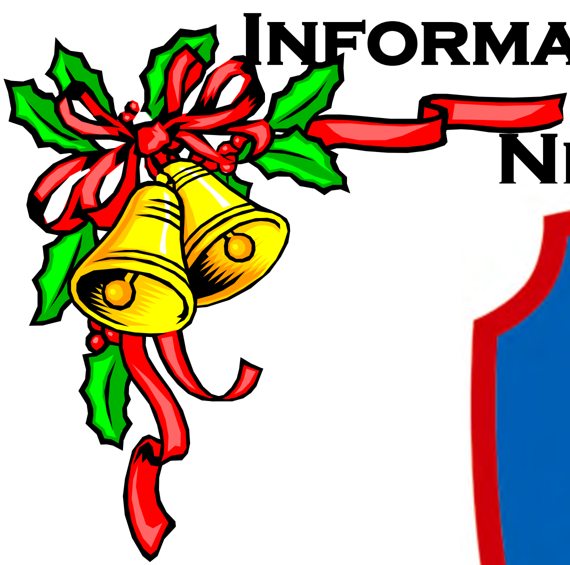


Information Operations Newsletter

US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion of research in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of the Army, or U.S. Army Strategic Command.

ARSTRAT IO Newsletter on Phi Beta Iota

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

Table of Contents

Vol. 13, no. 02 (November 2012)

Israel is Losing the PR War

By Annie Lubin, IsrealNationNews, 10/31/2012

For over forty years Israel has been losing a public relations war to the Arabs and now to the Palestinain Arabs. And no one in Israel seems to care.

Dr. Ron Schleifer, a professor at Ariel University, and an expert research academician on Psychological Warfare and military-media relations, has been studying the phenomena for years and has tried to sound the alarm on the importance of changing the way Israel uses the media. He has just returned from a trip to the United States in which he gave the Israeli perspective at a pro-Zionist conference that included thinker Bernard Lewis and Pamela Geller of subway ad fame.

"Subconsciously, we still have this attitude that the goyim hate us anyway so why bother with public relations" said Schleifer. "The answer should be that this question is totally irrelevant."

In his book Perspectives of Psychological Operations in Contemporary Conflicts, reviewed on Arutz Sheva, Schleifer documents how since Yassar Arafat's rise to prominence the Palestinians have been not only been winning the media war, but have seen to it that Israel should not even be considered a contender for its unwillingness to compete.

The idea the Arafat had was simple - use psychological warfare to portray Israel as the agressor and make the country weak from the inside by dividing the Israeli people. Arafat presented the Palestinian Arabs as victims, underdogs, the Davids pinned in the corner by the behemoth Goliath.

Nowhere was this seen more than during the first intifada. Palestinian Arabs manipulated the way the news was being reported by opening up numerous media branches and staging photo ops for the international media. For every reporter looking for a quote or a picture or details of an incident there was a Palestinian Arab within arms reach ready to paint Israel as the aggressor. By the time Israel decided to respond, the story had already been published.

Arafat's intent was to use the media to force a split in Israel. "Psychological warfare wishes to make enemy soldier pacifists and your own soldiers patriots," said Schleifer. The rationale was that once Israel crumbled socially, a military defeat would be much easier.

"A difference of opinion is okay, but a social split is very risky for a state…and that's what you see in Israel today," said Schleifer.

So, if Israel wants to stop having to fight for global recognition or for the right to exist and defend its borders then Israel has to change its public relations strategy. "If the Jews have decided they want an independent state, a state of their own, that state immediately falls into the international system of international relations. And we have to play according to those rules, especially in a case where we're not economically independent or secure. And even if we were, we still need to function within the international system," said Schleifer.

Yet Schleifer doesn't see this happening in the near future, if ever.

Part of the Israeli problem, as Schleifer sees it, is that if the state shows the world that Israel is not the aggressor it has been painted - that people in this country are worried - that some live in constant fear of rockets and attacks and instability - Israel believes it will be perceived as a weak country. "Israel has not managed to figure out how to be powerful but still perceived as the vulnerable one," said Schleifer. "That's the art of contemporary propaganda. Showing that you're strong without being perceived as a bully. The Palestinian's strength comes from showing their weakness."

"No independent state in the whole world would tolerate a barrage of rockets and mortars every day. Yet israel was conditioned to absorb all that for about a decade now and that is a psychological ploy by the Palestinians Arabs. Condition your enemy. Let them know, this is the situation and theres nothing you can do about it, because we control media sympathy."

Israel knows how it is perceived in the media and knows that the Palestinain Arabs have been winning the media war. So why does Schelifer believe change is not in the cards for Israel?

"Israel does not believe in propaganda. They don't want to manipulate anybody. Israel believes in deeds and not in words. This is the Zionist maxim. What matters is what you do and not what people say. It doesn't matter what the goyim think, what matters is what the Jews do…We're forever apologetic and always on the defense. Israeli leadership is still thinking that peace is dependent only on us. We don't want to start anything because we know how the world will interpet it.

"Finally after 60 plus years we have a Ministry of Hasbara (international outreach). But it has a very minimal budget and it's not ranked very high on the government's list of priorities. It's struggling to survive...Our media relations may be a bit more sophisticated than the Palestinian Authority's, but we're way behind the them in terms of understanding how the manipulation works.

"Israel, instead of conquering world public opinion by sending a barrage of visuals - images of the rockets and mortars falling on Israeli citizens every day, waits for the next attack and is forever seen as the oppressor."

Table of Contents

Indonesia's Cyber Defense Strategy and Its Challenges

By Yono Reksoprodjo, Jakarta Post, November 01 2012

A fast-growing economy has allowed Indonesia to increase its budget for infrastructure, education and defense. The government has proposed Rp 77 trillion (US$8 billion) for defense in 2013, up from Rp 72.54 trillion in 2012 and more than double the 2009 mark of Rp 33.67 trillion.

The defense budget will be spent on the Minimum Essential Forces (MEF) defense strategy, which has been developed based on financial constraints rather than threats.

The defense budget does not reflect the country's size and unique geographic terrain to cover, the spread of people to protect and the volume of natural resources to control. In short, the ratio of our defense capability and coverage in the region remains far from achieving a fair balance of strength with its neighboring countries.

In a show of commitment to fulfilling the mosaic of the MEF blueprint defense strategy, the Defense Ministry allocated funds to acquire 44 Leopard tanks, 24 F-16 jet fighters and some warships.

Nevertheless, we should look into the psychological aspect of this arms buildup; the purchase of more conventional hardware may increase the risk of an arms race in the region.

But military modernization should not and cannot ignore asymmetric warfare capabilities, especially due to the tight budget.

The Indonesian Military (TNI), known in the past for its guerrilla warfare strategy, needs to delve deeply into its creativity and develop a comprehensive approach to asymmetric warfare strategy. An asymmetric strategy combined with conventional military capability may form a hybrid warfare strategy that is believed to suit modern wars.

The modern era has seen the emergence of new non-state adversaries that have brought up complexities not only on rules of engagement but also the application of warfare strategies. The al-Qaeda attack in 2001, the breakup of the Soviet Union up to the Arab Spring show that many conventional military warfare strategies are no longer adequate to solve conflicts.

In the late 1950s, the US department of defense began to employ information communication technology to cope with the potential of a nuclear standoff during the Cold War. ARPANET, later known as the backbone of Internet, came as a result of collaboration between the US military and academic institutions to bring forth the era of the cybernetics network to modern society.

It has been growing rapidly into a vital international data communications backbone with utilizations going beyond business communications and financial data exchange. Military, economic, cultural and socio-political information in many nations is swiftly exchanged through the cyber network.

Striking the strategic center of gravity through the cyber network is defined as asymmetric warfare.

The implementation of network-centric systems and the use of tactical unmanned machines for hybrid warfare strategy purposes, as well as the growing reliance of civilian society in maintaining its daily activities, has offered channels within the cyber network system as means of attack.

Indonesia's MEF buildup strategy has provided opportunities for combining conventional hardware with a cyber warfare strategy. Indonesia is rich in human resources with expertise in information and communication technology (ICT).

Unfortunately, the military's ICT human resources lack the capabilities and opportunities despite their creativity and capacity. The reason is the fact that the TNI has long relied on supplied facilities purchased from sourced vendors while neglecting their own self-development and utilization of home-grown products.

Being online in Indonesia today is simple and cheap. A military cyber operation may only require a rental computer in a local Internet café at a meager Rp 10,000 per hour; this war machine is capable of shutting down important strategic systems of an adversary.

The most expensive part of the operation, in terms of time and cost, is preparing the capable military human resources while at the same time preparing its civilian counterpart within the strategic management level and developing commanders with proper capabilities to run cyber operations to go beyond the expertise of attacking a system, but also how to defend and exploit them.

Learning from indications of concerted cyber attacks directed at Georgia and Estonia launched from Russia in 2007-2008, which Russia later denied, a method of Distributed Denial of Service (DDoS) attack managed to cripple the communication and information systems of both target countries.

Estonia received the brunt of the attack, as it is the most wired country in Europe, and the country's financial and communications systems were hit hard. Within a week, citizens of Estonia, unable to access funds kept in various banks and conduct commercial transactions, resorted to chaos and looting.

Although there has been no proof of a country being taken over physically by a cyber attack the disturbances created have shown it is something to worry about. Such an event may occur in Indonesia mainly because not many are aware of the critical dangers of such an attack.

Indonesia has developed more cyber network infrastructure in order to link the communication and information exchange. Today, around 55 million people in Indonesia are connected through cyber space by cellular networks only. The main business activity in Indonesia remains concentrated in Jakarta. So imagine Jakarta comes under a cyber attack.

Research conducted by the Indonesia Defense University (Unhan) found that the weakest link in the Indonesian cyber network lies within its financial sector through its Internet banking system.

The potential loss of a non-working bank for one day would easily reach Rp 1 trillion, and if that attack solely hit its ATM system, the potential loss might reach up to Rp 100 billion. Imagine if the attack lasted for one month.

This is a direct threat to national stability and will further directly endanger the capability of the Indonesian defense forces.

In a military conflict situation, the financial aspect is one of the important key factors as a driving factor for combat logistics thus showing the connection between the civilian financial sector and the military.

That is why financial institutions are high on the list along with the military's own center of gravity.

The formation of the Defense Ministry and TNI's Cyber Defense Task Force that is taking shape today may not be able to work alone. They have to involve the Indonesian communication and financial sectors to start building up awareness of their vulnerability as key cyber warfare targets.

The Defense Ministry and TNI need to work closely with other ministries, the National Police and strategic interests governing bodies in order to draw the baseline of common understanding of terms and to define an operable rule of engagement in dealing with cyber warfare, which may look like a common cyber crime. The Defense Ministry and TNI will also have to prepare means of coordination with friendly countries as part of efforts to reduce the potential of a cyber attack by proxy.

A good awareness and mitigation program through human and vital-resources readiness, steady communication and regular exercises among institutions will help Indonesia strengthen its defense capability and beyond.

Table of Contents

NATO War Games Set To Begin on November 16, 2012

NATO Press Release

The North Atlantic Treaty Association (NATO) announced it will conduct simultaneous war games beginning November 12 and 16, 2012, according to an official NATO press release.

The exercise will test readiness and defense capabilities to an escalating threat from enemy chemical, biological and radiological attacks, in combination with a large scale cyber attacks affecting NATO critical infrastructure.

It's being dubbed informally the "doomsday war game exercises."

"The Crisis Management Exercise will this year run concurrently with the NATO cyber defense exercise Cyber Coalition 12. The purpose of Cyber Coalition 12 will be to test Alliance technical and operational cyber defense capabilities. The two exercises CMX 12 and Cyber Coalition 12 will be conducted based on one single fictitious scenario portraying an escalating threat from chemical, biological and radiological attacks, including large scale cyber attacks affecting NATO and national critical infrastructure. This exercise scenario will require Allied political direction taking into account the advice of NATO military authorities and technical cyber defense bodies on possible measures to handle asymmetric threats."

