"What we're seeing is a heightened sense in the United States that China is a potential threat and that it has the technology to be a threat if it wishes to," said Jonathan McDowell, with the Harvard-Smithsonian Center for Astrophysics.

"As China becomes a space superpower, and given that it does have a significant military component to its space program, it is inevitable that the U.S. will be concerned about threats to its most valued satellite systems, whether or not China actually intends to deploy such aggressive systems," he said.

CREATING SPACE DEBRIS

Six years ago, on January 11, 2007, China destroyed one of its own defunct weather satellites in low-earth orbit, which created over 10,000 pieces of debris that pose a threat to other spacecraft. A less-destructive test followed on January 11, 2010.

Space experts and U.S. officials say they expect China to continue testing anti-satellite technologies, although they doubt it would repeat the 2007 test, given the massive international outcry it triggered.

Gregory Kulacki, a respected researcher with the Union of Concerned Scientists, reported earlier this month on the group's website that there was "a strong possibility" of a new anti-satellite test by China within the next few weeks.

He said Chinese sources had told him in November that an announcement about an upcoming anti-satellite test had been circulated within the Chinese government, and a high-ranking U.S. defense official confirmed in December that Washington was "very concerned" about an imminent Chinese anti-satellite test.

The Chinese Defense Ministry did not respond to emailed queries by Reuters' Beijing office on the question.

The Pentagon said it was aware of reports predicting another test, but declined comment on what it called "intelligence matters."

"We monitor carefully China's military developments and urge China to exhibit greater transparency regarding its capabilities and intentions," said Lieutenant Colonel Monica Matoush.

Sources within the U.S. government and outside experts said there was no immediate evidence pointing to the preparations for the type of satellite or rocket launches used by China for past anti-satellite tests at lower orbits.

But they said Beijing could test its anti-satellite weapons in other ways that would be harder to detect, such as by jamming a satellite's signals from the ground or issuing a powerful electromagnetic pulse from one satellite to disable another.

China could also maneuver two satellites very close together at higher orbits, replicating actions it has already taken in lower orbits in August 2010 and November 2010. Such activities could be used to perform maintenance or test docking capabilities for human spaceflight, but could clearly be used for more destructive purposes as well, they said.

The United States has continued to test its own anti-satellite capabilities. In February 2008, a missile fired from a U.S. Navy cruiser in the north Pacific destroyed an ailing American satellite in orbit.

The U.S. government said the satellite's toxic fuel posed a risk upon re-entry of the earth's atmosphere. Skeptics said the test was a message to China.

Any further anti-satellite test by China would be troubling, especially if it occurred at higher altitudes, said Bruce MacDonald, a former White House official who is now a senior director at the U.S. Institute of Peace.

The United States operates its fleet of Global Positioning System (GPS) satellites in medium earth orbit about 11,000 miles above the surface of the earth, while U.S. military communications and early missile warning satellites are located in geostationary orbit 22,000 miles above the equator.

Brian Weeden, technical adviser for the nonprofit Secure World Foundation and a former Air Force space and missile expert, said a Chinese anti-satellite test at those higher orbits would put U.S. satellites at risk.

"Some critical U.S. assets in that region have been assumed for the most part to be safe from those kind of attacks," he said. "Such tests would signal that they're not."

Table of Contents

'Red October' Cyber-Attack Found By Russian Researchers

By Dave Lee, BBC News, 14 January 2013

A major cyber-attack that may have been stealing confidential documents since 2007 has been discovered by Russian researchers.

Kaspersky Labs told the BBC the malware targeted government institutions such as embassies, nuclear research centres and oil and gas institutes.

It was designed to steal encrypted files - and was even able to recover files that had been deleted.

One expert described the attack find as "very significant".

"It appears to be trying to suck up all the usual things - word documents, PDFs, all the things you'd expect," said Prof Alan Woodward, from the University of Surrey.

"But a couple of the file extensions it's going after are very specific encrypted files."

In a statement, Kaspersky Labs said: "The primary focus of this campaign targets countries in Eastern Europe, former USSR Republics, and countries in Central Asia, although victims can be found everywhere, including Western Europe and North America.

"The main objective of the attackers was to gather sensitive documents from the compromised organisations, which included geopolitical intelligence, credentials to access classified computer systems, and data from personal mobile devices and network equipment."

'Carefully selected'

In an interview with the BBC, the company's chief malware researcher Vitaly Kamluk said victims had been carefully selected.

"It was discovered in October last year," Mr Kamluk said.

"We initiated our checks and quite quickly understood that is this a massive cyber-attack campaign.

"There were a quite limited set of targets that were affected - they were carefully selected. They seem to be related to some high-profile organisations."

Red October - which is named after a Russian submarine featured in the Tom Clancy novel The Hunt For Red October - bears many similarities with Flame, a cyber-attack discovered last year.

Like Flame, Red October is made up of several distinct modules, each with a set objective or function.

"There is a special module for recovering deleted files from USB sticks," Mr Kamluk said.

"It monitors when a USB stick is plugged in, and it will try to undelete files. We haven't seen anything like that in a malware before."

Also unique to Red October was its ability to hide on a machine as if deleted, said Prof Woodward.

"If it's discovered, it hides.

"When everyone thinks the coast is clear, you just send an email and 'boof' it's back and active again."

Cracked encryption

Other modules were designed to target files encrypted using a system known as Cryptofiler - an encryption standard that used to be in widespread use by intelligence agencies but is now less common.

Prof Woodward explained that while Cryptofiler is no longer used for extremely sensitive documents, it is still used by the likes of Nato for protecting privacy and other information that could be valuable to hackers.

Red October's targeting of Cryptofiler files could suggest its encryption methods had been "cracked" by the attackers.

Like most malware attacks, there are clues as to its origin - however security experts warn that any calling cards found within the attack's code could in fact be an attempt to throw investigators off the real scent.

Kaspersky's Mr Kamluk said the code was littered with broken, Russian-influenced English.

"We've seen use of the word 'proga' - a slang word common among Russians which means program or application. It's not used in any other language as far as we know."

But Prof Woodward added: "In the sneaky old world of espionage, it could be a false flag exercise. You can't take those things at face value."

Kaspersky's research indicated there were 55,000 connection targets within 250 different IP addresses. In simpler terms, this means that large numbers of computers were infected in single locations - possibly government buildings or facilities.

A 100-page report into the malware is to be published later this week, the company said.

Table of Contents

Influence Operations and the Internet: A 21st Century Issue

Legal, Doctrinal, and Policy Challenges in the Cyber World

By Col Rebecca A. Keller, USAF, Maxwell Papers #52, Air University, Oct 2010

The conduct of information operations (IO) by the US military, which includes military deception (MILDEC) and psychological operations (PSYOP), is based on doctrinal precedence and operational necessity. The increasing use of cybertechnology and the Internet in executing IO missions offers technological advantages while simultaneously being a minefield fraught with legal and cultural challenges. Using Joint and Air Force doctrinal publications, published books, and academic papers, this thesis defines relevant terminology and identifies current operational and legal constraints in the execution of IO using cybertechnology. It concludes with recommended remediation actions to enhance the use of the Internet as a military IO tool in today's cyber world.

Primer on Influence Operations

According to Joint Publication (JP) 3-13, Information Operations, IO is "integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies . . . [in order] to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[1] Two of the five core capabilities of IO are PSYOP and MILDEC, while Public Affairs (PA) is considered an IO-related capability.[2] All three are inherent in the conduct of military operations from peacetime to wartime and are increasingly affected by cyber technology. In order to understand these missions, it is important to first explain their definitions and functions.

According to JP 3-13.4, Military Deception, short of perfidy, the intent of MILDEC is the execution of actions "to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and

operations."[3] Deception has been a recognized component of war for millennia; nearly 2,500 years ago, Chinese military strategist Sun Tzu stated "all warfare is based on deception."[4] In modern times, two classic examples of military deception are (1) Operation Mincemeat, the World War II deception strategy that convinced the Germans that the Allies were preparing to invade Greece instead of Italy, and (2) a perfectly executed ruse by the Egyptians and Syrians giving the appearance of a military exercise. Instead, they initiated the 1973 Arab-Israeli War, catching the Israelis completely off guard.[5]

While MILDEC is customarily a wartime mission, PSYOP is conducted during all phases of military operations, including peacetime, and is authorized under Title 10, section 167 of the US Code, which allows the Department of Defense (DOD) to conduct PSYOP as part of special operations campaigns.[6] JP 3-13.2, Psychological Operations, states the purpose of PSYOP is to influence foreign audience perceptions and behavior as part of approved programs supporting US policy and military objectives.[7] Since World War I, the United States has released psychological leaflets across enemy lines to persuade and influence behavior. Other traditional forms of PSYOP include ground-based and airborne loudspeaker or radio broadcasts to foreign audiences and show-of-force missions where military ground personnel, aircraft, or ships visibly remind foreign nations of US combat capabilities.

Propaganda is "a form of communication aimed at influencing the attitude of a community toward some cause or position."[8] While historically not a pejorative term, the terms PSYOP and propaganda are often freely interchanged and have taken primarily derogatory connotations. This is in spite of the fact that both provide important national security tools and are truthful in content during the execution of conventional military operations.

Where PSYOP and propaganda are communications directed at foreign audiences, military PA offices provide similar information to journalists and the American public to articulate DOD positions on policies and operations. The same principles based upon the freedom of the press that guide civilian journalists also guide the activities of PA professionals. Military PA responsibilities are captured in JP 3-61, Public Affairs—"providing truthful, accurate and timely information . . . to keep the public informed about the military's missions and operations, countering adversary propaganda, deterring adversary actions, and maintain[ing] trust and confidence of the US population, and our friends and allies."[9] Even Pres. Abraham Lincoln understood the importance of interacting with the public, stating, "Public opinion is everything. With it, nothing can fail. Without it, nothing can succeed."[10]

The requirement to influence foreign attitudes and behaviors is not unique to the DOD; the Department of State's (DOS) public diplomacy efforts can often overlap with military PSYOP or PA activities. Out of necessity, DOS public diplomacy and military PA distance themselves from the highly controversial MILDEC, PSYOP, and propaganda mission sets in order to maintain a sense of credibility and operational effectiveness which is "predicated on [the] ability to project truthful information to a variety of audiences."[11]

Impact of Cybertechnology on Influence Operations

Increasingly, the use of the cyber domain is being actively researched and exploited by the United States and its adversaries to conduct influence operations via cell phone, e-mail, text message, and blogs in both peacetime and combat environments. The cyber world will progressively become both a boon and a bane to IO personnel, allowing a global audience reach but providing a large vulnerability to enemy deception and PSYOP efforts requiring a near immediate response to worldwide operational events.

While traditional forms of MILDEC—operational feints, displays, or instances of camouflage and concealment—are increasingly negated by advancements in intelligence, surveillance, and reconnaissance technology that quickly uncover the deception, cybertechnology has brought a new generation of MILDEC options to military planners.[12]

These include digital imagery manipulation, computer file alteration, and false file storage where phony or deceptive electronic files are deliberately made accessible to an adversary.