"The CMX 12 will be jointly run by the NATO International Staff, the International Military Staff and the two NATO Strategic Commands, Allied Command Operations and Allied Command Transformation. This is NATO's 18th CMX since 1992. Finland and Sweden will participate as Partners alongside Allies in the exercise, as some elements of the scenario play out in their geographical proximity. Representatives of the International Committee of the Red Cross (ICRC) and of the Organization for the Prohibition of Chemical Weapons (OPCW) will observe the relevant aspects of the exercise and, representatives of the EU European External Action Service (EEAS) will actively contribute to the exercise. The annual exercise Cyber Coalition (CC) will test the effectiveness and efficiency of collaborative cyber defense procedures and capabilities. Together with Allies, 3 partner nations (Austria, Finland and Sweden) will participate this year as players, and 3 other partner nations (Australia, Ireland and Switzerland) will participate as observers. In addition, EU cyber defense staffs will observe the exercise"

Table of Contents

Army Leaders Emphasize Importance of Cyberspace Capabilities

From AUSA Annual meeting notes, 2 Nov 2012

The importance of the cyberspace capabilities will continue to grow, not only for specific cyber and space commands, but for the Army at large, according to a group of Army leaders in the cyber and space fields.

"Today cyberspace cuts across all sectors," said Lt. Gen. Rhett A. Hernandez, commanding general Army Cyberspace Command. "The Army is transforming the way it thinks about cyberspace…even in a period of reduced resources, we cannot afford not to."

Hernandez spoke, along with other Army leaders, at a panel form on Cyberspace during the Association of the United States Army's Annual Meeting and Exposition on Tuesday, Oct. 23.

He went on to describe how increased cyberspace capabilities allow the Army to prevent, shape, and win future conflicts. In addition, he explained how at every level now "coordination relies on cyberspace" and that it is now "indispensable for human interaction, including military actions."

Hernandez added that the growth of cyberspace is "changing the way we have to defend not only all Army networks…but also how we defend the nation [overall]."

"Neither space or cyber are ends in themselves," explained Lt. Gen. Richard P. Formica, commanding general, Army, Space and Missile Defense Command/Army Forces Strategic Command. "I don't envision a solely cyber war or a space war."

Formica added that space and cyber are separate domains that are interdependent but not interchangeable.

"We're not even fully there yet with space," said Formica, explaining that although the United States has operationalized and institutionalized space, the nation's space capabilities continue to expand.

From the intelligence perspective, Lt.Gen. Mary A. Legere, deputy chief of staff, G-2, explained the necessity of cyberspace capabilities in today's Army intelligence.

"Nothing we do in intelligence to support our warfighters around the world is possible without secure networks," she said.

Legere said that one of the main goals in the cyber realm as well as the Army at large is to "create a defensible, single network" that provides full-spectrum capabilities.

According to Lt. Gen. Donald M. Campbell, Jr., commanding general, III Corps and Fort Hood, "There are still a lot of challenges when it comes to permissions and levels of authority" in increasing the use of cyberspace and growing its capabilities in the Army.

"This is truly leaders' business and you have to be involved from the beginning," said Campbell, who later added that leaders must get incorporated in the cyber process early.

"We're a good investment because we do get the return on our investment," Lt. Gen. Susan S. Lawrence, chief information officer/G-6, said about cyberspace. "And we are definitely more secure at the end of the day."

Table of Contents

US Handoff in Afghanistan Includes Radio Training

By Sean Carberry, Transcript NPR News Weekend Edition, November 4, 2012

RACHEL MARTIN, NPR HOST: In Afghanistan, the U.S. military has long conducted propaganda campaigns to try to sway public opinion against insurgents. Now, the U.S. is teaching Afghan army units how to counter Taliban propaganda, especially with local radio. But it is hard to tell if the message is getting through.

NPR's Sean Carberry recently embedded with U.S. forces south of Kabul in Logar Province, and he brings us this story.

(MUSIC PLAYING)

SEAN CARBERRY, NPR CORRESPONDENT: From the outside, it looks like any other white metal container used for housing, offices or latrines here on Forward Operating Base Shank, the main NATO base in Logar Province south of Kabul. But inside is a fully functioning, - if spartan - radio studio. The U.S. military calls it a RIAB, or radio in a box.

SAIFITULLAH: (foreign language spoken)

CARBERRY: Saifitullah is the DJ and presenter this afternoon. He says the station is called Unity Radio and it broadcasts from 6 A.M. to 10 P.M. The signal reaches the surrounding provinces, and he says the station gets calls from listeners some 30 to 40 miles away.

SAIFITULLAH: We have different shows in this radio station, including political shows and also some recreational music and also messages.

CARBERRY: The propaganda messages are usually from the Afghan National Army, or ANA.

COLONEL HAYATULLAH MAMOND (through translator): The main focus of these messages is to tell the local people who the enemy is, and that the enemy is supported by people from outside Afghanistan.

CARBERRY: That's Colonel Hayatullah Mamond with the 4th Infantry Brigade of the Afghan army. He's one of the chief message writers. He says there are also messages targeting the insurgents and calling on them to lay down their weapons and join the peace process.

MAMOND (through translator): We tell them that fighting is not the answer. When there is peace in a country, there is development and jobs and people can live in prosperity.

MAJOR TOPAL WARED: (foreign language spoken)

CARBERRY: Major Topal Wared is the information dissemination officer for the 4th Brigade. It's a fairly new position. His job is to gather information from locals in areas patrolled by the Afghan army. He also researches Taliban propaganda and prepares counter-messages.

WARED (through translator): For example, the enemy recently went to a school in Maidan Warak Province. And they told the students that the ANA are not good people because they are cooperating with the Americans. So, we have to counter this propaganda.

CARBERRY: Major Chris Lawson is the information officer with the U.S. 173rd Airborne Brigade Combat Team. Since June, he's been helping the ANSF, or Afghan National Security Forces, with their messaging.

MAJOR CHRIS LAWSON: Initially, we were doing coalition-led messaging. Then, about a month or two in, our brigade commander said from here on out he wants all ANSF messages.

CARBERRY: He says the Afghans are increasingly self-sufficient. He says that in addition to the Radio in a Box, the Afghans can interact directly with the people and deliver messages face to face. That's important in a culture with a strong oral tradition, he adds, and where there are not a lot of TVs or radios to go around.

LAWSON: When it's time for us to leave, I think they'll be able to sustain that. But they need to start relying more on the local media.

CARBERRY: That's because the U.S. assets are disappearing amid the drawdown of forces. When he arrived in June, he had nine RIABs in Logar and neighboring Wardak province. And now they're down to four.

UNIDENTIFIED MAN: (foreign language spoken)

CARBERRY: The most difficult part of the equation is determining whether messages like this one, calling on young people to join the security forces and fight the foreign-backed enemies, are getting through and making a difference.

UNIDENTIFIED MAN: Since I've been here, I haven't done a study of how many people in whatever village listens to these RIABs that we have.

CARBERRY: So with coalition resources dwindling, getting the message out is just one more challenge the Afghans have to face as they confront the ongoing insurgency in Logar Province.

Table of Contents

China Most Threatening Cyberspace Force, U.S. Panel Says

By Tony Capaccio, BusinessWeek, November 05, 2012

China is “the most threatening actor in cyberspace” as its intelligence agencies and hackers use increasingly sophisticated techniques to gain access to U.S. military computers and defense contractors, according to the draft of an annual report mandated by Congress.

Chinese hackers are moving into “increasingly advanced types of operations or operations against specialized targets,” such as sensors and apertures on deployed U.S. military platforms, according to the report.

“China’s persistence, combined with notable advancements in exploitation activities over the past year, poses growing challenges to information systems and their users,” the U.S.- China Economic and Security Review Commission said in the draft obtained by Bloomberg News. “Chinese penetrations of defense systems threaten the U.S. military’s readiness and ability to operate.”

A U.S. intelligence official, speaking on the condition of anonymity to discuss classified matters, described as relentless China’s efforts to blind or disrupt U.S. intelligence and communications satellites, weapons targeting systems, and navigation computers.

The commission’s draft report bolsters warnings by U.S. officials that cyberattacks pose growing risks to the military and to critical industries such as electric utilities, pipelines, and telecommunications. Defense Secretary Leon Panetta cited Chinese and Russian capabilities in an Oct. 11 speech, saying cyber threats could become as devastating as the Sept. 11, 2001, terrorist attacks.

‘Zero-Day’ Attacks

Most cyber activity in China during the past year “relied on basic and straightforward techniques,” such as “zero-day” attacks that exploit a software vulnerability for which victims have no immediate fix or patch and the use of stolen digital certificates to make malware appear legitimate, according to the draft.

“Irrespective of the sophistication, the volume of exploitation attempts yielded enough successful breaches to make China the most threatening actor in cyberspace,” according to the draft.

Geng Shuang, a spokesman for the Chinese embassy in Washington, didn’t return an e-mail seeking comment on the draft report.

Most Chinese intrusions against U.S. government and military systems appear intended to collect intelligence or technology rather than launch attacks, the commission said. Penetrations of U.S. military systems, though, “could switch to become disruptive or destructive,” and that’s a danger because they “still reportedly require weeks to investigate.”

Illegal Subsidies

Created by Congress in 2000, the bipartisan commission has reported on China’s economic and military rise, usually in critical assessments accompanied by recommendations for counter- actions such as trade sanctions. Its annual overview and a yearly Pentagon report are the two primary publicly available official assessments of China’s military developments.

The draft on cybersecurity, part of an annual report scheduled for release on Nov. 14, calls for Congress to “develop a sanctions regime to penalize specific companies found to engage in, or otherwise benefit from, industrial espionage” and to define it as an “illegal subsidy subject to countervailing duties.”

The draft concludes that China’s network of civilian and military cyber specialists includes units of the People’s Liberation Army.

Retired Marine General James Cartwright, a former vice chairman of the U.S. Joint Chiefs of Staff, told the commission in March that, “While it is very difficult in cyber to have a ‘smoking gun,’ so to speak, the clear paths back into servers and other mechanical devices inside of the Chinese sovereign domain remain a constant problem for us.”

Cyber Militia

While the Chinese military’s ability to manage sophisticated computer systems is limited, according to the report, its leaders “recognize this weakness and intend to develop a pool of soldiers” who can manage cyber technology as well as advanced weapons systems.

China employs a “cyber warfare militia,” PLA civilian units “usually comprised of workers with high-tech day jobs” that focus on military communications, electronic warfare and computer network operations, the draft said.

The militia members are among the nation’s 538 million Internet users with access to 677 million devices that can be used to enter the Internet, according to the International Data Corp.

Holiday Dropoff

This scale of Internet access “greatly influences the global volume of malicious activity,” the draft says.

According to statistics supplied to the commission by San Francisco-based service provider CloudFlare Inc., attacks account for about 15 percent of global Internet traffic on any given day.

That “plummeted to about 6.5 percent” around Oct. 1, 2011, China’s National Day, “when many workers take leave,” according to the draft report.

China’s military capabilities, including cyberwarfare, haven’t been an issue in the U.S. presidential election even as Republican candidate Mitt Romney has criticized China on trade and currency issues.

Romney wrote in his book, “No Apology,” that China’s investments in “cyberwarfare, anti-satellite warfare and anti- ship weaponry, for example, are calculated to neutralize our military’s many strategic advantages.”

‘Strategic Competitors’

The commission in March released a report by Northrop Grumman Corp. (NOC) that concluded China’s cyber capabilities are advanced enough to disrupt U.S. military operations during a conflict over Taiwan. The draft report cites the Northrop Grumman study in outlining its broader conclusions about China’s advances.

The National Intelligence Council, using data culled from 13 U.S. agencies, concluded in November 2011 that “China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of U.S. economic information and technology.”

The China commission’s annual report last year disclosed that computer hackers, possibly from the Chinese military, interfered with two U.S. government satellites four times in 2007 and 2008 through a ground station in Norway.

Table of Contents

Data Triage and the Cyber Age

Posted By John Reed, Killer Apps, October 30, 2012

While the media has been getting itself worked up about the fact that American UAVs have broadcast video streams over unencrypted communications channels for years now, some in the military are taking a more nuanced approach to what battlefield data must be super secure.

Three years ago, news broke that insurgents in Iraq were able to watch UAV video feeds by using cheap software. This came more than a decade after video feeds from the MQ-1 Predator UAVs' first combat missions over the Balkans were inadvertently broadcast on local TV sets. And let's not forget the small frenzy that occurred when it was reported that a virus was recording keystrokes at U.S. Air Force drone command centers in 2011.

Some have dismissed the utility of hacking a drone feed without knowing exactly which aircraft's video is being looked at -- and therefore having the ability to warn potential targets. Others have a different take on this.

However, in light of ever-evolving cyber threats aimed at stealing as much data from -- well, everyone -- as possible, the Army is seeking to triage threats to its networks. What does this mean? It means figuring out what information warrants the significant investment in technology, time, and money required to protect it from hackers and what information will be useless if hacked. The latter is called perishable data, and in some cases it includes things like voice communications during a firefight. While this data would be encrypted against hacking by the enemy actually fighting U.S. forces, it wouldn't need to be hardened against hackers with advanced code-breaking abilities because by the time they tapped into the data and analyzed it, the fight would be over and the data useless.

"We recently made a big decision that's reducing a lot of our costs [and that] is going to [National Security Agency] Type 2 encryption for our push to talk radios at the tactical edge," said the U.S. Army's chief information officer, Lt. Gen. Susan Lawrence during a speech at the Association of the U.S. Army's annual conference in Washington last week. "We realized, did we really need full Type 1 encryption all the way to the dismounted soldier? No."

(Type 2 encryption is commonly used by the military to transmit sensitive but unclassified information.)

Lawrence's comments reflect the growing view among U.S. military commanders that it will be impossible to protect all of its networks and all the data on the networks. Therefore, the most important information must be heavily guarded against theft or corruption. and it must be kept on a network that is resilient enough to operate even while under attack.

"We can't protect all our networks . . . so it's more about the defense of our data. It's about the data, where do you put the information and the data, where should it reside so we can protect it," said Lawrence.

Table of Contents

Beyond Battleships and Bayonets

Space -- cyber and outer -- is the future frontier of the U.S. military. What kind of warfare will it yield?

By Alfred W. McCoy, TomDispatch, 8 Nov 2012

It’s 2025 and an American “triple canopy” of advanced surveillance and armed drones fills the heavens from the lower- to the exo-atmosphere. A wonder of the modern age, it can deliver its weaponry anywhere on the planet with staggering speed, knock out an enemy’s satellite communications system, or follow individuals biometrically for great distances. Along with the country’s advanced cyberwar capacity, it’s also the most sophisticated militarized information system ever created and an insurance policy for U.S. global dominion deep into the twenty-first century. It’s the future as the Pentagon imagines it; it’s under development; and Americans know nothing about it.

They are still operating in another age. “Our Navy is smaller now than at any time since 1917,” complained Republican candidate Mitt Romney during the last presidential debate.

With words of withering mockery, President Obama shot back: “Well, Governor, we also have fewer horses and bayonets, because the nature of our military’s changed… the question is not a game of Battleship, where we’re counting ships. It’s what are our capabilities.”

Obama later offered just a hint of what those capabilities might be: “What I did was work with our joint chiefs of staff to think about, what are we going to need in the future to make sure that we are safe?… We need to be thinking about cyber security. We need to be talking about space.”

Amid all the post-debate media chatter, however, not a single commentator seemed to have a clue when it came to the profound strategic changes encoded in the president’s sparse words. Yet for the past four years, working in silence and secrecy, the Obama administration has presided over a technological revolution in defense planning, moving the nation far beyond bayonets and battleships to cyberwarfare and the full-scale weaponization of space. In the face of waning economic influence, this bold new breakthrough in what’s called “information warfare” may prove significantly responsible should U.S. global dominion somehow continue far into the twenty-first century.

While the technological changes involved are nothing less than revolutionary, they have deep historical roots in a distinctive style of American global power. It’s been evident from the moment this nation first stepped onto the world stage with its conquest of the Philippines in 1898. Over the span of a century, plunged into three Asian crucibles of counterinsurgency — in the Philippines, Vietnam, and Afghanistan — the U.S. military has repeatedly been pushed to the breaking point. It has repeatedly responded by fusing the nation’s most advanced technologies into new information infrastructures of unprecedented power.

That military first created a manual information regime for Philippine pacification, then a computerized apparatus to fight communist guerrillas in Vietnam. Finally, during its decade-plus in Afghanistan (and its years in Iraq), the Pentagon has begun to fuse biometrics, cyberwarfare, and a potential future triple canopy aerospace shield into a robotic information regime that could produce a platform of unprecedented power for the exercise of global dominion — or for future military disaster.

America’s First Information Revolution

This distinctive U.S. system of imperial information gathering (and the surveillance and war-making practices that go with it) traces its origins to some brilliant American innovations in the management of textual, statistical, and visual data. Their sum was nothing less than a new information infrastructure with an unprecedented capacity for mass surveillance.

During two extraordinary decades, American inventions like Thomas Alva Edison’s quadruplex telegraph (1874), Philo Remington’s commercial typewriter (1874), Melvil Dewey’s library decimal system (1876), and Herman Hollerith’s patented punch card (1889) created synergies that led to the militarized application of America’s first information revolution. To pacify a determined guerrilla resistance that persisted in the Philippines for a decade after 1898, the U.S. colonial regime — unlike European empires with their cultural studies of “Oriental civilizations” — used these advanced information technologies to amass detailed empirical data on Philippine society. In this way, they forged an Argus-eyed security apparatus that played a major role in crushing the Filipino nationalist movement. The resulting colonial policing and surveillance system would also leave a lasting institutional imprint on the emerging American state.

When the U.S. entered World War I in 1917, the “father of U.S. military intelligence” Colonel Ralph Van Deman drew upon security methods he had developed years before in the Philippines to found the Army’s Military Intelligence Division. He recruited a staff that quickly grew from one (himself) to 1,700, deployed some 300,000 citizen-operatives to compile more than a million pages of surveillance reports on American citizens, and laid the foundations for a permanent domestic surveillance apparatus.

A version of this system rose to unparalleled success during World War II when Washington established the Office of Strategic Services (OSS) as the nation’s first worldwide espionage agency. Among its nine branches, Research & Analysis recruited a staff of nearly 2,000 academics who amassed 300,000 photographs, a million maps, and three million file cards, which they deployed in an information system via “indexing, cross-indexing, and counter-indexing” to answer countless tactical questions.

Yet by early 1944, the OSS found itself, in the words of historian Robin Winks, “drowning under the flow of information.” Many of the materials it had so carefully collected were left to molder in storage, unread and unprocessed. Despite its ambitious global reach, this first U.S. information regime, absent technological change, might well have collapsed under its own weight, slowing the flow of foreign intelligence that would prove so crucial for America’s exercise of global dominion after World War II.

Computerizing Vietnam

Under the pressures of a never-ending war in Vietnam, those running the U.S. information infrastructure turned to computerized data management, launching a second American information regime. Powered by the most advanced IBM mainframe computers, the U.S. military compiled monthly tabulations of security in all of South Vietnam’s 12,000 villages and filed the three million enemy documents its soldiers captured annually on giant reels of bar-coded film. At the same time, the CIA collated and computerized diverse data on the communist civilian infrastructure as part of its infamous Phoenix Program. This, in turn, became the basis for its systematic tortures and 41,000 “extra-judicial executions” (which, based on disinformation from petty local grudges and communist counterintelligence, killed many but failed to capture more than a handfull of top communist cadres).

Most ambitiously, the U.S. Air Force spent $800 million a year to lace southern Laos with a network of 20,000 acoustic, seismic, thermal, and ammonia-sensitive sensors to pinpoint Hanoi’s truck convoys coming down the Ho Chi Minh Trail under a heavy jungle canopy. The information these provided was then gathered on computerized systems for the targeting of incessant bombing runs. After 100,000 North Vietnamese troops passed right through this electronic grid undetected with trucks, tanks, and heavy artillery to launch the Nguyen Hue Offensive in 1972, the U.S. Pacific Air Force pronounced this bold attempt to build an “electronic battlefield” an unqualified failure.

In this pressure cooker of what became history’s largest air war, the Air Force also accelerated the transformation of a new information system that would rise to significance three decades later: the Firebee target drone. By war’s end, it had morphed into an increasingly agile unmanned aircraft that would make 3,500 top-secret surveillance sorties over China, North Vietnam, and Laos. By 1972, the SC/TV drone, with a camera in its nose, was capable of flying 2,400 miles while navigating via a low-resolution television image.

On balance, all this computerized data helped foster the illusion that American “pacification” programs in the countryside were winning over the inhabitants of Vietnam’s villages, and the delusion that the air war was successfully destroying North Vietnam’s supply effort. Despite a dismal succession of short-term failures that helped deliver a soul-searing blow to American power, all this computerized data-gathering proved a seminal experiment, even if its advances would not become evident for another 30 years until the U.S. began creating a third — robotic — information regime.

The Global War on Terror

As it found itself at the edge of defeat in the attempted pacification of two complex societies, Afghanistan and Iraq, Washington responded in part by adapting new technologies of electronic surveillance, biometric identification, and drone warfare — all of which are now melding into what may become an information regime far more powerful and destructive than anything that has come before.

After six years of a failing counterinsurgency effort in Iraq, the Pentagon discovered the power of biometric identification and electronic surveillance to pacify the country’s sprawling cities. It then built a biometric database with more than a million Iraqi fingerprints and iris scans that U.S. patrols on the streets of Baghdad could access instantaneously by satellite link to a computer center in West Virginia.

When President Obama took office and launched his “surge,” escalating the U.S. war effort in Afghanistan, that country became a new frontier for testing and perfecting such biometric databases, as well as for full-scale drone war in both that country and the Pakistani tribal borderlands, the latest wrinkle in a technowar already loosed by the Bush administration. This meant accelerating technological developments in drone warfare that had largely been suspended for two decades after the Vietnam War.

Launched as an experimental, unarmed surveillance aircraft in 1994, the Predator drone was first deployed in 2000 for combat surveillance under the CIA’s “Operation Afghan Eyes.” By 2011, the advanced MQ-9 Reaper drone, with “persistent hunter killer” capabilities, was heavily armed with missiles and bombs as well as sensors that could read disturbed dirt at 5,000 feet and track footprints back to enemy installations. Indicating the torrid pace of drone development, between 2004 and 2010 total flying time for all unmanned vehicles rose from just 71 hours to 250,000 hours.

By 2009, the Air Force and the CIA were already deploying a drone armada of at least 195 Predators and 28 Reapers inside Afghanistan, Iraq, and Pakistan — and it’s only grown since. These collected and transmitted 16,000 hours of video daily, and from 2006-2012 fired hundreds of Hellfire missiles that killedan estimated 2,600 supposed insurgents inside Pakistan’s tribal areas. Though the second-generation Reaper drones might seem stunningly sophisticated, one defense analyst has called them “very much Model T Fords.” Beyond the battlefield, there are now some 7,000 drones in the U.S. armada of unmanned aircraft, including 800 larger missile-firing drones. By funding its own fleet of 35 drones and borrowing others from the Air Force, the CIA has moved beyond passive intelligence collection to build a permanent robotic paramilitary capacity.