Ubiquitous Internet availability and the global use of cell phones present new opportunities for PSYOP efforts. The proliferation of cell phone ring tones offers options for embarrassment or message delivery.[13] For instance, altering a terrorist cell chief or military leader's ring tone to the refrain "God bless the USA" would cause embarrassment or shame when triggered to ring within earshot of subordinates or superiors. Additionally, some cell phone frequencies are "not detectable to people over the age of 30, while those younger than 30 can hear the frequency," which enables a targeted audience for some messages.[14] Student revolutionaries in an adversary's country could be targeted to encourage their antiestablishment activities. In theory, the student could be alerted to a new text message or voice mail with a high-frequency alert tone audible to them without tipping off older, anti-American parents, teachers, or government officials.

The traditional airborne psychological leaflet has been modernized by an Internet version called an "E-flet," and the loudspeaker is being superseded by text messages delivered to cell phones and called the "silent loudspeaker."[15] Messages can even be sent to specific cell phone towers in a given geographic area, thus enabling regular news updates to a target audience to be sent.[16] Again, the student protestors in an adversary's country could be targeted to receive text messages supporting their activities.

Web sites like YouTube and other social networking sites have become a battleground for "a global audience to share firsthand reports, military strategies, propaganda videos, and personal conflict as it unfolds."[17] This public participation in conflict blurs the lines between combatant and noncombatant when operational data is involved. New counterpropaganda tools aided by the Internet combat this trend.

One method to fight foreign propaganda and lies is for the United States to use a blog or Web site in native languages to educate foreign citizens on political issues and to influence attitudes and advance education on a topic area. For example, if a country holds a constitutional referendum to do away with presidential term limits and the incumbent president is not a US ally, the United States could use the Internet to educate the citizens about the significance and impact of the referendum prior to the vote. Another example is "alert" software, such as "Megaphone," that notifies a special interest group about chat rooms or Internet polls that are counter to their special interest. This alert enables a counterpropaganda response and offers alternate or contradictory views.[18]

The importance of proactively capitalizing on the new range of cyber tools in performing IO missions is surpassed only by the requirement to identify and provide a defense against similar efforts by opponents.

Challenges to Effective Information Operations

While the lanes in the road between MILDEC, PSYOP, and PA seem clear cut in doctrine and theory, cyber operations have blurred the lines between operational missions and authorities due to outdated US laws, Internet technology, global media, and transnational threats. Seven challenges highlight conflicts and uncharted cyber areas in IO that must be addressed if the United States' national defense is not to be left vulnerable, both legally and defensively. If these areas are not addressed, the United States risks not only the ability to conduct effective cyber-related influence operations but also the capability to effectively employ military instruments of power throughout the range of operations from peacetime to wartime and defend against the same.

Keeping the American Public Informed

The American public plays a large role, both directly and indirectly, in the arena of influence operations. Doctrinally, "MILDEC operations must not intentionally target or mislead the US public, the US Congress, or the US news media."[19] This insulation of the US public from US deception operations is understandable; however, it also leaves the United States vulnerable to foreign deception and propaganda efforts and "a questioning mind is the first line of defense."[20] Therefore, the general public should be taught how to identify and respond to propaganda, PSYOP, and deception operations launched by any foreign nation or other entity.

In the 2006 war between Israel and Hezbollah, Israel launched an airstrike on 30 July 2006 that allegedly killed as many as 57 civilians. It was later called the Qana massacre in the significant international media coverage.[21] Ultimately, in light of post-battle assessment, the Qana massacre was determined to actually be "a stage-managed Hezbollah production, designed precisely to enflame international sentiment against Israel and compel the Israelis to accept a ceasefire that would enable the jihad terrorist group to gain some time to recover from the Israeli attacks."[22] The Hezbollah manipulated the attack timeline and doctored photos of recovery workers and corpses to make the air strike appear genocidal and to cover up the military nature of the target. The inconsistencies in the images and the timeline of events were evident upon close scrutiny. Awareness of this type of deception must be developed in the American public and military personnel.

Legal Challenges to Combatant Command Responsibilities

In June 2007, the deputy secretary of defense (DEPSECDEF) issued a "Policy for Department of Defense (DOD) Interactive Internet Activities" memo authorizing the geographic combatant commands to provide information to foreign audiences via two-way communications—e-mail, blogs, chat rooms, and Internet bulletin boards.[23] A "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences" followed in August 2007, which further authorized geographic COCOMs to produce and maintain "regionally-oriented websites" with "non-interactive" content for foreign audiences.[24] By direction, the Web site data must be accurate, truthful, and, in all but cases of operational necessity, attributable. On the surface, it makes sense for a COCOM to use interactive Internet activities (IIA) and regionally focused Web sites to counter extremist activity and thwart pro-terrorist mind-sets as well as to advance US political-military interests overseas. However, IIA as defined and structured is the legal responsibility of the DOS and not the DOD.[25]

The legal crux of the issue is whether these activities are PSYOP, which is a legally defined military mission set, or if they fall into the area of public diplomacy, which is the sole jurisdiction of the DOS.[26]

While the DEPSECDEF policy letters did direct interagency cooperation with the DOS for international engagement, the term PSYOP is never used to define DOD activities. The DOD has limited congressional authority to conduct public diplomacy, and once it "no longer labels its communication measures as PSYOP, it potentially subverts its own statutory authorities to engage foreign audiences."[27] At its core, IIA is public diplomacy conducted as a military mission, yet the appropriation of funds and the use of contractor support for foreign engagement via public diplomacy are more in line with congressional appropriations targeted to the DOS rather than the DOD.[28]

Modernizing the Smith-Mundt Act

Related to the discussion of geographic COCOM and DOS responsibilities are the legal boundaries in the conduct of US propaganda instituted by the Smith-Mundt Act. Passed in 1948, the US Information and Education Exchange Act, also known as Smith-Mundt, was enacted to counter the worldwide communist propaganda being released by the Soviet Union during the Cold War era. "The Act's principles are timeless: tell the truth; explain the motives of the United States; bolster morale and extend hope; give a true and convincing picture of American life, methods and ideals; combat misrepresentation and distortion; and aggressively interpret and support American foreign policy."[29] In other words, create a forum for the international release of American news and information (propaganda) to counter the communist propaganda from the Soviet Union, which was "defaming our institutions in the eyes of the peoples of the world."[30]

The result was the creation of the US Information Agency (USIA), now a part of DOS, to undertake the mission. Additionally, some well-known media entities are also covered by the Smith-Mundt Act (Voice of America [VOA], Radio Free Asia and Europe, and Radio and TV Marti). A domestic dissemination clause was further strengthened by Congress in 1972 and 1985 to completely "block Americans from accessing USIA materials to the point USIA products were exempt from the Freedom of Information Act."[31] In essence, US citizens cannot be trusted to have access to the truthful materials promoting American ideals that are available to the rest of the world.

With the collapse of the Soviet Union and the worldwide communist threat, as well as the shrinking of the world due to the cyber age, a number of Smith-Mundt constraints have outlived their usefulness. First, the Smith-Mundt Act restrictions only cover the current DOS activities previously conducted by USIA, and not those of the entire US government. A 2006 legal review requested by the Defense Policy Analysis Office concluded that "the Act does not apply to the Defense Department."[32] However, based upon implicit congressional support for the act that extends to the government, the DOD has applied the restrictions in its COCOM public outreach activities.[33]

The Internet and satellite radio have also made it impossible to separate domestic from international audiences, calling into question whether it is illegal for online products supposedly covered by Smith-Mundt (a DOS or COCOM article produced for foreign consumption) to be accessible by American citizens.

Finally, the ability of the Department of Homeland Security (DHS) and US Northern Command to counter radical ideological products of terrorists, foreign and domestic, requires US truthful information developed by the DOS to be made available. For example, a Minneapolis, Minnesota, community radio station requested permission to rebroadcast a VOA news show that targeted Somalians. The intent was to "offer an informative, Somali-language alternative to the terrorist propaganda that [was] streaming into Minneapolis," home of the largest Somali community in the United States.[34] The VOA, as regulated by the Smith-Mundt Act, denied the request. This example highlights a new strategic vulnerability, the inability to combat a transnational terrorism threat within our own borders.

Countering Adversary Influence Operations

While Smith-Mundt prohibits dissemination of US influence information to American citizens, no corresponding law prohibits foreign nations or organizations from targeting US citizens with propaganda and/or deception. The lack of public awareness of this threat and the proliferation of cheap means for global message distribution leave the US public vulnerable to influence operations (propaganda) and deception by adversaries and other nations. This can include altered imagery, intentional falsehoods, and planted rumors. Some modern examples of influence operations against the US public include the Soviet KGB spreading "bogus stories linking the United States to the creation of HIV/AIDS . . . and [accusing the United States of] employing a Korean civilian airliner as a reconnaissance aircraft over the Kamchatka peninsula. [Additionally], John Kerry appeared in an altered image seated near Jane Fonda at an anti-Vietnam War rally."[35]

In order for Americans to recognize another nation's propaganda, the American educational system should have an information literacy program to ensure that US citizens "have the ability to distinguish truth from falsehood when information is presented."[36]

Changing Pejorative Terminology

It seems that the modern usage of the terms propaganda and psychological operations is generally viewed by Americans as pejorative in nature, in spite of the fact that conventional military IO missions are truthful and accurate. As Hubert H. Humphrey once said, "In real life, unlike in Shakespeare, the sweetness of the rose depends upon the name it bears. Things are not only what they are. They are, in very important respects, what they seem to be."[37]

Unfortunately, the words propaganda and psychological operations have evolved in usage over the past half century to imply deceit and trickery. Thus, the harmful connotation in the minds of Congress, the American public, and even some military leaders impacts negatively on the ability of the US military to effectively conduct influence operations, even truthful ones. When discussions of DOD information operations are made public, the potentially positive effects of the operations are overshadowed by the negative association of the terms themselves. Because the derogatory connotation associated with today's IO terminology can negatively impact the conduct of the mission and the ability to communicate, a name change should be considered.

Loss of High Ground in the Information Domain

That the United States has no peer competitor in conventional war fighting is not in question. However, the use of nonconventional, asymmetric techniques, particularly those enabled by the Internet, allows nonpeer competitor nation-states and nonnation-state actors a strategic equivalence or an advantage not found in conventional settings. During past conventional conflicts, the US military PA structure could effectively manage the information released to the public by civilian combat newsmen, protecting operations and personnel. However, today's technology, such as the cell phone, enables everyone the "capability to transmit audio, video and photographs . . . [and] such contributions from the street carry their own form of psychological persuasion."[38] Any incident occurring in a conflict today can be reported, correctly or incorrectly, via Internet chat room, YouTube, cell phone, or text messaging—long before a "legitimate news service can adjudicate its authenticity."[39] A cell phone enables a group, or even an individual, the ability to conduct unilateral psychological or deception operations against the US, negatively impacting both peacetime and wartime missions by influencing public opinion. This can put pressure on public officials and military leadership regarding conduct, expected outcomes, and even the duration of combat operations.