In the same years, another form of information warfare came, quite literally, online. Over two administrations, there has been continuity in the development of a cyberwarfare capability at home and abroad. Starting in 2002, President George W. Bush illegally authorized the National Security Agency to scan countless millions of electronic messages with its top-secret “Pinwale” database. Similarly, the FBI started an Investigative Data Warehouse that, by 2009, held a billion individual records.

Under Presidents Bush and Obama, defensive digital surveillance has grown into an offensive “cyberwarfare” capacity, which has already been deployed against Iran in history’s first significant cyberwar. In 2009, the Pentagon formed U.S. Cyber Command (CYBERCOM), with headquarters at Ft. Meade, Maryland, and a cyberwarfare center at Lackland Air Base in Texas,staffed by 7,000 Air Force employees. Two years later, it declared cyberspace an “operational domain” like air, land, or sea, and began putting its energy into developing a cadre of cyber-warriors capable of launching offensive operations, such as a variety of attacks on the computerized centrifuges in Iran’s nuclear facilities and Middle Eastern banks handling Iranian money.

A Robotic Information Regime

As with the Philippine Insurrection and the Vietnam War, the occupations of Iraq and Afghanistan have served as the catalyst for a new information regime, fusing aerospace, cyberspace, biometrics, and robotics into an apparatus of potentially unprecedented power. In 2012, after years of ground warfare in both countries and the continuous expansion of the Pentagon budget, the Obama administration announced a leaner future defense strategy. It included a 14% cut in future infantry strength to be compensated for by an increased emphasis on investments in the dominions of outer space and cyberspace, particularly in what the administration calls “critical space-based capabilities.”

By 2020, this new defense architecture should theoretically be able to integrate space, cyberspace, and terrestrial combat through robotics for — so the claims go — the delivery of seamless information for lethal action. Significantly, both space and cyberspace are new, unregulated domains of military conflict, largely beyond international law. And Washington hopes to use both, without limitation, as Archimedean levers to exercise new forms of global dominion far into the twenty-first century, just as the British Empire once ruled from the seas and the Cold War American imperium exercised its global reach via airpower.

As Washington seeks to surveil the globe from space, the world might well ask: Just how high is national sovereignty? Absent any international agreement about the vertical extent of sovereign airspace (since a conference on international air law, convened in Paris in 1910, failed), some puckish Pentagon lawyer might reply: only as high as you can enforce it. And Washington has filled this legal void with a secret executive matrix — operated by the CIA and the clandestine Special Operations Command — that assigns names arbitrarily, without any judicial oversight, to a classified “kill list” that means silent, sudden death from the sky for terror suspects across the Muslim world.

Although U.S. plans for space warfare remain highly classified, it is possible to assemble the pieces of this aerospace puzzle by trolling the Pentagon’s websites, and finding many of the key components in technical descriptions at the Defense Advanced Research Projects Agency (DARPA). As early as 2020, the Pentagon hopes to patrol the entire globe ceaselessly, relentlessly via a triple canopy space shield reaching from stratosphere to exosphere, driven by drones armed with agile missiles, linked by a resilient modular satellite system, monitored through a telescopic panopticon, and operated by robotic controls.

At the lowest tier of this emerging U.S. aerospace shield, within striking distance of Earth in the lower stratosphere, the Pentagon is building an armada of 99 Global Hawk drones equipped with high-resolution cameras capable of surveilling all terrain within a 100-mile radius, electronic sensors to intercept communications, efficient engines for continuous 24-hour flights, and eventually Triple Terminator missiles to destroy targets below. By late 2011, the Air Force and the CIA had already ringed the Eurasian land mass with a network of 60 bases for drones armed with Hellfire missiles and GBU-30 bombs, allowing air strikes against targets just about anywhere in Europe, Africa, or Asia.

The sophistication of the technology at this level was exposed in December 2011 when one of the CIA's RQ-170 Sentinels came down in Iran. Revealed was a bat-winged drone equipped with radar-evading stealth capacity, active electronically scanned array radar, and advanced optics "that allow operators to positively identify terror suspects from tens of thousands of feet in the air."

If things go according to plan, in this same lower tier at altitudes up to 12 miles unmanned aircraft such as the "Vulture," with solar panels covering its massive 400-foot wingspan, will be patrolling the globe ceaselessly for up to five years at a time with sensors for "unblinking" surveillance, and possibly missiles for lethal strikes. Establishing the viability of this new technology, NASA's solar-powered aircraft Pathfinder, with a 100-foot wingspan, reached an altitude of 71,500 feet altitude in 1997, and its fourth-generation successor the "Helios" flew at 97,000 feet with a 247-foot wingspan in 2001, two miles higher than any previous aircraft.

For the next tier above the Earth, in the upper stratosphere, DARPA and the Air Force are collaborating in the development of the Falcon Hypersonic Cruise Vehicle. Flying at an altitude of 20 miles, it is expected to "deliver 12,000 pounds of payload at a distance of 9,000 nautical miles from the continental United States in less than two hours." Although the first test launches in April 2010 and August 2011 crashed midflight, they did reach an amazing 13,000 miles per hour, 22 times the speed of sound, and sent back"unique data" that should help resolve remaining aerodynamic problems.

At the outer level of this triple-tier aerospace canopy, the age of space warfare dawned in April 2010 when the Pentagon quietly launched the X-37B space drone, an unmanned craft just 29 feet long, into an orbit 250 miles above the Earth. By the time its second prototype landed at Vandenberg Air Force Base in June 2012 after a 15-month flight, this classified mission represented a successful test of "robotically controlled reusable spacecraft" and established the viability of unmanned space drones in the exosphere.

At this apex of the triple canopy, 200 miles above Earth where the space drones will soon roam, orbital satellites are the prime targets, a vulnerability that became obvious in 2007 when China used a ground-to-air missile to shoot down one of its own satellites. In response, the Pentagon is now developing the F-6 satellite system that will "decompose a large monolithic spacecraft into a group of wirelessly linked elements, or nodes [that increases] resistance to… a bad part breaking or an adversary attacking." And keep in mind that the X-37B has a capacious cargo bay to carry missiles or future laser weaponry to knock out enemy satellites — in other words, the potential capability to cripple the communications of a future military rival like China, which will have its own global satellite system operational by 2020.

Ultimately, the impact of this third information regime will be shaped by the ability of the U.S. military to integrate its array of global aerospace weaponry into a robotic command structure that would be capable of coordinating operations across all combat domains: space, cyberspace, sky, sea, and land. To manage the surging torrent of information within this delicately balanced triple canopy, the system would, in the end, have to become self-maintaining through "robotic manipulator technologies," such as the Pentagon's FREND system that someday could potentially deliver fuel, provide repairs, or reposition satellites.

For a new global optic, DARPA is building the wide-angle Space Surveillance Telescope (SST), which could be sited at bases ringing the globe for a quantum leap in "space surveillance." The system would allow future space warriors to see the whole sky wrapped around the entire planet while seated before a single screen, making it possible to track every object in Earth orbit.

Operation of this complex worldwide apparatus will require, as one DARPA official explained in 2007, "an integrated collection of space surveillance systems — an architecture — that is leak-proof." Thus, by 2010, the National Geospatial-Intelligence Agency had 16,000 employees, a $5 billion budget, and a massive $2 billion headquarters at Fort Belvoir, Virginia, with 8,500 staffers wrapped in electronic security — all aimed at coordinating the flood of surveillance data pouring in from Predators, Reapers, U-2 spy planes, Global Hawks, X-37B space drones, Google Earth, Space Surveillance Telescopes, and orbiting satellites. By 2020 or thereafter — such a complex techno-system is unlikely to respect schedules — this triple canopy should be able to atomize a single "terrorist" with a missile strike after tracking his eyeball, facial image, or heat signature for hundreds of miles through field and favela, or blind an entire army by knocking out all ground communications, avionics, and naval navigation.

Technological Dominion or Techno-Disaster?

Peering into the future, a still uncertain balance of forces offers two competing scenarios for the continuation of U.S. global power. If all or much goes according to plan, sometime in the third decade of this century the Pentagon will complete a comprehensive global surveillance system for Earth, sky, and space using robotics to coordinate a veritable flood of data from biometric street-level monitoring, cyber-data mining, a worldwide network of Space Surveillance Telescopes, and triple canopy aeronautic patrols. Through agile data management of exceptional power, this system might allow the United States a veto of global lethality, an equalizer for any further loss of economic strength.

However, as in Vietnam, history offers some pessimistic parallels when it comes to the U.S. preserving its global hegemony by militarized technology alone. Even if this robotic information regime could somehow check China's growing military power, the U.S. might still have the same chance of controlling wider geopolitical forces with aerospace technology as the Third Reich had of winning World War II with its "super weapons" — V-2 rockets that rained death on London and Messerschmitt Me-262 jets that blasted allied bombers from Europe's skies. Complicating the future further, the illusion of information omniscience might incline Washington to more military misadventures akin to Vietnam or Iraq, creating the possibility of yet more expensive, draining conflicts, from Iran to the South China Sea.

If the future of America's world power is shaped by actual events rather than long-term economic trends, then its fate might well be determined by which comes first in this century-long cycle: military debacle from the illusion of technological mastery, or a new technological regime powerful enough to perpetuate U.S. global dominion.

Table of Contents

Cyber Response's Fatal Flaw: Mistrust

By Nicole Blake Johnson, Federal Times, 4 Nov 2012

In case of a major cyber attack on critical networks, experts warn that deep reluctance among the governmental and private-sector organizations to share vital information could blunt a swift response.

A number of former high-ranking federal officials staged a mock cyber attack exercise last week. The scenario: A computer virus of unknown origin cripples 40,000 computers and key business systems at a major U.S.-based oil company the day after Thanksgiving. The virus also infects backup systems and systems storing data on the pressure and safety parameters for drilling in the Gulf of Mexico. Computer systems that direct the company's trading operations also are down.

As a precaution, the CEO shuts down drilling in the Gulf, bringing one-fifth of the nation's daily oil production to a halt. His first priorities:

- Estimate the extent of the damage and prevent further impact.
- Get operations back online as soon as possible because it's the start of the holiday season and there are demands from the transportation sector and customers who need to heat their homes during the winter.
- Work with the company's lawyers to respond to U.S. and foreign regulators.

Sharing details about the attack with the FBI, Department of Homeland Security or the National Security Agency is last on the list.

"[I'm] not going to rush into sharing," said Dmitri Alperovitch, who played the oil company CEO at the Washington Post-sponsored event. Alperovitch is co-founder and chief technology officer at CrowdStrike, a security startup firm.

He said he first needed to understand the regulatory impact and legal liabilities before contacting the Energy Department, Environmental Protection Agency, Securities and Exchange Commission, Federal Energy Regulatory Commission and others. There might also be civil liabilities from customers and potential impact on oil and stock prices if details of the attack got out.

As CEO, Alperovitch said he would likely contact the director of the FBI and share the malicious code to help determine who was behind the attack, but he would share little, if any, information about the impact of the attack and wouldn't give the government access to the company's network.

"I don't need other folks in the kitchen," especially those the company has no control over, he said.

DHS Secretary Janet Napolitano, who spoke at the event but did not participate in the exercise, said the government needs to get better at sharing cyber information, at various classification levels, to assist companies. Real-time information sharing is key, Napolitano said. Without it, efforts to secure critical cyber networks will be delayed.

When DHS learns of an attack days or weeks later, it can't help mitigate the damage or alert other critical sectors of the attack, she said. It also delays forensics work to determine the source and intentions of the attack.

Former FBI deputy assistant director Steven Chabinsky, who played the role of FBI director, said information sharing with the company about the source of the attack would be slight initially. Chabinsky said some company officials could get limited security clearances to learn details about the attack.

The FBI would also ask for the company's incident log files to gather more details about the attack, Chabinsky said. When asked how hard the FBI would press to get those files, he said the aim is not to revictimize a victim. While there are forceful means of getting information, Chabinsky said the goal is for the company to voluntarily share the information.