With the growing dependence on the use of interconnected networks to function in an e-commerce society, cyber weapons are rapidly becoming the "nuclear weapon" of the millennial age. In the past, nuclear weapons were considered the ultimate deterrent and battlefield equalizer, which prompted the creation of international controls on development and possession of such technology. Fortunately, the cost of a nuclear weapons program was prohibitive to all but a handful of sovereign nations. But cybertechnology is inexpensive, easy to obtain, and ubiquitous, thus offering an asymmetric advantage to adversaries, state sponsored and otherwise, to conduct "quite literally, war on the cheap."[40] As a result, it is incumbent upon the US military IO community to develop tactics, techniques, and procedures (TTP) for using the new technologies. The military must become proficient in the identification and defeat of foreign attempts at IO and learn to release "precision guided messages . . . to target friendly or enemy soldiers with equal ease."[41]

Defining Neutrality in Cyber Operations

The 1907 Hague Convention requires combatant nations to recognize the rights of neutral nations and that the territory of a neutral nation is inviolable by combatant nations.[42] The latter neutrality specification causes many questions and is ill defined relative to the realm of cyber operations. The century-old Hague Convention was written when sovereign borders and national boundaries were purely geographic in nature. It must now be reconsidered in the cyber age.

Specifically, the Hague Convention states that, "belligerents may not move forces, weapons, or war materiel across a neutral country's territory, or conduct hostilities within a neutral's territory, waters, or airspace. A neutral nation jeopardizes its status if it permits belligerents to engage in such violations."[43] Two primary Internet-based examples highlight the difficulty of applying international laws of neutrality as they pertain to cyber operations—the use of a neutral country's cyber infrastructure and execution of cyber missions that cross neutral borders.

During the 2006 Israeli-Hezbollah conflict, Israel bombed the Al-Manar facilities in Lebanon prompting Al-Manar (an organization outlawed in the United States due to its jihadist activities) to rehost its operations on an Austin, Texas–based server owned by Broadwing Communications.[44] The nature and intent of this rehosting were apparently unknown to Broadwing at the time. It could be argued that Hezbollah is not a

sovereign state and the Al-Manar jihadist organization is not a legal combatant, so the Hague and Geneva neutrality conventions were not in play. However, this scenario and similar others demand some very intricate legal discussion on neutrality when cyber conflict occurs between nation-states and nonnation-states, especially the legal and practical consequences of a belligerent "occupying" a neutral nation's cyber infrastructure.

Another example of Internet re-hosting by a belligerent took place in July 2008 in the cyber portion of the conflict between Russia and Georgia. When the Georgian government's Internet capabilities were rendered virtually nonfunctional by a Russian denial of service attack, Tulip Systems, a US Internet hosting company in Atlanta, "contacted [the] Georgian government officials and offered assistance in reconstituting Georgian Internet capabilities."[45] While Tulip Systems provided this assistance without the knowledge or permission of the US government, it calls into question the status of US neutrality during the cyber conflict between these two belligerents. Can a sovereign nation lose its neutral status based upon the unilateral actions of a single citizen?

Another gray area in the realm of cyber neutrality deals with influence operations and the release of E-flets, text messages, or deception efforts (such as altering the contents of a Web site) that involve crossing sovereign borders with respect to physical infrastructure. Similar to the conventions limiting belligerents' use of radio towers and broadcast equipment in neutral countries, does the execution of a cyber mission traveling across a neutral country's web infrastructure violate international neutrality laws? The neutrality laws must be modernized or the negative impact to the DOD is obvious.

Recommended Changes to Doctrine and Policy

The breadth of questions raised by the use of cybertechnology in the prosecution of influence operations requires further investigation and correction. To deal with the challenges discussed in the previous section, the following represent some suggested remediation efforts.

As a public service, DHS needs to develop and implement an IO education campaign to develop critical thinking skills to assist the American public in identifying foreign propaganda and deception encountered on the Internet and in cyber media. Additionally, business owners of Internet servers would receive education on how their actions in hosting or assisting corporations or nations in countries under cyber attack could put the United States in jeopardy of losing its neutral status and unintentionally becoming a warring party within a conflict.

The DOD must determine whether new legal authorities to undertake Internet-based communications and Web site interactions with foreign audiences are required, as directed by secretary of defense policy letters of 2007. Regardless, the DOD must inform Congress of its public diplomacy (vice PSYOP) efforts and may even need to leave public diplomacy responsibilities to the DOS.[46]

"Congress must undo changes to the Smith-Mundt Act that prevent accountability and effective global engagement. This language, inserted in the 1970's and 1980's, prevents transparency and awareness while ignoring the global movement of information and people."[47]

Congress must amend Smith-Mundt to remove the ban on domestic dissemination of materials originally developed for foreign audiences. "In this age of communication without borders, the existence of such statutory language only subverts America's most powerful tool of soft power: our ideals."[48]

Change the terms propaganda and PSYOP to something less pejorative to the American public. Hubert H. Humphrey once stated, "Propaganda, to be effective, must be believed. To be believed, it must be credible. To be credible, it must be true."[49] Given that IO and PA activities in conventional military operations are factual and truthful, the pejorative terms in use hinder the accomplishment of the mission. New terminology could be as simple as operational communications, strategic effects, broadcast operations, or CYOP (cyber psychological operations).[50]

Update US influence operations doctrine to include cybertechnology. Specifically, develop TTPs for employing PSYOP, MILDEC, and PA using the new cybertechnology. Once developed, the TTPs must be incorporated into all applicable military exercises to allow the military IO operator an avenue for developing proficiency in the release of "precision-guided messages" to foreign audiences.[51]

Codify a US cyber policy on cyber neutrality that includes belligerent and neutral nation responsibilities. Since international law is often derived from common practice, the United States can be in the forefront of shaping international cyber neutrality laws and sovereign nation responsibilities when a "belligerent takes cyber refuge in a neutral country's territory."[52] Ultimately, this requires a worldwide collaborative effort to "create a single set of cyber laws and procedures internationally in order to insure that there is no safe harbor for cyber criminals."[53] Cyber criminals would include state and non-state actors threatening our security.

Putting It All Together—Operational Examples

Assuming all of the previous challenges are addressed and resolved, the following example summarizes how the military commander can benefit from information operations in the cyber age. The examples use radical Islamic extremists as the notional enemy.

As radical Islam extremists expertly use the Internet and global media to publicize and advance their propaganda and lies, an educated American civilian and military population can recognize misinformation and deception using critical thinking skills, asking hard questions, and seeking alternate or corroborating sources of information before making judgments or believing the foreign stories. With a Smith-Mundt Act modification, DHS, in conjunction with the Northern Command, can provide a direct counterinformation campaign within US borders via the Internet, radio, and television (in English and other foreign languages). This campaign will reduce the domestic threat from misinformed potential terrorist recruits living in the United States.

Once cyber TTPs are codified and a well trained cadre of military professionals developed, the combatant commander will be able to informationally bombard Islamic terrorists and their potential supporters by sending precision-guided messages to specific cell towers, cell phones, e-mail, or Web sites as part of a public diplomacy or CYOP effort.[54] The ability to incorporate these tools as standard procedures will enhance a counterinsurgency campaign by actively persuading less radical terrorists and sympathizers to give up the fight without resorting to expensive (both monetarily and socially) conventional warfare.

Once international norms are established for cyber-based laws of armed conflict, commanders will better understand legal boundaries to recognizing, initiating, and defending against cyber warfare. This, in turn, leaves a training and education task for both the military professionals and the American information technology public. But, until those norms are codified, the United States is at risk of unintentionally becoming a belligerent in other countries' conflicts, having our military and civilian cyber professionals unwittingly held liable under the international court of justice or not recognizing that a cyber war attack has taken place against our nation, thus forfeiting our opportunity for a prompt and appropriate response.

Conclusion

The remediation actions and operational examples outlined in this thesis are not exhaustive and still leave a large gray area in the realm of influence operations and the use of cybertechnology. They do represent a start, however, in identifying doctrinal gaps, outdated legal roadblocks, and deficiencies in policies, laws, and education. The United States must "amend existing policies to allow [influence operations] to embrace the range of contemporary media . . . as an integral asset" to military operations.[55] These changes would provide structure to largely disorganized and unnecessarily constrained efforts to fully employ cybertechnology and provide a new opportunity for the United States to conduct effective and efficient influence operations using that technology. Without addressing these challenges promptly, the national security of our nation is at risk in current and future conflicts.

Notes

1. JP 3-13, Information Operations, 13 February 2006, I–1.

2. Ibid., II–8–9.

3. JP 3-13.4, Military Deception, 13 July 2006, vii. Perfidy is "the use of unlawful or prohibited deceptions. Acts of perfidy are deceptions designed to invite the confidence of the enemy leading to the belief that he/she is entitled to, or is obliged to accord, protected status under the law of armed conflict, with the intent to betray that confidence. Acts of perfidy include but are not limited to: feigning surrender or waving a white flag to lure the enemy into a trap; misusing protective signs, signals, and symbols to injure, kill, or capture the enemy; using an ambulance or medical aircraft marked with the red cross or red crescent to carry armed combatants, weapons, or ammunition in order to attack or elude enemy forces; and using false, deceptive, or neutral flags, insignia, or uniforms [in actual combat]." Ibid., I-8.

4. Sun Tzu, The Art of War, ed. and trans. Samuel Griffith (London: Oxford University Press, 1963), 66.

5. JP 3-13.4, Military Deception, I–7. A ruse is "a cunning trick designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary." Ibid., I-7.

6. Daniel Silverberg and Joseph Heimann, "An Ever-Expanding War: Legal Aspects of Online Strategic Communication," Parameters, Summer 2009, 80.

7. JP 3-13.2, Psychological Operations, 7 January 2010, vii.

8. Wikipedia, s.v. "Propaganda," http://en.wikipedia.org/wiki/Propaganda (accessed 25 January 2010).

9. JP 3-61, Public Affairs, 9 May 2006, xi.

10. Ibid., II–1

11. Air Force Doctrine Document (AFDD) 2-5, Information Operations, 11 January

2005, 5.

12. JP 3-13.4, Military Deception, I–7. A feint is "an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary of the location and/or time of the actual main offensive action." Displays are "the simulation, disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the military deception story. Such capabilities may not exist but are made to appear so (simulations)." Ibid., I-7.

13. Timothy L. Thomas, "Hezballah, Israel, and Cyber Psyop," IO Sphere, Winter 2007, 31.

14. Ibid.

15. Ibid.

16. Ibid., 32.

17. Ibid.

18. Ibid.

19. JP 3-13.4, Military Deception, II–8

20. Scot Macdonald, Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations (New York: Routledge, 2007), 178.

21. Robert Spencer, "Stage-Managed Massacre," Frontpagemag.com, 2 August 2006, http://97.74.65.51/readArticle.aspx?ARTID=3281 (accessed 13 February 2010).

22. Ibid.

23. Gordon England, deputy secretary of defense, "Policy for Department of Defense (DOD) Interactive Internet Activities," policy memorandum, 8 June 2007.

24. Gordon England, deputy secretary of defense, "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," policy memorandum, 3 August 2007.

25. Silverberg and Heimann, "Ever-Expanding War."

26. Ibid., 78

27. Ibid.

28. Ibid.

29. Matt Armstrong, "Smith-Mundt Act," Small Wars Journal, 28 July 2008.

30. Ibid.

31. Ibid.

32. Ibid.

33. Ibid.

34. Matt Armstrong, "Censoring the Voice of America," Foreign Policy, 6 August 2009.

35. Macdonald, Propaganda and Information Warfare, 182.

36. Ibid.

37. Hubert H. Humphrey, Quoteopia.com, http://www.quoteopia.com/famous.php?quotesby=huberthhumphrey (accessed 13 February 2010).