Several cybersecurity bills in the Senate and House attempt to address the bureaucratic hurdles that prohibit intelligence agencies from sharing classified cybersecurity information with companies and that discourage companies from sharing information with each other or the government.

One of those, the Cyber Intelligence Sharing and Protection Act, which passed the House in April, would allow the government and industry to voluntarily share information about malicious attacks and viruses. Companies that share information under the bill's provisions would be granted legal protections if they are subject to a cyber attack.

Many experts argue that absent incentives, such as tax breaks or liability protection, there are no benefits for some companies to share cyber threat information with the government, let alone their competitors.

Failed legislation introduced by Sen. Joseph Lieberman, I-Conn., in February would have provided liability protection for companies that met voluntary security standards yet still but fell victim to an attack. Jeffrey Ratner, a top aide on the Senate Homeland Security and Government Affairs Committee, which Lieberman chairs, said he expects Senate Majority Leader Harry Reid, D-Nev., will reintroduce the bill during the lame duck session after the Nov. 6 elections. Potential changes to the bill have not been ruled out.

Table of Contents

'Dagger' Brigade Electronic Warfare Office Named Best In Army

By Sgt. Daniel Stoutamire, 2nd ABCT Public Affairs, October 22, 2012

PHOENIX -- In recognition of their efforts during the brigade's 2010-2011 deployment in support of Operation New Dawn, the Electronic Warfare Office with the 2nd Armored Brigade Combat Team, 1st Infantry Division received the Army Outstanding Unit Award from the Association of Old Crows during the association's annual convention Sept. 23-26 in Phoenix.

Founded in 1964 by veteran officers from the Strategic Air Command and Electronic Countermeasures when informal reunions of those men had become so large as to necessitate organization, the AOC has more than 14,000 members and chapters in more than a dozen countries spanning four continents. The nickname of "Old Crows" harkens back to World War II, when servicemen who jammed German and Japanese radar eventually became known as "Crows," a variant of their codename, "Raven."

"We didn't think we would win, but we knew we had done a lot," said Chief Warrant Officer 2 Eric Colon, 2nd ABCT EWO team. "But we honestly didn't realize exactly how much we'd done until we saw it all put together in our nomination (packet)."

Colon, along with his noncommissioned officer-in-charge, Sgt. 1st Class Brian Smith, presided over an impressive array of accomplishments, perhaps none more eye-catching than their efforts in increasing qualified specialists in electronic warfare from 20 percent of the Forces Command requirement to 319 percent within five months. As part of the last brigade in United States Division -- Center, Colon and Smith became a locus of counter-IED expertise.

"We were responsible not only for the safety of all of our convoys and logistical patrols, we were also in charge of coordinating the redeployment of our forces out of Iraq," Colon said. "We had to maintain the safety and security of nearly 1,000 vehicles (and) 3,500 Soldiers every day."

They accomplished this by using equipment such as CREW devices (Counter Remote-Control Improvised Explosive Device Electronic Warfare), which essentially place a jamming cloud, or bubble, around the vehicle in which they are located. This prevents insurgents from using cell phones, walkie-talkies, or other remote methods of detonating an IED.

"The system attacks those (remote device signals) and gives a layer of protection that we didn't have 7 or 8 years ago and has significantly reduced the casualties from those types of IEDs," Colon said. "The battlefield changed vastly when those devices were created."

Historically, the onus on electronic warfare in the U.S. military has fallen on the Navy, but following years of heavy casualties, the Army instituted its own EW program in 2009.

"I was one of the lucky Soldiers who got to graduate from the first official class in the (military occupational specialty) in 2009," said Smith, a former infantryman.

While they are enjoying their award, both Smith and Colon know that in such an evolving field, they must stay attentive to change.

"There's always new equipment coming out, so we are constantly training on those platforms to stay current," Smith said.

It's interesting to think, Colon said, that three or four years ago an Army unit winning this award would have been impossible. Now, it is quite normal.

"We've come from nowhere to running, without really crawling or walking," he said.

Table of Contents

IPO, KC Chiefs Enter Training Partnership

By Melanie L. Marcec, Information Operations Proponent Office Public Affairs, Nov. 1, 2012

The U.S. Army and the Information Operations Proponent Office recently entered into partnership with Kansas City Chiefs Media and Marketing through the Training with Industry Program — the first TWI with a National Football League franchise.

The TWI Program is officially defined as "a work-experience program to provide an extensive exposure to managerial techniques and industrial procedures within corporate America to competitively selected officers and non-commissioned officers."

TWI selectees continue to serve in the Army but they work exclusively for the civilian corporation for a specified period — usually one year.

For the Army to enter into a TWI partnership with a civilian corporation, the training received must not normally be available either through the military school system or civilian university system.

Seeking a TWI with the Kansas City Chiefs was not a quick process for Maj. Matt Yandura.

In 2009, Yandura was a "snowbird" before beginning the Functional Area 30 Information Operations Qualification Course at the IPO at Fort Leavenworth.

"The personnel chief at that time asked me to explore some options for the TWI Program, so I started looking at industry leaders — not just sports teams," Yandura said.

While many of the companies he researched were leaders in producing their respective products, Yandura said, "They weren't recognized leaders in their marketing efforts."

After completing the FA 30 QC and his next Army assignment, Yandura returned to the IPO — this time to serve as the personnel chief — and he resumed his research into a TWI partnership.

Yandura discovered the Kansas City Chiefs Media and Marketing production crew had received several Emmy awards for their live and streaming broadcasts, and he learned why the organization worked so well.

"In my opinion, the Chiefs invest in their people and technology. They have the right leaders with the right technical expertise," Yandura said.

When he became a seminar leader for the FA 30 QC, Yandura soon arranged an "off-site" marketing briefing for the students at Arrowhead Stadium.

After the briefing, Yandura said, "We were blown away. We started TWI negotiations soon after."

Rob Alberino, vice president of Kansas City Chiefs Media and Marketing, didn't hesitate when he was approached to host an off-site with the FA 30 students.

"We've given tours and taught a couple of classes so far," Alberino said. "Having the Army here is the best day of my whole year."

Even though Alberino never served in the military, many of his family members did, and he said he feels a profound appreciation and connection to the Army.

So much so that when the IPO and FA 30 QC showed up Oct. 24 to commemorate the TWI partnership, they surprised Alberino with an honorary enlistment.

During his recruiting interview, Alberino was asked which of the Army Values he felt was the most important.

"Loyalty — it comes easy when your team is winning," Alberino said. "When your team's losing, it's harder, but it's even more important."

The IPO will review applications for the TWI with the Chiefs at a panel scheduled later.

Some training objectives for the officer chosen for the TWI are to understand civilian "measures of effectiveness," such as audience analysis, polling and surveys, along with theme and message development and branding techniques.

In addition to the Kansas City Chiefs, the IPO also has established TWI partnerships with Hill and Knowlton Government Services and Siemens Corporation.

Table of Contents

Satellite Jammers Turned On

From Strategy Page, 25 Oct 2012

October 25, 2012: Syria and Iran are being accused of jamming news service by BBC, France 24, Deutsche Welle, and the Voice of America, via radio and satellite, directed at Iran and Syria. This jamming was apparently in retaliation for European communications satellite operators refusing to continue carrying 19 Iranian TV and radio channels (as part of the growing embargo on Iran). Syria and Iran denied they were jamming but there is ample evidence that the jamming is coming from Syria and Iran. Over the last decade the U.S. has developed equipment and techniques for locating the source of jamming with considerable accuracy.

Then there is the increasing number of incidents of space satellites being "hacked". It turned out that this was actually just an increase in the number of satellites up there and the number of ground stations broadcasting information up into the sky. Most of these "hacks" are just satellite signals interfering with one another. Same with cases where people believe their GPS or satellite communications signals are being jammed. On further investigation the real reasons tend to be less interesting and a lot more technical. All this usually has a large element of human error mixed in. But the recent problems with signals directed at Iran and Syria appear to be jamming.

But all this accidental jamming only demonstrates how easy it is to do it on purpose, and there have been several examples of that. In response the U.S. Air Force, which has taken the lead in developing electronic tools for attacking and defending satellite communications, and the satellites themselves, has been training people to attack and defend space satellites. This effort involves figuring out new, or improved, ways to jam satellites. Then you keep that stuff secret, in case potential enemies have not figured this out themselves. Next, you work on ways to defeat the weapons developed. Most of this is playing around with the signals themselves. You can un-jam a jamming signal with another signal. However, a lot of trial and error is required, and you want to get that done way in advance of any actual war. When you do have to use this stuff for real, you have to expect that the enemy may well have come up with some angle you missed. Thus there will be some rapid improvisation, and you will have more time and resources for this if you have worked out ahead of time the details of disasters you have already anticipated. No one is releasing much information about this, for obvious reasons. There won't be much discussion from any government, unless there is a terrorist attack using these techniques. That's yet another thing to worry about. There have already been such attacks in China, by a banned religious group, and elsewhere. It can be done, it just isn't easy and it's not getting any easier.

Table of Contents

Another Tool in the Influencer’s Toolbox: A Case Study

By LTC Jamie Efaw and SFC Chris Heidger, Global ECCO – Combatting Terrorism Exchange vol 2, no 4, 2012

Much of the recent writing within military circles surrounding social media has centered on what can be learned from "bad guys'" use of social media sites, or the role social media played (and play) in events such as the Arab Spring and Haiti disaster relief. However, from an information operations perspective, the "golden ticket" in our operations is the ability to influence behavior and attitudes. The questions we address in this article are: "Can an information operator use social media to influence audiences, and if so, how?" Attitudes and behaviors cannot be changed overnight; doing so requires exposure to a persuasive message repeatedly over an extended period of time—a task social networking tools are perfectly designed to accomplish. One should not, however, view social media as the single best way to exert influence, but rather, see online networking as another tool in the communicator's toolbox that enhances larger influence campaigns. In this paper, we will share some of our experiences from putting theory into practice, our phased approach, some lessons learned, and recommendations for getting started in your own organization.

Getting Started and Building the Target Audience

In the winter of 2008, I (Jamie Efaw) published a paper in IO Sphere titled "Social Networking Services: The New Influence Frontier."[1] I had been thinking about these ideas for quite a while, and at the time, the paper was largely theoretical, focused on the "whys" and "hows" of social networking platforms and their application toward counterterrorism efforts. In 2009, my new NCOIC (non-commissioned officer in charge) and co-author Chris Heidger and I arrived at the United States European Command (EUCOM) in Stuttgart, Germany at the same time. We found we had inherited an eightyear old regional Web news and information initiative called the Southeast European Times or SETimes, which had an accompanying eight-month old Facebook companion presence.[2] We both saw this situation as a perfect opportunity to leverage social media and apply the theoretical framework I'd developed in my paper to a real-world situation. As a starting point, we identified four goals for having a social media presence:

1. Take advantage of the existing social media community to introduce and draw them to SETimes.com.
2. Provide an additional forum that exposes our target audience to our themes and messages.
3. Provide a convenient place for the SETimes community to discuss regional topics of interest and interact in an environment where they are comfortable and familiar.
4. Establish a communication platform we could use during a crisis, humanitarian assistance, or disaster relief operation.

In an effort to minimize the risk of our enterprise failing to catch hold or committing a public relations foul, while simultaneously maximizing learning and flexibility, our social media expansion efforts took a very deliberate five-phase approach, which is laid out in detail below:

Phase 0: Establish a Facebook Presence

Phase I: Research and Improvement

Phase II: Focused Advertising

Phase III: Increased User Interaction

Phase IV: Shift Focus onto Established Social Networks

Figure 1 summarizes the SETimes' Facebook fan growth by phase from March 2010–January 2011.

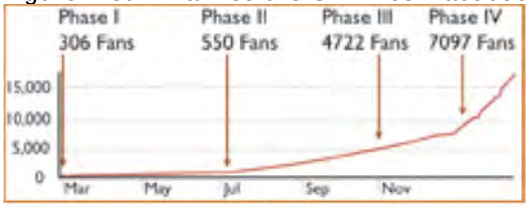
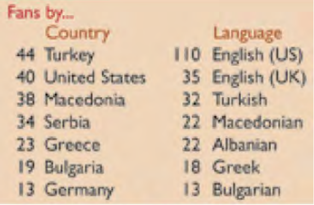


Figure 1. Fans by Phase

Phase 0: Establish a Facebook Presence (March 2009– February 2010)

Phase 0 started prior to our arrival at EUCOM, and consisted of creating a Facebook page for SETimes, adding a RSS feed from the webpage to the Facebook page, and putting a Facebook link at the top of the SETimes homepage.

During our first six months on the job we made no changes; noting that readership ("fans") and interaction (fans "liking" a post or making a comment) on the Facebook page did not increase over that time, however, we realized that in preparation for Phase 1 we needed to benchmark the current initiative. We do not see ourselves as competitors with the Department of State (DoS), but we used official DoS Facebook pages to serve as a yardstick for our site, since they have a comparable presence around the globe. A year after its creation, the SETimes' Facebook page gained an average of less than one fan per day, for a total of 306, and ranked in the bottom 15% when compared to similar DoS pages. Our audience was largely U.S.-based, and there were more English-speaking fans than all other languages combined (see Figure 2).



Fans by...

	Country		Language
44	Turkey	110	English (US)
40	United States	35	English (UK)
38	Macedonia	32	Turkish
34	Serbia	22	Macedonian
23	Greece	22	Albanian
19	Bulgaria	18	Greek
13	Germany	13	Bulgarian

Figure 2. Phase 0 Results

Phase 1: Research and Improvement (March–June 2010)

In March of 2010, we began our research and improvement phase, which started with the question: "What is the dominant social media platform in Southeast Europe?" A good surface-level tool for this research is Alexa.com,which identifies the most popular sites in a targeted region. With Facebook rated as the frontrunner (which will not always be the case), we then evaluated successful Facebook presences similar to SETimes, such as U.S. government pages and those of other regional news organizations, to get an idea of what they were doing right.

Based on our findings, we took a few minor steps to improve our Facebook page. First, we opted to manually post content in lieu of RSS feeds, which for a social platform we decided were too impersonal, mechanical, and annoying. Second, we added new features such as photo albums and a discussion tab with conversation topics, in an effort to promote a social atmosphere that was more in line with Facebook's interactive environment. Third, we published a story on SETimes.com about Facebook in Southeast Europe, which also encouraged readers to join our Facebook page (see Figure 3).[3]

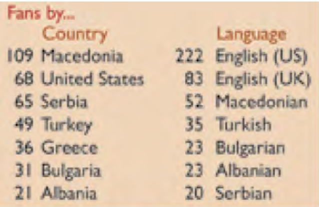
SETimes.com

Facebook has a friend in Southeast Europe

Figure 3. SETimes Article about Facebook in Southeast Europe

Lastly, in May 2010, we provided basic Facebook instruction at our annual SETimes writers' conference, and encouraged our contributors to become "fans" and interact on our page.

Despite focusing on Southeast European audiences, Figure 4 shows that we still had a very large U.S.-based audience and an even larger ratio of English-speaking fans than we had at the end of phase 0. While we understood that we still had a long way to go, we were encouraged that our new fans per day had doubled, indicating an increase in the page's appeal.



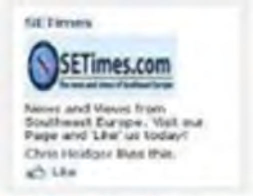
Fans by...

	Country		Language
109	Macedonia	222	English (US)
68	United States	83	English (UK)
65	Serbia	52	Macedonian
49	Turkey	35	Turkish
36	Greece	23	Bulgarian
31	Bulgaria	23	Albanian
21	Albania	20	Serbian

Figure 4. Phase I Results

Phase II: Focused Advertising (July–October 2010)

Phase II, which started in July 2010, is where our project started gaining significant momentum. The first noteworthy change was the introduction of advertising to Facebook users in SETimes' twelve core countries (see Figure 5).



SE Times

SETimes.com

News and Views from Southeast Europe. Visit our Page and 'Like' us today!

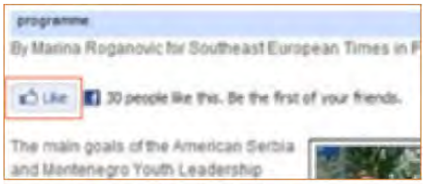
Chris Heidger likes this.

Figure 5. Facebook Advertisement

We chose a rate of $5/day, which made Facebook advertising a cost-effective as well as user-friendly tool. Getting started requires only a credit card, some small thumbnail images, an introductory sentence, and an intended audience. Once established, advertising costs are set through a daily geographically- dependent bidding process that ranges from less than U.S. 10 cents to more than $1.00 per ad click.

Demographic data are the greatest advantage that Facebook provides a planner. These data include age, sex, country, city, marital status, education level, and even interests, all of which are gathered as users establish and update their profiles. These are the data that focus advertising and provide excellent, real-time, demographically separated measures of performance. Although we have used Facebook ads only to increase the number of fans on our Facebook page, these ads can satisfy other objectives such as advertising an event, directing people to a website, or simply getting a target audience to download an application.

While advertising was an important step, we also added some additional features to enhance the users' overall experience during this phase. First, we added the "Like" button to individual articles on SETimes (Figure 6).



programme

By Marina Roganovic for Southeast European Times in P

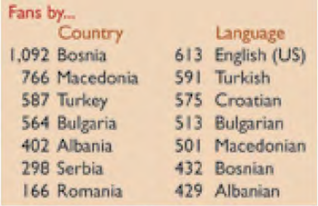
30 people like this. Be the first of your friends.

The main goals of the American Serbia and Montenegro Youth Leadership

Figure 6. Facebook Like Button on SETimes Article

When SETimes readers who are also Facebook users click that they "like" something, the action is indicated on their Facebook pages, and shows up on their friends' pages, along with a link to the "liked" content. Second, we added prompts to our Facebook posts in order to encourage interaction. Typically, we would link to a recently published SETimes article and then post a related question or comment. For example, we posted an article about the start of the Croatian president's second year in office, along with the following question: "Josipovic started his 2nd year as President of Croatia. How do you think he did in his 1st year? Share your thoughts."

Throughout Phase II we saw a sharp increase in the growth of fans from our target region (see Figure 7). Due to focused advertising, we now gained a daily average of 35 new fans, 99% of whom were from our target audience. As also depicted in Figure 7, U.S. readers dropped off the readership chart, and English language usage as a proportion diminished.



Fans by...

	Country		Language
1,092	Bosnia	613	English (US)
766	Macedonia	591	Turkish
587	Turkey	575	Croatian
564	Bulgaria	513	Bulgarian
402	Albania	501	Macedonian
298	Serbia	432	Bosnian
166	Romania	429	Albanian

Figure 7. Phase II Results

After four months of posting content to our page once every five days, we realized that Facebook users tended to visit pages other than their own only on the day new content appeared on their wall. The "if you build it, they will come" model, in other words, does not apply in social media. In the world of "new media," consumers no longer actively seek out or pull information; instead, they subscribe to topics of interests and have the information fed to them. In Phase III we adjusted our approach to fit this model.

Phase III: Increased User Interaction (November–December 2010)

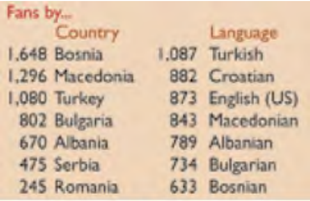
Phase III began in November 2010. The goals in this phase were to implement lessons learned from Phases I and II, increase fan interaction, and test some of the more specific advertising techniques.

Observations from previous phases revealed that the timing of Facebook posts affected interaction levels. For two weeks we logged hourly Facebook traffic from 0600–2300. This showed us that peak traffic for our target audience occurred between 0900–1000 and 1700–1830. Based on these findings, we began posting to Facebook twice a day, during each of these periods. We reasoned that this technique would optimize views and reader interaction while minimizing the risk of becoming a nuisance. To further encourage interaction, we started producing exclusive content for our Facebook page such as video essays, and we introduced a weekly "hook," such as a survey question, a "complete the sentence" statement, a "fan of the month" post, or a quote of the week.

Other early engagement efforts taught us several useful lessons. First, heavier content, such as the re-posting of a SETimes feature article, performed better in the morning, while lighter posts received better traction in the evening. These lighter interactive evening posts (often devoid of core themes and messages) were essential to keep the page in line with the social nature of Facebook. Finally, we found that simple encouragement such as, "Thanks for your comment, we value your insight," or "Interesting photo, can you tell us more about it?" proved invaluable as a method to keep fans engaged and let them know we were paying attention to them.

From our advertising campaign, we observed another interesting trend. During Phases I and II, audiences from our lower-priority countries (based on existing national and command guidance) quickly used the majority of our daily advertising budget by clicking on our ads more frequently than higher priority-country audiences. To rectify this, we divided our increased advertising budget of $10/day in accordance with SETimes' established three tier priority system. Tier 1 (highest priority) audiences received $5/day, while Tier 2 audiences received $3/day, and Tier 3 received only $2/day. Lastly, due to the steadily increasing number of fans and interaction, we anticipated a need for a Facebook Terms of Service statement that would provide general information about SETimes, and codify acceptable and unacceptable member conduct.[4] Our Terms of Service proved useful later when dealing with inappropriate reader comments.

Until this phase, EUCOM command policy was to block all social media sites, so all these Facebook activities had to be managed from non-government computers. After months of dialogue with communicators across the staff, Admiral James Stavridis, the EUCOM commander, published a comprehensive social media policy granting command access to social media sites. In addition to making our Facebook campaign far more convenient to maintain, workplace access enabled us to determine peak traffic times, increase posting frequency, and continuously monitor our Facebook page— maximizing the efficiency of a real-time communication platform. During Phase III, English-language users continued to drop off, while fans who used SETimes target-country languages continued to increase at a rapid pace (see Figure 8). While our advertising doubled, there was, surprisingly, an increase of only four more fans per day compared to our daily average in Phase II—a trend that has not changed. In fact, the return on investment dropped off very rapidly as daily advertising levels increased. For example, if a Facebook page gets twenty new fans per day for $10, it does not necessarily mean that investing $50 per day will bring in one hundred fans.



Fans by...

	Country		Language
1,648	Bosnia	1,087	Turkish
1,296	Macedonia	882	Croatian
1,080	Turkey	873	English (US)
802	Bulgaria	843	Macedonian
670	Albania	789	Albanian
475	Serbia	734	Bulgarian
245	Romania	633	Bosnian

Figure 8. Phase III Results

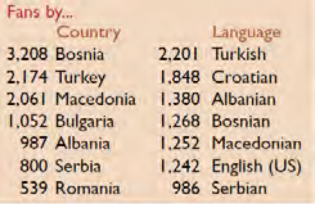
Phase IV: Shift Focus to Established Social Networks (January 2011–ongoing)

At the beginning of 2011, we initiated Phase IV, which involved increasing the advertising budget to $100/day and focusing our efforts on increasing four measurable Facebook page user actions: 1) page visits; 2) page "likes"; 3) fan interaction; and 4) referrals to SETimes.com (i.e., reads of SETimes.com content). In order to promote an increase in the above actions, we recognized the need to leverage the power of social comparison that is inherent in the Facebook platform. Social Comparison Theory postulates that people evaluate their opinions and actions based on their peer group. When one's own opinions or beliefs are in contradiction to the comparison group, there is a tendency to either change one's own opinions or attempt to convince others that your beliefs are correct in order to re-establish group cohesion. Typically, when encountering content on a traditional website, the reader does not know what other friends have read the same article, who liked it, or what they thought about the content they read. Social media platforms, however, are by definition built on social connections, and thus are formatted to allow the reader or fan to engage in social comparison.[5]

In previous phases, we advertised to all Facebook users within SETimes' established target audience (over 30 million Facebook users, and growing). This all-encompassing approach established nodes in existing social networks in every corner of our focus countries; however, the majority of our fans were not connected in any meaningful way. To rectify this, we expanded established nodes (existing SETimes Facebook fans) and began advertising only to their Facebook "friends." Currently, a tag at the bottom of every SETimes Facebook ad might say something like, "Joe Smith likes this." As more "friends" within a circle "liked" the ad, it might say "Joe Smith and 5 of your friends like this"—increasing the power of social comparison with every new fan.