38. Thomas, "Hezballah, Israel, and Cyber Psyop," 30.

39. Ibid.

40. Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, research publication (Colorado Springs, CO: Institute for Information Technology Applications, 1999), 10.

41. Thomas, "Hezballah, Israel, and Cyber Psyop," 30.

42. Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008–9, 62.

43. Ibid.

44. Thomas, "Hezballah, Israel, and Cyber Psyop," 33.

45. Korns and Kastenberg, "Georgia's Cyber Left Hook," 67.

46. Silverberg and Heimann, "Ever-Expanding War," 90.

47. Armstrong, "Smith-Mundt Act."

48. Gregory L. Garland, "Editorials and Op-Eds," AmericanDiplomacy.Org, 3 January 2009, www.unc.edu/depts/diplomat/item/2009/0103/ed/garland_smithmundt.html (accessed 23 October 2009).

49. Hubert H. Humphrey, BrainyQuote.com, http://www.brainyquote.com/quotes/authors/h/hubert_h_humphrey_2.html (accessed 13 February 2010).

50. Thomas, "Hezballah, Israel, and Cyber Psyop"; and AFDD 2-5: Information Operations, 30.

51. Thomas, "Hezballah, Israel, and Cyber Psyop."

52. Korns and Kastenberg, "Georgia's Cyber Left Hook," 66.

53. Paul Rosenzweig, "National Security Threats in Cyberspace," McCormick Foundation Conference series (Wheaton, IL: McCormick Foundation, 2009), 30.

54. Thomas, "Hezballah, Israel, and Cyber Psyop."

55. Angela Maria Lungu, "War.com: The Internet and Psychological Operations," Joint Forces Quarterly, Spring/Summer 2001, 13–17.

Abbreviations

AFDD Air Force doctrine document
COCOM combatant command
CYOP cyber psychological operations
DEPSECDEF deputy secretary of defense
DHS Department of Homeland Security
DOD Department of Defense
DOS Department of State
E-flet Internet psychological leaflet
IIA interactive Internet activities
IO information operations
JP joint publication MILDEC military deception PAPublic Affairs
PSYOP psychological operations
TTP tactics, techniques, and procedures
USIA US Information Agency
VOA Voice of America

Table of Contents

When the Network Dies

The Army lacks the battle drills that would help it fight on

By Lt. Col. Michael J. Lanham, Armed Forces Journal, Dec 2012

Unprepared soldiers are ineffective soldiers, and the rise of the networked battle space has made this ancient wisdom no less true.

It is curious, then, that when the Army practices operating in contested cyberspace environments, it does so largely in echelons above corps and not throughout the force. What exercises do take place generally understate the likely effects of network outages and overstate our ability to adapt to them.

If we continue to avoid rigorous rehearsal for cyber attack, or fail to implement it at all levels, we are training to meet incompetent adversaries and setting the stage for improvised, ill-coordinated and ineffective responses to competent ones.

Just as the Army has done for every other aspect of combat, it needs to develop a set of battle drills for such environments and work them into the standard training regimen at each echelon of command. These drills must include individual and collective tasks of the sort that would prepare soldiers, commanders and units to face many varieties of cyber events: short- and long-duration, point and pervasive, man-made and natural. To make this practical, we must also give units at all levels the modeling and simulation capabilities they need to hone their defenses, responses and training efforts.

What We Do

What are our current capabilities and willingness to conduct rigorous rehearsals of operations in contested cyberspace environments?

Before addressing that explicit question, we should acknowledge that there are certainly concerns with authority to conduct rehearsals — unlike tankers skirmishing at the National Training Center, cyber warriors often hone their craft on the actual Internet — but I'll defer such a discussion and presume there are safe, legal, moral and ethical ways of getting better at our jobs.

We should also properly frame what we wish to accomplish. I'm going to borrow an idea from Maj. Gen. Richard Webber, a past commander of the 24th Air Force, his service's component of U.S. Cyber Command. His vision of his command was that he and his airmen will provide "mission assurance," not "information assurance" — that is, that his main goal is not to defend computers per se but rather to assure commanders that they can continue their missions in contested cyber environments. The Army uses different vocabulary, but it's apparent that these two Cyber Command service components share a view.

To that end, the Department of Defense holds rehearsals for cyber attack; these exercises go by names such as Cyber Flag, Bulwark Defender, Turbo Challenge and Cyber Endeavor. But these are largely echelons-above-corps exercises, and the ways we execute them are insufficiently rigorous.

Too often, exercise commanders and planners make fundamental assumptions about retained availability or unrealistically rapid restoration of cyber resources. The exercises tend to be short-duration, not long-duration; to feature degradations or losses of limited scope, not pervasive ones; and to clearly differentiate natural and man-made effects. This allows commanders and staffs to extrapolate impacts and reactions to circumstances they've not encountered. I'm confident readers can recall breezy hand-waving about operating through cyber outages, predictions of restoration of host-nation cyber capabilities despite high-altitude electromagnetic pulse detonations, and otherwise confident assertions that the collective "we" would overcome whatever nature or adversaries threw at us. I'm also confident those same anecdotes are colored by the remembered irritation and pain of actual cyber degradation or losses well below "Cyber Pearl Harbor" thresholds that were not planned, not rehearsed, not well-tolerated and were poorly muddled through by units at every echelon.

At the risk of over-generalizing, most cyber tabletop exercises and general officer-level leadership games I've been exposed to involved either too few (or too low-ranking) technical-oriented people to splash the cold water of technical realities on the attendees and too few maneuver commanders to splash the cold water of mission priorities beyond cyber on the technical-oriented folks.

An informal and unscientific poll of the Functional Area 53 and INTELST mail lists contributes to the notion that we are also not rehearsing well or often for cyber contingencies at echelons below corps. (By contrast, government officials — at least to judge by their quotes in the media — are quite worried about just these kinds of environments.)

What We Used to Do

Our collective failure to perform rigorous cyber-related rehearsals in the form of individual soldier tasks, unit tasks and integral parts of larger-purpose exercises stands in stark contrast to our preparations for threats in the 1980s and '90s. I recall two forms of contingency rehearsals I regularly executed as a platoon leader that could, with analogical reasoning, help us in contested cyberspace environments. The first was rehearsing

operations in persistent and nonpersistent chemical environments. The second was the use of radio listening silence, radio silence and signal operating instructions (SOIs) in platoon- through battalion-level operations.

For cyber strikes, what are our standard, rehearsed individual, small-unit or even battalion-level tasks and responses? One response, at an emotional level, could be relief: At last, we can operate without micro-management from afar! But the relief will likely be soon overtaken by confusion and improvisation. How will soldiers navigate when their commercial off-the-shelf mapping hardware and software stop working unless they have practiced using paper maps and lensatic compasses?

When plotting the coordinates of a chemical strike broadcast message, soldiers knew to avoid the affected coordinates and its downwind hazard areas. Can units identify and locate specific hazards from a broadcast cyber strike? Do we rely on cyber resources to broadcast alerts about cyber strikes or cyber malfunctions? Are reports from national or combatant-command-level entities sufficiently detailed to allow, say, D Company, 1-327th Infantry, 101st Airborne Division, to know it just received a cyber strike? How does a message from faraway entities even get to D Company? If a report contains an IP address with no other identifying information, are there rehearsed drills to identify the owning unit and the analogous downwind hazards? Can the Army, with high confidence, train soldiers and leaders to recognize adversary-caused cyber effects compared to self-induced problems — i.e., is that unscheduled and unannounced reboot of the commanding general's computer evidence of hostile action or just an ill-advised move by local IT support? Is the temporary loss of NIPR Wi-Fi at an installation a temporary glitch or a man-in-the-middle attack? Are immediate action drills for man-made degradations different from those for confirmed or suspected adversary actions? Are the differences purposeful and meaningful?

Certainly, the "identify and react to a chemical strike" battle drill is no perfect analogy to "cyber strike" battle drill. But it shows the kind of past competency that we must regain in the modern era. Years ago, we willingly put large numbers of people, including high-ranking commanders, through time-consuming and physically uncomfortable battle drills for biological and chemical environments. We developed expectations and rules of thumb for operating tempo slow-downs within planning staffs and standard operating procedures for mechanized and armored forces. At the battalion level, at least, these rehearsals led to confidence that a sufficiently small chemical strike would not inflict too great a casualty rate.

We have yet to consistently inconvenience high-level commanders or develop such expectations for cyber, although DoD leaders appear far more confident of future network attacks then we ever were of chemical strikes by the Soviets.

What We Can Do

A second contingency rehearsal we could resurrect would require us to use seemingly long-forgotten skills: operating without our networks and radios for extended periods of time across large battle spaces. Mechanized infantry used to lay communications wire between tracked vehicles when at long halts or in a laager. Soldiers used to use SOI-encoded messages and messengers/couriers for days. Tactical units may still practice these alternate and contingency ways of exercising command and control — but how fast does failover occur, and how comfortable are higher echelons without their data addictions being fed from their subordinates? I am dubious that staffs of division and higher units will find it trivial to work through the old-but-forgotten ways of commanding large outfits without the near-instant gratification of cyberspace capabilities.

Here are a few ways we might practice for such situations. Commanders at various echelons can:

- Self-inflict announced and unannounced reductions of bandwidth in our day-to-day networks: C2, medical, logistics, personnel, finance and contracting — that is, deliberately move to "soda-straw" levels compared to normal levels for days at a time.
- Coordinate with higher commands and request nondestructive defensive fires. A cyber analog could be isolating a network segment or cutting off all online connections except those to a white list of pre-approved, known safe systems.
- Rehearse defensive reconfigurations, deployments of cyber assets that would not be susceptible to the envisioned threat or other "cyber maneuvers."
- Practice failover and load-reduction to alternative transmission modes. If a host nation's communications fail, how does a unit behave when restricted to military or commercial satellite links?

Staffs can practice this, as can commanders. They might, for example, relay past orders from Cyber Command or elsewhere, ask for and implement their services' Cyber Command contingency plans and execute notional cyber defense orders that actually impinge on their perceptions of what's important. Brigade-and-above headquarters can practice reporting timelines that take hours or days instead of seconds or minutes

and practice collecting data with clipboards and grease pencils instead of Command Post of the Future and Tactical Integrated Ground Reporting. Crucially, they should practice these drills and tasks not only in garrison, but also during training center rotations. There's no use excluding unit training for deployment — Strategic and Cyber Command have already demonstrated that being "in the fight" is an insufficient rationale for ignoring cyberspace orders and directives.

Finally, non-maneuver forces must rehearse as well. Medical, logistics, acquisition, strategic intelligence, morale-welfare-recreation and other organizations should also practice cyber operations battle drills. How do they prioritize and continue their missions in the face of long-term or pervasive degradation? Can they send and receive messages up and down the chain of command sufficient for high-priority mission tasks? Can they receive reports from outside their day-to-day operations channels (e.g., Cyber Command or Army Cyber) about a bad computer? Do they have the manpower to find and fix dozens or hundreds of systems amid day-to-day or degraded operations? Can they react in ways short of self-inflicted denial of service to an entire installation, as happened at Fort Campbell in 2004? If the answers to these questions are not reasonably clear and rehearsed, no commander should have confidence in the answers' accuracy.

In short, we should periodically apply the enemy's most dangerous cyber course of action and work through how we adapt to it. We should resist the temptation to assume cyber capabilities will return to normal or near normal after only brief periods of interruption with no substantial or long-term degradation of operations. We should test our self-confidence with rigor, not blithely trust in our use of "superior" technology and information.

What We Need To Do This

Of course, there are challenges to all this. Full-participation exercises are expensive for units and the services to plan and execute. There are almost always more staff-recommended training objectives than commanders can reasonably fit into a schedule and budget.

With too few resources and too many demands, what are other options? Commands could pick the cyber-analogs of map exercises, tactical exercises without troops, or command-post exercises.

Here's another option, one that promises better preparation without much increase in cost: Use rapid, decentralized and customizable modeling and simulation tools. This suggestion raises a number of questions. For example, can such tools:

- Reflect the variety of knowledge, beliefs, practices, behaviors and capabilities possessed by soldiers, units, other services, other coalition partners and host nations?
- Adequately depict cyber capabilities, including specific systems and their dependencies, classified networks and communications mediums?
- Reduce our cyber rehearsal gap?

The answer to the first two questions is "yes, with caveats," but to the last, it is a definitive yes. We know this because such tools already exist. Leading research universities such as Carnegie Mellon University, George Mason University, Vanderbilt University and others have taken them from laboratory experiments to commercial applications.

One example of such a set of tools and workflow exists at Carnegie Mellon's Center for Computational Analysis of Social and Organizational Systems. Its AutoMap tool uses machine learning to quickly create models of organizations, which can then be used to analyze data flows, look at social networks and perform what-if experiments using agent-based simulations.

A staff might feed AutoMap a collection of documents that describe the organization: joint and service doctrine; descriptions of tactics, techniques and standard operating procedures; emails; reports; briefings; etc. The software can sort the documents' words and concepts into categories — agents, organizations, roles, beliefs, knowledge, tasks, resources, events, locations and actions — and create a complex representation of the organization.

The commander and staff can then take this socio-technical, multi-mode model and inflict simulated cyber attacks on their organizations. The tools for the assessment of the attacks' effects are already in wide use by the intelligence, counter-IED and service academy communities. Such tools include ORA, UCINet, Palantir, Pajek and Analyst Notebook. (Helpfully, the Joint IED Defeat Organization has produced side-by-side comparisons of these tools.)

The results of these simulated attacks may inspire confidence in one's cyber preparations. When the Air Force Research Lab used Air Force doctrine documents to model the service's Air Operations Centers, the resulting model indicated that the AOCs were significantly more resilient to cyber attack than a cursory review suggested. But these kinds of models can also reveal vulnerabilities in organizational structure, IT setup,

manning and processes. As commanders and staffs create adaptations, and possibly even solutions to the vulnerabilities, they can tweak their model and re-run the simulated attacks until they achieve a satisfactory response. Such simulations are certainly not proof or prediction of real-world success, but they allow us to move beyond gut feelings, personal opinions and hyperbole toward rigorous and repeatable experimentation.

All this can be done without disrupting a command's operational networks and with relatively little impact on the rest of the unit. The next step is staging soldier-in-the-loop exercises to calibrate the model to reality, and ultimately, developing battle drills to hone the unit's ability to carry out its missions under cyber attack.

Conclusions

From short-duration denial-of-service attacks to sophisticated advanced persistent threats, from seafloor landslides to high-altitude electromagnetic pulses, a vast range of potential network problems threaten our wired way of war. Yet rehearsing operations in contested cyber environments remains a capability gap at all Army echelons. If we fail to adequately plan and rehearse for adversaries that exploit that gap, we almost assure ourselves a difficult initial future fight and a hard slog out of an initial future mess.

Tools like AutoMap have drastically reduced the time, money and expertise needed to construct useful organizational models to just hours or days instead of the weeks to months needed by the Battle Labs. Best of all, the Army does not need to wait for gold-plated, grade-A M&S capabilities from a defense contractor that require a staff of statistical analysts and professional model builders. We can use capabilities coming out of our research universities, give them to soldiers and their commanders, and begin reducing the gap today.

Table of Contents

Cyber Operations: Bridging from Concept to Cyber Superiority

By Jan Kallberg and Bhavani Thuraisingham, Joint Forces Quarterly, Issue 68, 1st Qtr 2013

The United States is preparing for cyber conflicts and ushering in a new era for national security. The concept of cyber operations is rapidly developing, and the time has come to transpose the conceptual heights to a broad ability to fight a strategic cyber conflict and defend the Nation in a cohesive way. Richard M. George, a former National Security Agency official, commented on recent developments: "Other countries are preparing for a cyberwar. If we're not pushing the envelope in cyber, somebody else will."[1] Therefore, increased budgets are allocated to cyber operations research and education. The Defense Advanced Research Projects Agency (DARPA) Plan X (for which a formal solicitation has not yet been issued at the point of authorship) will, according to media outlets, give an additional infusion of $110 million to research in pursuit of cyber operational capacities. Herbert S. Lin of the National Research Council of the National Academy of Sciences commented, "They're talking about being able to dominate the digital battlefield just like they do the traditional battlefield."[2] Plan X adds to the DARPA budget of $1.54 billion for cyber research in the period 2013–2017.[3] Additional funds are allocated for a variety of Federal agencies.

The most desirable goal is to acquire cyber supremacy—global U.S. dominance in cyberspace that permits the secure, reliable conduct of operations by U.S. forces and related land, sea, air, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.[4]

Universities are instrumental in bridging from concept to methodology, tools, and implementation. They are the force multiplier of the cyber defense doctrine as research hubs, educating thousands in the civilian and military-contractor workforces, and as a provider of technical solutions to ensure mission success. It is pivotal for cyber superiority that institutions of higher learning are aligned with the strategic goals of our national cyber defense strategy and clearly understand its doctrinal underpinnings. Put differently, if cyber security research is driving in a different direction than the national cyber strategy, we are getting in trouble by creating a gap and a weakness that can be exploited by hostile parties. Not only do we lose the opportunity to acquire cyber superiority, but we also become the prey in cyberwar.

This article challenges the universities' abilities to provide support for the doctrinal change to cyber operations, mainly because of the overemphasis on information assurance and the lack of intra-university collaboration.[5] Another issue considered is that in case we fail to transpose the theory to broad implementation, adversaries may be watching and learning what we should be implementing. The support for this scenario is drawn from the development of armored warfare.

The Business of Information Security

Traditionally, information security research and education have been founded on the key concept of information assurance—actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Information assurance is often expressed in underlying subfields such as forensics, network security, and penetration testing. It is similar to positional warfare

displayed at the Western Front of World War I. The front would be quiet for a long period, then an attack would erupt in heavy bombardment followed by an attempt to penetrate the defense lines, and the key to victory would be to hold a few heavily fortified positions in a battle of attrition.

In information security, victory has included providing for restoration of information systems by incorporating detection, protective, and reactive capabilities. Restoration is similar to recapturing a lost trench, to use terminology from trench warfare. The defensive posture has been reflected in research, research funding, and scholarly output. From information security's early inception in the 1980s to today's secured environments, we have become skilled in our ability to secure and harden information systems. The fluid and soon-to-be-automated battlefield of cyber operations is a novelty. The defense and intelligence establishments are moving quickly toward full-spectrum cyber operations.[6] The challenge for cyber security research centers is to adapt to the changing environment as the earlier academic paradigm assumption of future conflict is invalidated.

The Lure of Traditional Thinking

The cyber warfare concepts and abilities of the early years will continue to evolve over the decades to come. Developments tend to take longer than first anticipated not only because of technological hindrances, but also due to a path-dependent culture favoring earlier methods and a natural instinct to prefer what is known. There is a valid analogy between the dawn of cyber warfare and the dawn of armored warfare. It took 25 years for Western armies to figure out a proper use for the armored tank. Once that was understood, the way wars were fought was fundamentally changed. That has continued for 70 years and still counting.

For the first 25 years, the French and British saw the battle tank as a moveable machinegun pillbox from trench warfare. The tank was not a fighting platform; it was a mobile fortification that supported infantry. This perception changed when those countries suffered a horrifying defeat to the Germans in May 1940; the Germans had studied, developed, and understood armored warfare. For the Allied forces, it was too late; the damage was done. The irony is not only that the French developed many of the ideas the Germans utilized, such as Charles de Gaulle's proposed armored warfare tactics and the French airmen's innovation of advanced dive-bombing, but also that the Allies publically and vocally debated the opportunities these tactical innovations offered. The Germans were listening, but not the Allied high command. Due to groupthink and intellectual path dependency, the French military never accepted it or even considered it seriously.

The French preferred structured positional warfare. An integral part of positional warfare was fighting for fixed hardened positions—a war of holding positions and attrition. In 1940, France had the largest land army and also the largest number of battle tanks in Western Europe. In addition, there were Allied forces such as the British Expeditionary Force.

The difference between the combatants was the tactics of how to use battle tanks. The German strategy—which was old and known to the French—was an attempt to encircle the French after a breakthrough, but the tactics and operational performance were revolutionary. The German tanks were in the hands of Heinz Guderian, who carefully studied how to utilize tanks in an unconventional manner. He invented and refined armored warfare, ensuring that he could exploit the adversary's weaknesses. The number of French tanks and massive French army did not matter. The reason was simple: the French were not able in their minds to fight modern warfare and therefore were doomed to destruction or submission.

Guderian utilized the embedded abilities of armored units. The Germans changed the aim point, and instead of racing toward Paris through Belgium, the armored units pushed toward the Atlantic Coast to cut off the Allied forces in Flanders and Belgium where they waited for a repeat of the attack of 1914. The Sichelschnitt Plan of 1940 was designed for armored warfare; it had momentum and speed and captured the initiative. Once executed by the Germans, the French line of defense collapsed. After the Blitzkrieg of 1940, Guderian wrote about his preparation:

> For someone observing tank theory from afar, unburdened by tradition, there were lessons to be learned in the employment, organization and construction of armor and of armored units that went beyond the doctrines then accepted abroad. After years of hard struggle, I had succeeded in putting my theories into practice before the other armies had arrived at the same conclusions. The advance we had made in the organization and employment of tanks was the primary factor on which my belief in our forthcoming success was based.[7]

The opportunity in cyber operations in the next decade is not a revolutionary technology, but instead derives from how we utilize and militarize existing technologies in a way that is unburdened by tradition, to use Guderian's words.

The French in 1940 were still thinking of warfare as a solid front between two adversaries, consisting of three lines of units: infantry, artillery, and bakery. The traditional way of fighting war was that infantry faced and fought the enemy, artillery supported the infantry with indirect fire, and the rear echelon, here called bakery,

provided logistic support. Guderian broke the rules and fought the war in reverse order. He concentrated his units and overran the French lines at a weak point, and in a deep stroke attacked the bakery, ignored the infantry, and let the artillery panic. The attack was identical to the sketches of deep-penetrating armored assaults that Liddell Hart and de Gaulle envisioned before the war.