These newly formed pockets of SETimes fans not only increased the effectiveness of our advertising, but also increased the potential of both online and offline conversations with friends surrounding the content of the

Facebook posts. Figure 9 illustrates that previously observed trends continued, with a marked increase in the growth of fans from the target audience.



Fans by...

	Country		Language
3,208	Bosnia	2,201	Turkish
2,174	Turkey	1,848	Croatian
2,061	Macedonia	1,380	Albanian
1,052	Bulgaria	1,268	Bosnian
987	Albania	1,252	Macedonian
800	Serbia	1,242	English (US)
539	Romania	986	Serbian

Figure 9. Phase IV Results

Once a social media user joins the site or page, social comparison continues to have an influence. When readers interact with content on Facebook, they immediately know how many other total users have "liked" the content, but more importantly, they know how many and which of their own friends (their comparison group) "liked" it (they do not see which of their friends do not like an article). Additionally, they can see any comments made about the content and make comments of their own in real-time. Whether the reader tries to change the opinion of friends or changes his or her own to match theirs, either outcome could be useful for the influencer if properly managed.

Lessons Learned and Difficulties

Over the last eighteen months we have identified several advantages, difficulties, and lessons learned while using Facebook, many of which already have been discussed above. The following section offers nine broad topics we consider principles for getting started.

1. Research and listen.

Where are the conversations among your target population taking place? On what platforms? What are the advantages and disadvantages of the different social media platforms for reaching your audience? Answer these basic questions before launching a social media effort.

2. Have a plan, but experiment. Be deliberate, expect failures, and be flexible.

Before starting, have a plan and be deliberate in your method, but also leave room to experiment. The same principles that worked for us will not necessarily work for everyone. As you experiment, start small, expect failures, and be prepared to make adjustments. This will ensure you have the flexibility to make required changes while minimizing the negative effects of failures and growing pains.

3. Provide fans with experiences. Make interaction easy. But do not saturate!

We found that to get fans involved with our content, we needed to provide online "experiences" that invited them to interact. An activity that encourages engagement, participation, and conversation, yet remains easy and quick for the reader, is ideal. In the social media world, more is not always better. A user typically is not going to join in an in-depth erudite dialogue, but most will likely vote in a poll, complete a sentence, or "like" a quote. Too much information (i.e., too many posts) hinders your effort. At best you run the risk of being ignored, and at worst, annoying the individuals you want to influence.

4. Benchmark your efforts and progress.

Benchmarks help you see progress toward your goal. If you do not establish a reliable baseline from the outset of your activity, it is impossible to show how far you've come at subsequent benchmarks, or at the end of your effort. In March of 2010, SETimes' Facebook page had 306 fans and was ranked in the bottom 15% when compared to similar DoS Facebook pages. Less than a year later, we had over 17,300 fans and it was ranked in the top 6% compared to similar pages. Other aspects can be benchmarked as well. Our Phase IV measurable actions provide a good starting point: 1) page visits; 2) page "likes;" 3) fan interaction; and 4) referrals to an external website (i.e., reads).

5. Add a Terms of Service policy.

A Terms of Service policy outlines acceptable and unacceptable user behavior on the site. By stating policies upfront, you have de facto authority to delete inappropriate posts and ban disruptive users from the site. On several occasions, this policy enabled our fans to regulate each other and make sure that fellow fans abided by the spirit and the letter of the policy. This was also a welcome indication to us that our page's fans were taking "ownership" of the page and regarded it as theirs to monitor.

6. Educate the organization.

Much can be written about educating your organization. Be aware that some individuals will never understand, or desire to understand, what you're doing and how you're doing it. However, there are others who are willing to learn. Help these people set up an account and show them how social media work, then encourage them to experiment from their personal computers. Ensure you are an available resource to answer questions, but be careful to do it without making anyone feel stupid. Locate and mobilize key personnel in your organization. If possible, find senior leaders in your organization who "get it" and who will act as advocates when needed. Similar to the "start small and expect failures" discussion above, do not make unreasonable or unrealistic promises to your bosses. We kept our developmental phases pretty quiet until we were able to demonstrate some solid metrics. Furthermore, because we started small, there was no need or requirement to report setbacks.

7. Real-time interactions.

Real-time interactions are both Facebook's greatest advantage and its greatest challenge. The challenge lies in the fact that these interactions require constant monitoring in order to respond appropriately. Social media encourage conversation, which assumes timely responses. Failure in this area alienates fans and discourages future participation. A unique advantage of real-time interaction on Facebook, however, is that every time a fan comments on a discussion thread, the comment is sent out to everyone who has previously taken part in that thread, as well as all of the friends of the commenters. This feature continues to draw people back into the dialogue.

8. Translation and the use of an official language.

It is important to be aware that social media tools are ideally suited for campaigns focused on a single audience with a common language and problem set. Our audience, in contrast, spans twelve countries and ten spoken languages. Regardless of language(s) used, there are two translation management issues: 1) fan comments submitted in a language other than the page's official language(s); and 2) the general difficulty of maintaining oversight on a second-language (for the manager) fan page. For the first issue, on-call translators are required; this, however, can take time. While waiting for full translation, we have found the Google Translate and Live Translate applications to be useful for an immediate base-line understanding. To maintain oversight of a second-language Facebook page requires a minimum of one full-time, native speaking-level employee.

9. Leadership's lack of understanding.

There are many people who view Facebook as an invasive site that reveals far too much information about its users. Although mistrust was a more common problem three to four years ago, it still is an identifiable generational issue and a recognizable hindrance to social media initiatives within an organization.[6] While many senior-level leaders still do not fully understand social media, most at least understand its importance. Basic understanding and acceptance is all one needs to move forward.

Summary and Conclusion

When we look back at the original four goals we set for getting involved in Facebook, we are gratified to see that we achieved each of them.

- *Leverage the existing social media community to introduce and draw them to SETimes.com*.

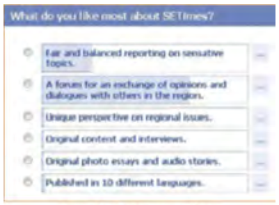
By the middle of 2012, we will have accumulated nearly 400,000 SETimes Facebook fans. Nearly all of these members of our target audience are individuals who had never heard of SETimes.com, nor been exposed to the website's themes and messages prior to the launch of our Facebook page. Additionally, in 2011, we recorded over 120,000 visits to SETimes.com from readers who came directly from our Facebook page; in other words, they were on the SETimes' Facebook page, clicked on a hyperlinked headline that interested them, and then read the full article on SETimes.com.

- *Provide an additional forum that exposes our target audience to our themes and messages.*

If a fan never clicked on one of the Facebook-posted links taking them to the SETimes.com content, they would still be exposed, three times a day, seven days a week, to its themes and messages via postings and interactive features on the SETimes' Facebook wall.

- *Provide a convenient place for the SETimes community to discuss regional topics of interest, and interact in an environment where they are comfortable and familiar.*

We assessed our achievement of this goal by asking our fans, in a Facebook poll on January 23, 2012, what they liked most about the SETimes' Facebook page. The great majority (72%; 1720 of 2390) of respondents acknowledged that the feature they appreciated most was that the page provided "a forum for an exchange of opinions and dialogues with others in the region" (see Figure 10).



What do you like most about SETimes?

○ Fair and balanced reporting on sensitive topics.

○ A forum for an exchange of opinions and dialogues with others in the region.

○ Unique perspective on regional issues.

○ Original content and interviews.

○ Original photo essays and audio stories.

○ Published in 10 different languages.

Figure 10. Poll Question: What do you like about SETimes?

- *Establish a trusted communication platform that can be leveraged during a crisis, humanitarian assistance, or disaster relief operation.*

This function was validated on several different occasions. A good example occurred in September 2011 during a flare-up of tensions at the Serbia-Kosovo border. Utilizing the SETimes' Facebook page, we were able, first, to inform the target audience of the actual situation on the ground, thereby discrediting rumors and disinformation. As a result of this effort, combined with our Google advertising, SETimes' coverage of the event was the #1 overall search result in Google news. Second, by utilizing the Facebook polling option, we were able to quickly gauge sentiment among the target audience, and provide that information to commanders and decisionmakers. The fact that our audience trusted the integrity of our information was key to our success on these occasions.

The question posed in the first paragraph of this article, you may recall, was: "Can an information operator use social media to exert influence and if so, how?" After two and a half years of daily experience with the SETimes platform, it is evident to us that Facebook and other social media sites are valid influence tools. First, social media allow an influencer to expose the target audience multiple times to the crafted content. As one can observe in Figure 11, over one million Facebook users were exposed to (had read or viewed) SETimes Facebook content more than five times in a seven-day period.

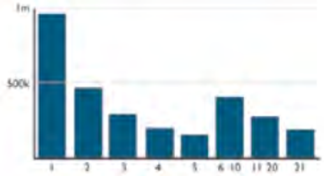
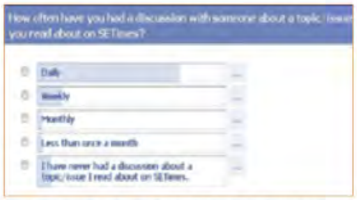


Figure 11. Total Views x Frequencies of Views from 1–7 January 2012

One reason this statistic is encouraging is that users not only saw SETimes content several times, but they chose to have our content delivered to them or they actively sought it out.

Second, we discovered that appropriately designed content prompts the target audience to share the message with others. Participation in a dialogue or a conversation about a topic encourages an individual to think deeply about the topic. To see how often this was occurring, in December 2011, we asked the poll question: "How often have you had a discussion with someone about a topic/issue you read about on SETimes?" (see Figure 12). Eighty-nine percent (2099/2365) of respondents acknowledged that they had had conversations about SETimes' content either daily or weekly.



How often have you had a discussion with someone about a topic/issue you read about on SETimes?

○ Daily

○ Weekly

○ Monthly

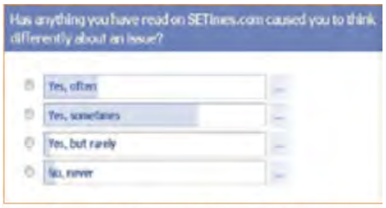
○ Less than once a month

○ I have never had a discussion about a topic/issue I read about on SETimes.

Figure 12. Sharing with Others Poll Question

These results confirmed that our target audience is thoughtfully considering the material presented by SETimes. The results also indicate that the online target audience is expanding the reach of the SETimes' message by having conversations with their off-line, real-world social network, thus expanding SETimes' sphere of influence.