The lure in applying traditional military thinking on cyber warfare is that we can fight cyberwar based on the doctrines and intellectual underpinnings of land battle as we know it. Carl von Clausewitz assumed that the soil, woods, heights, and rivers of the Napoleonic battlefield were fixed. In a Clausewitzian world, the battle commander could understand and study the battlefield, and by objective permanence, the intended battlefield would be there the next day ready for battle. The woods would not move, the rivers would not disappear, and the heights would not sink. In cyber, the map and terrain that form the battlespace change continuously in real time and beyond our imagination as new nodes are discovered and a kaleidoscope of network patterns occurs and disappears. Traditional military theories could be less relevant in cyberspace than we are ready to admit. Traditional thinking appeals to us, but it could be spurious.

If we assume that we have control of the situation and knowledge of our enemy's positions and the full extent of the map, with our defense focused on hardened strongpoints, then we are fighting the digital cyberwar with the tools of analogue positional warfare. Edward N. Luttwak noted that strategy only matters if we have the resources to execute the strategy, and embedded in Luttwak's statement is the general condition that if we are unable to identify, understand, and utilize our resources, strategy does not matter.

Cyber supremacy will be achieved if we can understand the unique tenets of cyber, create a doctrine that exploits opportunity and technical ability, achieve broad societal alignment to cyber strategy, and assemble the workforce to execute it. Universities play a vital part in the last three components. Even if the military develops the brightest and most thought-through doctrine ever conceived, it will still be only a doctrine and nothing more. Doctrines are instruments of war, but they tell only how to play the cards; the actual deck of cards in cyberwar is mainly produced by private enterprises and academia.

Inability to Transpose Theory to Practice

The United States is having an extensive public debate about the future of cyber warfare and how it should be conducted. We debate openly as a free and democratic society. We are not the first open society that has been able to generate magnificent ideas and theories about future warfare. In the 1930s, B.H. Liddell Hart, Giffard Le Quesne Martel, and John F.C. Fuller wrote extensively about the future of mobile warfare. Martel was considered one of the world's leading tank experts of the 1930s. He went so far to prove his case that he built a light tank in his own garden, at his own expense, which became the platform for the British Bren gun-carrier.[8] Liddell Hart was a prolific writer and developed theories of exploits after an armored breakthrough of enemy lines, the deep strike that would force the enemy to react and lead to the collapse of the defense. In France, then–Colonel Charles de Gaulle advocated for armored divisions, freeing the tank corps from the infantry and utilizing armored warfare's full potential. France and Britain in the 1930s saw the potential in armored warfare, but for institutional reasons and internal biasness, they refused to capitalize on these modern ideas.

In the 1930s, both France and Britain failed to transpose theory to methods, tools, and implementation. In military terms, theory transposes to tactics, weapons, and training. Theory was created in France and Britain but transposed by Germany through generals such as Erich von Manstein and Guderian to tactics, weapons, and training. Guderian wrote after the war: "The proposals of de Gaulle, Daladier and others along these lines had been ignored. From this it must be concluded that the highest French leadership either would not or could not grasp the significance of the tank in mobile warfare."[9]

The United States faces the same risk as Britain and France in the 1930s, except our military leadership clearly understands the changing paradigm; there are other obstacles to transposing theory. We are the creators of cyber ideas and concepts, but we fail to move beyond the present and implement them. Today, the Department of Defense (DOD) and Intelligence Community are world leaders in developing cyber operation concepts and innovative strategies to ensure future American cyber supremacy. Instead of the military being the blockage for intellectual proliferation as it was in France 75 years ago, the hindrance for cyber warfare's development today is in the civil society and the academic realm.

We can assume that our adversaries or covert adversaries in the digital age carefully study our new strategies and ideas and develop plans to utilize these publically discussed innovative concepts. The most loyal online readers of the offensive cyber operation discourse in American journals are likely our adversaries. All of them are ready to capitalize on our ideas if they can.

The University Role in Cyberwar

A nation's cyber warfighting ability will be determined by its ability to mobilize resources and knowledge and coordinate the effort. These resources are not as easily identified. At the entrance to the contested cyberspace as a warfighting domain, academia and university research centers have to find their new roles. University cyber researchers have continued to deliver mainly information assurance. Even the information assurance context has been following the Zeitgeist by focusing on Cold War spies, terrorists, drug cartels, white-collar crime, and economic espionage. The bottom line is that it is still information security with a theoretical foundation from the 1980s. Information security has had a decade of high levels of funding as a response to 9/11 and society's increased reliance on the Internet and computerized systems. This posture has been built on hardening systems. The surge of resources to research centers, contractors, Federal agencies, and private industry has resulted in a greater understanding of how to secure systems.

Basic operational questions as to why things are done, their strategic value, how they can tangibly strengthen operations, and the factual effects have sometimes been overshadowed by details with limited systematic thinking behind them. Traditional information security—the hardening of systems—has been so prevailing that it is often misinterpreted as exchangeable with cyber defense and cyber operations.

In the pursuit of cyber superiority, information security, renamed information assurance, is one piece among many and, depending on the operational environment in different scenarios, is of even less importance than other measures. DOD defines cyber superiority as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary."[10] Dominance in cyber space can only be achieved if there is an ability to collect information, attack and intercept other actors' cyber activities thus preventing their interference, and likely also utilizing digital lethality to destroy or severely damage other actors' cyber systems. Information assurance is not enough. It is part of cyber defense—but it is not cyber defense.

The National Security Agency (NSA) has set up criteria for the designation of academic departments as Centers of Academic Excellence (CAE) to ensure that the quality of education and research is upheld. There are 48 research centers and university departments that have been considered Centers of Academic Excellence–Research (CAE-R). NSA's latest addition is CAE Cyber Operations.[11] According to the NSA, key abilities are collection, exploitation, and response. The majority of the CAE-R institutions are likely to pursue the CAE Cyber Operations.

A Quick Survey

As an experiment, we conducted a survey to get a snapshot of where CAE-R research centers stand today in relation to the broader systematic full-spectrum view on cyber warfare pursuing cyber superiority. The question was whether the academic institutions are embracing the cyber operations paradigm shift or are institutionally path-dependent and continuing with the information assurance track that has been prevailing since the Cold War. The purpose of the survey was to determine how many research universities have broken down their internal walls between departments in professional and engineering schools and successfully pursued a broader approach to match the complexity of cyber operations. We acknowledge that this paradigm shift is a work in progress, and we have credited schools that are moving toward cyber operations even if the actual approach as of today is ad hoc and less defined.

Cyber operations research requires linkages outside of the engineering schools and benefits from collaboration with other university-wide schools and departments. The research can then be transferred through research-based education to the workforce that is needed to achieve national cyber defense objectives. A broader knowledge base enables the research center to do work that can support, prepare, and conduct defensive countercyber operations, offensive cyber operations, and cyber operational preparation of the environment aligned with the national interest.

A set of variables was created and then each academic CAE-R research center's Web presence was visited, along with their leading researchers' Web presence, and the materials presented on the Web site were evaluated against the variables. Some of the observations were reviewed and validated by an external reviewer to ensure that the evaluation did not contain systematic errors. There were 48 academic cyber research centers in nonmilitary higher education in the United States in February 2012. All schools that met the CAE-R criteria had information assurance programs in place as the foundation for the designation. The variables used were:

- whether there is research on offensive and responding cyber defense and if the research conducted steers toward offensive countercyber, cyber operational preparation of the environment, and pursuing cyber superiority in cyber warfare, or is predominantly based on information assurance only

- if there is a legal component supporting utilization of weapons control status, especially international law, ethics, and privacy, and a future need for assessments of military ethics, cyber rules of engagement, and the legal foundation for collateral effects, first and second tier
- whether the research has involved political scientists or other social scientists, especially in theories about national institutional stability and international relations, creating understanding of foreign societies or institutions that are the targeted adversaries, aligned with the concept of cyber operational preparation of the environment and information operations, leading to increased effect on adversarial society
- if the university has a designed policy school or similar entity to determine the extent of resources available on campus to optimize cyber operations research to take advantage of intelligence-gathering opportunities, human terrain, political instability, and fragile institutional design of target countries or institutions
- whether there is a clear linkage between the cyber research program and policy school of the same university, if one exists
- if security studies scholars are involved in the cyber security research, creating an understanding of security fundamentals and military science that would support a better understanding of the final goal with the cyber operation mission and doctrinal goals
- whether there is an international relations component in the research to determine the degree the opportunity to exploit human terrain, political instability, and fragile institutional design of target countries or institutions is understood
- if the cyber research covers the space domain since the importance of the defense of the global information grid is clearly identified by the term cyber operations, defined as the "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[12]

Cyber attacking U.S. space assets can give high returns for an adversary.[13] The global information grid is pivotal to U.S. military might and information supremacy.[14]

Results and Reflections

We do not consider this survey as delivering a perfect picture of the state of national cyber research, but it will reveal a fundamental understanding of what research universities are able to deliver and where the majority of the U.S. cyber security research centers are on the learning curve. All 48 CAE-Rs are researching information assurance. Only five are actively researching offensive and defensive cyber operations to a broader extent. This includes research supporting information operations and psychological operations aligned with future military operations. If a military commander wants to have cyber weapons made, these universities are able to make military grade cyber weapons.

The high number of CAE-Rs that have legal components in their research reflects privacy research, which is also an integral part of information assurance. Only 10 CAE-Rs involve social scientists in their research. A significant number of schools do not involve social scientists in projects that are focused on human behavior and institutional arrangements. A few universities go as far as to design complex research projects that are partly based on behavior, sociopolitical institutions, and societal factors with only computer scientists and engineers on the team. Of the 48 CAE-Rs, 10 have a full-size policy school on campus, with numerous specialized scholars running research over a spectrum of policy related inquiries and with understanding of core tenets of societal cyber operation components. Only 5 CAE-Rs out of these 10 collaborate to a visible degree with their own policy school and utilize the joint knowledge. In other terms, half of the tier-one universities with cyber security research centers underutilize their own policy schools' pool of competence. Even if we are in a globalized world with cyber as not only a warfighting domain, but also an arena for international cybercrime and transnational illicit activities, only 6 CAE-Rs involved international relations scholars in their projects. Cyber issues in space only draw interest from 5 CAE-Rs.

Survey Results of 48 Centers of Academic Excellence-Research (Defense Department Institutions Not Counted)

Variable	Number of schools	Percentage of total
Offensive cyber research, such as offensive countercyber and cyber operational preparation of the environment	5	10.4
Legal considerations and privacy	18	37.5

Involving social scientists and/or behavioral scientists	10	20.8
Policy school on campus	10	20.8
Utilizing the assets of a policy school	5	10.4
Presence of security studies scholars or activity in research	14	29.2
International relations	6	12.5
Cyber in outer space, considering outer space as a part of cyber defense	5	10.4

The largest portion of the CAE-R cyber research centers is doing information assurance research independently and separated from other scholarly activity on their campuses. The results are presented in the accompanying table.

Concerns and Opportunity

Cohesive cyber defense research requires universities to optimize their campus-wide resources to fuse knowledge, intellectual capacity, and practical skills in an unprecedented way. This is a major challenge for universities that have historically separated departments and schools and driven specialization so far that intra-university collaboration seldom occurs. In an era of austerity, it is justifiable for DOD to steer toward applied research that can strengthen the abilities of the Armed Forces and Intelligence Community and provide policymakers and Federal executives with more options.

The future will require cyber defense research teams that can address not only computer science, electrical engineering, and software and hardware security, but also political theory, institutional theory, behavioral psychology, deterrence theory, military ethics, international law, international relations, and additional social sciences. Researchers working alongside DOD to develop tool sets for information operations as a subset of cyber operations, utilizing social media and exploiting collective behavior, would require a broad mix of social science and behavioral psychology competencies.

The problem, and our disadvantage, is that theoretical concepts do not become transposed into research and education to create methodologies, tools, and implementation. A vast number of our academic institutions are unable, as of today, to look at and conduct research beyond information security. Cyber operations require a different academic culture where collaboration in the national interest prevails over departmental turf wars. To quote Sayre's Law, "In any dispute the intensity of feeling is inversely proportional to the value of the stakes at issue"—and its corollary—"that is why academic politics are so bitter." A sense of what is ultimately at stake needs to be infused. Cyber research centers and dedicated researchers within different departments can be brought to an understanding of the need to collaborate, and they can even seek to collaborate, but the internal culture often prevails.

There could be several reasons why the academic turf war mentality exists. One is funding; cyber defense is seen as one of the few areas where funding could increase significantly in the future. Academic departments are trying to set out on their own journeys to seek sponsored research instead of jointly seeking grants with other disciplines, which would lead to fewer resources once they are shared.

For researchers, it is always more pleasant to be granted more money in the field we have already submerged ourselves in and fully understand. For researchers in general, it is also hard to admit that our little niche of science may not matter that much in the future. The academic community in many ways is driven to seeking more funding for what has interested researchers in the past rather than adapting to the new cyber paradigm, thus digging deeper trenches in the turf war.

A second reason the turf war exists is academic gridlock, which is a matter of institutional culture, intellectual path dependency, and the fact that many institutions became used to access to funding during what then–Secretary of Defense Robert Gates called an era of endless money. Once universities figured out the magic algorithm to get funding, the universities were less responsive to signals of change. If that predicted stream of funding disappears, action will be taken. The fastest way to correct the gridlock and increase the transformation of research and education to better mirror the interest of DOD is to steer funding. One of

America's advantages in research is its universities' ability to quickly adapt when facing the risk of losing funding.

The conducted survey presents a misalignment between what is researched and educated in the Nation's cyber security research centers and DOD's overarching goals and doctrine. It has to be made clear that the stakes are so high that a correct balance has to trump any internal academic politics. The misalignment creates a gap that can be closed by steering funding and increasing interaction among the actors in the national cyber defense. Unless corrected, the misalignment will continue to create a national security risk. These innovative ideas can be put to use by our adversaries while we as a nation fail to achieve cyber superiority

References

1.Ellen Nakashima, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace," The Washington Post, May 30, 2012, available at <www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html?hpid=z1>.

2.Ellen Nakashima, "U.S. accelerating cyberweapon research," The Washington Post, March 13, 2012, available at <www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html>.

3.Nakashima, "With Plan X."

4.Air Force Doctrine Document 3-12, Cyberspace Operations (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating Change 1, November 30, 2011), 2.

5.Jan Kallberg and Bhavani Thuraisingham, "Towards cyber operations—The new role of academic cyber security research and education," IEEE Intelligence and Security Informatics 2012, Washington, DC.

6.David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," The New York Times, June 1, 2012, available at <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=3&hp>; Evan Perez and Adam Entous, "FBI Probes Leaks on Iran Cyberattack," The Wall Street Journal, June 5, 2012.

7.Heinz Guderian, Panzer Leader (New York: Dutton, 1952).

8.Obituary of General Sir Giffard Martel, The Glasgow Herald, September 4, 1958, 9.

9.Guderian.

10.James E. Cartwright, memorandum, "Joint Terminology for Cyberspace Operations," Department of Defense, Washington, DC.

11.National Security Agency, "Criteria for Measurement for CAE/Cyber Operations," available at <www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml#4>.

12.Cartwright.

13.Jan Kallberg, "Designer Satellite Collisions from Covert Cyber War," Strategic Studies Quarterly (Spring 2012).

14.William J. Lynn III, "A Military Strategy for the New Space Environment," Washington Quarterly 34, no. 3 (Summer 2011), 7–16.

Table of Contents

Army Electronic Warfare Goes On The Offensive: New Tech Awaits Approval

By Sydney J. Freedberg Jr., AOL Defense, January 29, 2013

WASHINGTON: Today, somewhere inside the Pentagon, senior Army officers will likely recommend development of new radio-jamming equipment for the post-Afghan War world. After a decade desperately playing defense against radio-detonated IEDs -- and, before that, a decade of neglect in the 1990s -- Army electronic warfare is taking the offensive again.

With their eyes on future adversaries more technologically sophisticated than the Taliban, commanders want new capabilities to shut down enemy electronic networks and protect their own. It's a challenge intimately interwoven with but distinct from the higher-profile field of cyber warfare. Hackers infiltrate enemy networks to steal data and infiltrate viruses, while jammers simply shut them down -- though that distinction gets blurred by new techniques such as "protocol attacks" that scramble digital radios.

The Army's Training and Doctrine Command (TRADOC) is drafting a new field manual for "Cyber-Electromagnetic Activity," CEMA, a concept that joins the two functions at the hip. A new Army school at Fort Sill, Oklahoma has so far trained almost 700 electronic warfare specialists -- many of them combat veterans, ranging from young sergeants to, as of Jan. 1st, the field's first full colonel -- who will oversee not only traditional EW but also cyber operations, at least on the tactical level.

But these new personnel need new equipment to execute their new doctrine. If today's formal Analysis of Alternatives (AoA) goes as expected, the Army will soon launch a new "multi-functional electronic warfare" (MFEW) program to develop an integrated arsenal of powerful, sophisticated sensors and jammers for use on drones, ground vehicles, and fixed locations.

It's not that the Army doesn't already have jammers. It has thousands, carried by many vehicles and even some foot patrols in Afghanistan and, until recently, Iraq. But these are limited systems, fielded in haste to save lives, often waiving the normal Army tests and standards, largely incompatible with one another, and all designed for the urgent but ultimately narrow mission of shutting down radio-detonated roadside bombs (aka radio-controlled improvised explosive devices, RCIEDs). Only one jammer has been institutionalized as a

formal, fully funded "program of record," the Duke CREW (counter-RCIED electronic warfare) system, and even Duke was never designed to protect more than the convoy of vehicles carrying it.

"It provides a defensive bubble around the soldiers to prevent a radio-controlled IED from being triggered," said Col. Joe Dupont, the Army's program manager for electronic warfare. The future multi-functional EW system should go much farther.

In the new concept, Dupont told AOL Defense, once the sensors pick up an enemy transmission, "a commander has several options. He could have his SIGINT [signals intelligence] team exploit the signals, just sit there and listen to them. Or he could decide to attack it" -- in various ways: "He can do a physical attack using kinetic weapons systems, meaning he can blow the crap out of it; or he can use an electronic attack using one of his EW systems; or in the future he may have the ability to do a cyber attack."

Blowing something up is the most permanent solution, but missiles, bombs, and artillery shells might miss and, at worst, kill civilians. Cyber is the most subtle, but potentially the most challenging and time-consuming as US hackers figure out how to infiltrate and subvert the enemy network. Electronic warfare -- jamming and spoofing -- is non-lethal, for good and ill, and its effects only last as long as you keep transmitting, but because its ammunition is electromagnetic, it's literally as fast as the speed of light.

Today, however, the Army has very little ability to jam enemy systems more sophisticated or distant than a roadside bomb. The service is fielding about two dozen ground-based jammers, called GATOR, and a handful of converted C-12s, called CAESAR. Otherwise it has to rely on the other services' jamming aircraft, principally the Navy's. But those are scarce, expensive, high-powered planes. For most Army missions, it's like swatting flies with a shotgun.

"We could always bring in an EA-6B [Prowler] and blanket jam everything, but those things are in very high demand," said Col. Jim Ekvall, an electronic warfare expert on the Army's Pentagon staff, section G-39, speaking to AOL Defense in his windowless Pentagon office.

"Prowlers are awesome"; their successor, the Navy's new EA-1G Growler, is "wonderful"; and the Navy's EC-130 Compass Call is "absolutely fantastic," Ekvall enthused. "They're the best in the world at doing what they're designed to do -- but they're not available 24 hours a day to the ground maneuver commander...and they happen to be often fratricidal to our own communications systems and our own electronic warfare": The Navy jammers in particular are designed to shut down enemy air-defense radars, which makes them so powerful they can scramble friendly systems on the ground.

That is, they do when the Army can get them. "There's not enough joint assets to meet these needs of the ground components today," said Col. Gary Hisle, who served as an Army liaison to the Combined Air Operations Center overseeing Afghanistan and Iraq. "They were only able to fill about 34 percent of the validated requirements -- [that's] not the number that was actually submitted."

"And that's in a COIN [counterinsurgency] environment," added Hisle, now TRADOC's director of electronic warfare. Low-tech insurgents have little electronic equipment for the US to jam and still less ability to attack our networks. Future adversaries such as nation-states or even sophisticated non-state groups -- the so-called hybrid threat -- will have both more electronic warfare capacity to attack us with and more electronic assets of their own for us to attack.

Radio-detonated IEDs will hardly go away -- they're too cheap and effective -- but they'll will become just one part of an even deadlier and much more complex electromagnetic battlefield. "It's a much broader perspective than just worrying about counter-IED," said Ekvall. "Anybody can buy a two dollar walkie-talkie or a remote key fob, [and] I can use a key fob to detonate an IED," he said, but the US has largely figured out how to shut down such threats. "When you fight a more sophisticated enemy who has more resources," he said, "things become much more difficult."

The Army's new weapon in that fight will be something called the Integrated Electronic Warfare System, IEWS -- assuming they can get it funded.

The first piece of IEWS is simply a spectrum management and planning tool for "electronic warfare integration": "Think apps for EWOs," said Michael Ryan, Col. Dupont's deputy. The idea is software that can take in sensor inputs and tell those EWOs -- electronic warfare officers -- what's out there: These are enemy transmissions, these are friendly ones, these are unknown; here are our own electronic attack systems, here are the likely effects if we use them to attack a given target -- including "unintended consequences" such as inadvertently jamming a friendly system nearby. ("We've had a lot of problems in the past with electronic fratricide," sighed Ryan).

The Army's already issued formal Requests For Proposals from industry for the planning tool: "The RFP's out now, we expect proposals back in February, we'll run a selection in spring," Ryan told AOL Defense.

The next step is to develop the new electronic attack systems themselves. That's the multi-function electronic warfare program, the jammers to go on drones, ground vehicles, and fixed installations. If today's Analysis of Alternatives meeting approves, said Ryan, MFEW will go to Milestone A, technology development, later this year, with testing in 2019 and actual fielding in the 2020s.

All this assumes the military finds the money -- no easy feat when the budget process is so dysfunctional that the Army and every other federal agency don't know what they will have to spend in March, let alone in 2020.

"We all understand the budget of the future and that's going to have an impact on every program the Army has," said Ekvall. "Where this will ultimately wind up in the priority efforts of the Army, I can't tell you."

But a priority it has to be, he said: "We've got to get back into the ground electronic warfare fight."

As a young artillery officer stationed in West Germany in the late eighties, Ekvall had the importance of electronic warfare drilled deep into him. "I was always concerned that the Soviets [in a war] would have the ability to disrupt my communications," he said. Even in peacetime, he said, "we kind of assumed that the Soviets were listening to us, so we just talked in code." But in the 1990s, with the Soviet threat gone and budgets shrinking, the Army essentially got out of the electronic warfare game -- as did, to a lesser extent, the Air Force - and left it largely to Navy jamming aircraft. Then Iraq and Afghanistan shocked the Army back into the business again.

"There's been this ebb and flow," Ekvall told AOL Defense. Today, he said, "we're flowing."

Table of Contents

Army Manual Highlights Role of “Inform and Influence Activities”

By Steven Aftergood, FAS, February 1st, 2013

The use of information-related tools to support military operations and to help shape their outcome is discussed in a newly updated Army manual on what are now called “Inform and Influence Activities.”

Inform and influence activities (or IIA) refers to “the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking.”

In some circumstances, the manual says, information operations can play a decisive role.

“Activities occurring in, through, or by means of the information environment have a consequential effect on an operational environment and can impact military operations and outcomes. Therefore, commanders and their staffs must understand their operational environments completely. This understanding includes the information environment and the potential impacts it can have on current and planned military operations.”

But the effectiveness of such activities is naturally limited by the realities of the military engagement.

“Soldiers’ actions powerfully influence the credibility of IIA. Visible actions coordinated with carefully chosen, credible words influence audiences more than uncoordinated or contradictory actions and words. All audiences–local and regional as well as adversary and enemy–compare the friendly force’s message with its actions. Consistency contributes to the success of friendly operations by building trust and credibility. Conversely, if actions and messages are inconsistent, friendly forces lose credibility. Loss of credibility makes land forces vulnerable to enemy and adversary information or countermessaging and places Army forces at a disadvantage.”

“Aligning information-related capabilities with the overall operation ensures that messages are consistent with the forces’ actions to amplify the credibility of those messages. It is paramount that inform and influence efforts complement not contradict. Failing to do so jeopardizes credibility.”

The updated Army manual replaces a 2003 document titled “Information Operations.”

“The publication does not address every information-related capability commanders can use to help shape their complex operational environments. It should, however, generate introspection and provide just enough guidance to facilitate flexibility and innovative approaches for commanders to execute the art of command to inform and influence.”

See Inform and Influence Activities, U.S. Army Field Manual 3-13, January 2013.

Table of Contents

DoD Looking to 'Jump the Gap' Into Adversaries' Closed Networks

By Zachary Fryer-Biggs, Defense News, Jan. 15, 2013

Iran's uranium enrichment facility at Natanz may have had one of the most secure computer systems in the world. The building housing the nuclear program's equipment is underground, protected by a combination of concrete walls, earth and military guards.

And it was a "closed" network, sealed off from the Internet and unsusceptible to vulnerabilities in the system's Windows-based software.

All those precautions, however, didn't stop the Stuxnet worm from infecting the system, disrupting the delicate balance of uranium-enriching centrifuges and rendering them useless. Stuxnet, part of a broader U.S./Israeli cyberwarfare campaign against Iran's nuclear program called "Olympic Games," was carried in on a small flash drive. Someone, either a spy or an unwitting accomplice, plugged it into a USB port on a computer inside the complex and let loose into the "secure" Iranian system the most devastating cyber weapon ever known.

Without smuggling that cyber weapon physically into the plant, the operation never would have worked, which underscores the problem: No matter how high-tech the cyber tool, the glaring weak link has been the ability to reach out and touch a system. A breach of physical security was required, either secretly getting hold of an employee's thumb drive and infecting it, or working with someone on the inside to covertly plug the device into the network.

With thumb drives now a known vulnerability, most countries have banned their use on sensitive systems. Iran forbade them at Natanz shortly after the Stuxnet worm began to work its magic; the Pentagon banned their use in 2008.

It was right around that time that scientists began to turn their attention to another project: trying to access these protected networks remotely, through the air, by reading activity via electromagnetic field distortions and inserting code via radio frequencies. Accessing these networks — networks that don't have wireless routers and aren't connected to the Internet — became something of a holy grail, dubbed "jumping the gap."

The science has progressed significantly, and now the Army is looking at demonstrating technology that can be deployed on aircraft and ground vehicles that can wage this kind of cyber warfare.

The Army's Intelligence and Information Warfare Directorate, known as I2WD, hosted a classified planning day Nov. 28. Representatives from 60 companies and labs attended to discuss what can be done in the realm of electronic warfare and cyber, according to a source familiar with the program.

The roughly half-dozen objectives of the Tactical Electromagnetic Cyber Warfare Demonstrator program are classified. (The TECWD program is pronounced "techwood" by participants.) The source said the program is designed to demonstrate ready-made systems, dubbed "boxes," that can perform a variety of tasks. Some are somewhat typical fare, like systems aimed at the improvised explosive device threat.

But among the objectives are these: inserting and extracting data from sealed, wired networks. The possibilities are remarkable. Imagine being able to roll a vehicle near a facility, sit for a short period while inserting a worm, and leave without having to buy off any employee or sneak anything past an attentive guard. Better yet, a stealthy unmanned aerial vehicle could be quietly flown far above a facility to insert code even in contested airspace. With that kind of tactical deployment, cyber could become a critical part of a wide variety of operations, as localized effects could be integrated with kinetic activities.

The Army program is designed specifically to test capabilities for air and ground platforms, according to an invitation to an information day on the program released by I2WD.

"The TECWD demonstration effort will serve as a technology demonstrator for offensive electronic attack, defensive electronic attack, electronic protection, and electronic support, and EW enabled cyber on ground and air platforms," the invitation read. "TECWD will help the Army assess technologies and capabilities for potential applicability in the Army's next generation EW and beyond."

The program, which will consist of a series of demonstrations roughly every three months for the next two years, will test a variety of electronic warfare, or EW, capabilities, said Moses Mingle, branch chief of the EW systems ground branch at I2WD.

"It's not a system; it's a demonstration platform," Mingle said. "Basically, we're vetting systems concepts: tactical EW cyber scenarios that could be deployed in the future."

Asked if one of the objectives is to demonstrate a system that could jump the gap and access systems remotely, Mingle declined to go into detail, citing classification issues, but said, "That's a part of it, but not all of it."

U.S. intelligence agencies began to worry about distortions to the electromagnetic fields around computer systems, and the potential that they would provide unique signatures that could tip off network activity, in the 1980s. The principle behind it is based on simple physics. Electronics in even a closed network emit an electromagnetic signal, however faint and accidental.

So at the time, a series of research efforts was undertaken to study these distortions, known as compromise emanations, under the code name “Tempest.” Could these the emanations be exploited in any reliable way? Researchers found that keystrokes could be detected from signals sent from keyboards to computer units, as well as information on a monitor. The ability to detect these disturbances has become increasingly sophisticated, with systems able to pick out signals from greater distances with greater clarity.

More recently, scientists have been paying special attention to the inverse of reading these emanations: insertion of data using radio frequencies. Again, in theory, since a wire can act as an antenna, an electromagnetic signal can be engineered and potentially transmitted to that wire.

The precision required is tremendous. Popular culture has introduced much of the world to the concept of the electromagnetic pulse, as featured in the George Clooney movie “Ocean’s Eleven.” (Don Cheadle’s character, quite implausibly, fries the electrical grid of Las Vegas.) The pulses are typically created by extraordinarily large systems supported by tremendous supplies of energy or as a side effect of nuclear detonations. They work as blunt-force instruments, frying a system and rendering the electronics useless.

The TECWD challenge would be a technique that would transmit not a destructive pulse but a signal finessed to a specific network. It’s more scalpel than sledgehammer.

The technology does exist, but the ability to add data still has limitations, mainly proximity and bandwidth, experts said. The “transmission” system has to get quite close to the targeted network. And at current levels, complex data can take extended periods to insert. Experts declined to provide full specifics on data transfer rates and range for data insertion using radio frequencies, citing the classified status of the capabilities and national security issues.

The actual power usage is far less than you’d expect: One expert said systems as small as man-packable radios could serve as the forward entry point for these types of cyber penetrations.

The recognition that electronic warfare methods can be critical for future cyber applications is clearly making its way up the leadership chain.

At a recent event at the Naval Surface Warfare Center’s Crane Division in Crane, Ind., Adm. Jon Greenert, chief of naval operations, made the case.

“We have to understand better the electromagnetic spectrum,” he said. “Cyber, our radar and communication, everything. If you control the electromagnetic spectrum, you control the fight.”

The cryptic remarks reflect the classified nature of nearly everything in the cyber realm, and particularly in regards to offensive cyber EW capabilities.

But the possibilities are being explored as the U.S. military increasingly recognizes the potential of cyber weapons in operations.

The actual technology that allows for the insertion of data — transmitting cyber into a closed system — isn’t novel, said retired Air Force Maj. Gen. Dale Meyerrose, former associate director of national intelligence.

“This is old technology,” he said. “The technology itself isn’t new, but the application of the technology is new, and the software running the technology on some of these devices is new.”

Meyerrose, who runs the Meyerrose Group, said connecting to closed networks using radio frequencies is about five years old, but some of the complications of cyber, including legal authority, have slowed progress. “This could be used to drop a Trojan into a system,” he said. “Like everything else in cyber, there are not a lot of legal parameters. Like everything else in cyber, our legal system is about 20 years behind.”

But if the legal questions and technical limitations are worked out, a new era of integrated cyberwarfare may be dawning.

Table of Contents

President Putin orders FSB to protect media sites from cyber attack

From RT, 21 January, 2013

The Russian President has told the country’s federal security service to set up a system that would detect, counter and prevent computer attacks on state information resources.

The order defines official resources as information systems and networks that are located in the territory of the Russian Federation and in its diplomatic and consular offices.

The work and control over the system will be run by the FSB. The state security department will also cooperate with other state ministries and agencies to ensure anti-terrorist cyber systems work properly. Putin's order published on an official web site on Monday states that law enforcers should establish how several recent cyber attacks against government agencies have been allowed to happen.

In recent years there have been a number of attacks but only a few claimed to be successful.The attacks are mostly launched through networks of infected computers belonging to unsuspecting users, which makes the work of FSB specialists difficult.

It has been established that in early May 2012 some internet activists who claimed to belong to the Anonymous hackers' group promised to launch an attack on Russian government web-sites to support the rally against alleged election violations that took place in early May.

The attacks by Anonymous yielded at least one result – on May 9 the hackers managed to block access to the Russian President's official web-site kremlin.ru for about four hours.

Before that, hackers who claimed to belong to the Anonymous group, managed to deface the web-sites of some regional offices of Russian parliamentary majority United Russia, posting texts that accused top officials of corruption.

Due to the Anonymous group being very loose and evasive such cases are rarely investigated with success.

However, in mid-January this year, the FSB directorate for the Krasnoyarsk Region in Siberia filed a case in court against a local hacker who is suspected of attacks on the Russian President's web-site in May. The activist has been charged with spreading malicious software, which is a criminal offence punishable with up to four years in prison.

Table of Contents