Lastly, while we have illustrated that well-designed social media offer the tools to deliver a message and encourage dialogue, measuring influence (effectiveness) still remains difficult. Besides observing a change in the behavior of members, self-reporting (polling) is often the only method for determining effectiveness. To this end, we asked our Facebook fans: "Has anything you have read on SETimes.com caused you to think differently about an issue?" (see Figure 13). Although people are often reluctant to admit they have been influenced, an impressive 93 percent (2693/2916) of SETimes' Facebook fans who responded acknowledged they had been affected by our product. As one can gather from our experiences, social media initiatives require constant attention; the good news is that they require only limited personnel and funding to have an impact. No matter how enticing this high return on investment may sound, however, it is essential to keep in mind that Facebook, or any social media platform, is not a stand-alone tool. In fact, it will always work best in concert with traditional communication tools supporting a larger effort, event, or cause, such as, in our case, the SETimes news and information website. Used properly, this rapidly evolving capability is proving itself a tremendous addition to the communication toolbox.



Has anything you have read on SETimes.com caused you to think differently about an issue?

○ Yes, often

○ Yes, sometimes

○ Yes, but rarely

○ No, never

Figure 13. Influence Indicator Poll Question

About the Author: LTC Jamie Efaw serves as the Fort Story ASA Commander and Deputy Commander for Joint Expeditionary Base Little Creek-Fort Story in Virginia Beach. He was commissioned into the Corp of Engineers by the United States Military Academy at West Point in 1993 with a degree in Psychology. After receiving his Master's Degree in Social Psychology, LTC Efaw went on to teach in the Behavioral Science and Leadership Department at West Point, and branch transferred to Psychological Operations. After serving in the 4th Psychological Operations Group at Fort Bragg, North Carolina, LTC Efaw served as the United States European Command's Military Information Support Operation officer. From 2009–2012, SFC Chris Heidger was the Senior Enlisted Military Information Support Advisor at the U.S. European Command in Stuttgart, Germany, where he and LTC Efaw managed Southeast European Times. A nine-year PSYOPS veteran, Chris has spent five years overseas with tours in Iraq, Afghanistan, Africa, and, most recently, Europe. Chris earned a BA in Political Science from American Military University, and recently finished the coursework for a Master's of Professional Studies in Strategic Public Relations at George Washington University.

Footnotes:

[1] James M. Efaw, "Social Networking Services: The New Influence Frontier," IO Sphere (Winter 2008): 4-7; http:// www.au.af.mil/info-ops/iosphere/09winter/iosphere_ win09_efaw.pdf; accessed on September 27, 2012.

[2] The Southeast European Times website is a central source of news and information about Southeastern Europe, offered in ten languages: Albanian, Bosnian, Bulgarian, Croatian, English, Greek, Macedonian, Romanian, Serbian, and Turkish.

[3] Natasa Radic, "Facebook has a friend in Southeast Europe," SETimes.com, March 8, 2010; http://www.setimes. com/cocoon/setimes/xhtml/en_GB/features/setimes/ articles/2010/03/08/reportage-01; accessed on October 1, 2012.

[4] View the SETimes' Facebook terms of usage at http:// www.facebook.com/SETimes#!/SETimes?v=info

[5] Leon Festinger, "A theory of social comparison processes," Human Relations vol. 7, no. 2 (1954): 117-140.

[6] Meagan Johnson and Larry Johnson, Generations, Inc.: From Boomers to Linksters—Managing the Friction Between Generations at Work (New York: AMACOM, 2010).

Table of Contents

US Military behind Africa News Websites

By Jason Straziuso, Associated Press, Nov 13, 2012

NAIROBI, Kenya (AP) — The website's headlines trumpet al-Shabab's imminent demise and describe an American jihadist fretting over insurgent infighting. At first glance it appears to be a sleek, Horn of Africa news site. But the site — sabahionline.com — is run by the U.S. military.

The site, and another one like it that centers on northwest Africa, is part of a propaganda effort by the U.S. military's Africa Command aimed at countering extremists in two of Africa's most dangerous regions — Somalia and the Maghreb.

Omar Faruk Osman, the secretary general of the National Union of Somali Journalists, said Sabahi is the first website he's seen devoted to countering the militants' message.

"We have seen portal services by al-Shabab for hate and for propaganda, for spreading violence. We are used to seeing that. In contrast we have not seen such news sites before. So it is something completely unique," Osman said.

But although he had noticed prominent articles on the site, which is advertising heavily on other websites, he had not realized it was bankrolled by U.S. military.

The U.S. military and State Department, a partner on the project, say the goal of the sites is to counter propaganda from extremists "by offering accurate, balanced and forward-looking coverage of developments in the region."

"The Internet is a big place, and we are one of many websites out there. Our site aims to provide a moderate voice in contrast to the numerous violent extremist websites," Africom, as the Stuttgart, Germany-based Africa Command is known, said in a written statement.

Al-Shabab and other militants have for years used websites to trade bomb-making skills, to show off gruesome attack videos and to recruit fighters. The U.S. funded websites — which are available in languages like Swahili, Arabic and Somali — rely on freelance writers in the region.

Recent headlines on sabahionline.com show a breadth of seemingly even-handed news. "Death toll in ambush on Kenyan police rises to 31," one headline said. "Ugandan commander visits troops in Somalia," another reads.

Web ads for the site appear on occasion on mainstream websites such as YouTube, and they show a clear anti-terror slant. Ads showing men on the ground blindfolded or Somalia's best known American jihadi, Omar Hammami, entice web users to click. They then access a headline like: "Somalis reject al-Zawahiri's call for violence," referring to the leader of al-Qaida.

The site, which launched in February, is slowly attracting readers. The military said that Sabahi averages about 4,000 unique visitors and up to 10,000 articles read per day. The site clearly says under the "About" section that it is run by the U.S. military, but many readers may not go to that link.

Abdirashid Hashi, a Somalia analyst for the International Crisis Group, said he has read articles on Sabahi, mostly because of advertisements on other Somali websites, but he also didn't realize it was funded by the U.S. He said he has no issues with the U.S. government running a news site.

"I don't think they hide it. That's up there. There's an information war going on, so I don't have any problem with that," Hashi said.

Osman said the articles on Sabahi are accurate and professional. But he said he feared that militants could attack writers who work for the site. Eighteen Somalis who work with media outlets have been killed this year, often in targeted killings.

Somali writers "can lose their life for working for this kind of a news outlet because of the extremists who target any critical voice or news service," Osman said. "The other issue is professionalism, because if someone is intimidated and is threatened all the time then he or she is reduced to self-censorship. He or she would be afraid if he files some important news that he would be targeted."

The military said there are nine writers who work for Sabahi from Kenya, Tanzania, Djibouti and Somalia. The other site — magharebia.com — concentrates on Libya, Algeria, Morocco and Mauritania.

Africom says the websites are part of a larger project that costs $3 million to pay for reporting, editing, translating, publishing, IT costs and overhead. It believes the project is paying dividends.

"The fact that we have seen an increase in website traffic is good news alone. The website's readers provide a significant number of comments on a regular basis, which often reflect their growing frustration and anger with extremist organizations in the region. Those comments are one indicator of a positive effect," Africom said.

Seth Jones, the associate director of the International Security and Defense Policy Center at the Rand Corporation think tank in Washington, said a significant part of the struggle with extremist groups like al-Shabab is ideological and is a battle for the hearts and minds of local populations.

"Based on this reality, the U.S. and other governments should be involved in countering extremist messages on websites and other forms of social media. After all, every Arab government provides substantial money to television, radio, print media, and Internet sites," Jones said.

"They key question for the United States is gauging whether locals view these kinds of news sites as legitimate sources of information and read them. If not, it's worth asking: Is the United States getting a bang for its buck?"

Table of Contents

Pentagon Propaganda Plan Is Source of Controversy

By Tom Vanden Brook, USA Today, 20 Nov 2012

WASHINGTON -- Senior officers at the Pentagon are being advised on countering Taliban propaganda by a marketing expert whose company once weeded out reporters who wrote negative stories in Afghanistan and helped the military deceive the enemy in Iraq, according to military documents and interviews.

Since 2000, the military has paid the Rendon Group more than $100million to help shape its communications strategy, analyze media coverage, run its propaganda programs and develop counternarcotics efforts around the world, Pentagon documents show.

One aspect of the company's work is aimed at changing attitudes of U.S. adversaries through messaging and advertising. Some Pentagon officials, including retired admiral Michael Mullen, former chairman of the Joint Chiefs of Staff, reject that, preferring instead to provide information and context about military operations.

John Rendon insists his company simply helps the military avoid mistakes in getting its message across to foreign audiences.

He offers advice "to people who face tough challenges and choices in a complex global information environment." A government watchdog found Rendon's access to Pentagon decision makers troubling.

"Rendon's previous work vetting journalists, performing public relations, and engaging in propaganda campaigns cause some concerns about the company's advice about changing the narrative in Afghanistan," said Scott Amey, lead counsel for the Project on Government Oversight. "However, in Washington, D.C., officials might be less concerned about objectivity or organizational conflicts of interest, and more interested in hearing what they want."

Mullen refused to use the term "strategic communication" and told USA TODAY in an interview shortly before he retired last year that he had no use for it.

"I really do not like the term at all. It confuses people," Mullen said. "It means all things to all people. It's way overused and way overrated. I literally try never to use the term. We communicate as much if not more by our actions. I have become particularly concerned at a time that resources are so precious. It has become a thing unto itself. It is taking resources from the fight. I don't have time for it."

On Oct. 12, Rendon appeared at the Pentagon at a forum to help the military "synchronize our strategic narrative and counter the Taliban's," according to an announcement about his appearance. It was an off-the-record event and included dozens of senior military officers and civilian officials. They gathered in a Pentagon conference room outfitted with large television screens to allow officials in Kabul, Pakistan and Tampa, home of U.S. Central Command, to take part.

The Joint Chiefs declined to name the officer or civilian responsible for inviting Rendon.

The Rendon Group has had a controversial history. Rendon also helped the Pentagon develop its policy on strategic communications, advising the Defense Science Board in 2001 that it needed to do more to shape public opinion. The firm was the subject of a Pentagon investigation into concerns raised in Congress that Rendon helped rally support for the 2003 invasion of Iraq. That investigation, by the Pentagon inspector general, found that Rendon employees had not done anything improper.

More recently, in 2009, John Rendon's contract in Afghanistan for strategic communication was severed by the military after it was learned that the company was weeding out reporters who might write negative stories.

Table of Contents

Panetta's Wrong About a Cyber 'Pearl Harbor'

By John Arquilla, Foreign Policy, 19 Nov 2012

In recent months, the specter of a looming cyber "Pearl Harbor" has reappeared -- the phrase having first come into use in the 1990s. But it is the wrong metaphor. Given the surefire emotional effect evoked by memories of the "day of infamy," how can this be? How are good cyber security legislation and regulations to be enacted and pursued in the absence of such galvanizing imagery? Clearly, the Obama administration thinks that trotting out the Pearl Harbor metaphor is essential, and so a range of officials, right up to Defense Secretary Leon Panetta, have been using it recently. But there is a fundamental problem: There is no "Battleship Row" in cyberspace.

In December 1941, a great deal of American naval power was concentrated at Pearl Harbor and Japan dealt it a sharp blow, enabling Imperial forces to pursue their expansionist aims for a while. Of the eight U.S. Navy battleships that were there, four were sunk and the other four were seriously damaged. And if the Kido Butai, the Japanese carrier strike force, had caught the three American aircraft carriers deployed to the Pacific in port -- they were out to sea at the time of the attack -- or had blown up the base's massive fuel storage tanks, the damage would have been catastrophic. Pearl Harbor was a true "single point of failure."

Nothing like this exists in cyberspace. Indeed, part of the logic behind the creation of the Internet, going back more than 40 years now, was to ensure continued communications even in the wake of a nuclear war. Redundancy and resilience are the key notions that shaped the structure of cyberspace. Yes, there are very important nodes here and there; but workarounds and fallbacks abound. Cyberspace is more like the oceans that cover two-thirds of the world: it has its choke points, but there are always alternate routes.

If the Pearl Harbor metaphor is misleading -- encouraging the belief that strong defenses concentrated in one or a few major areas can protect most, if not all, threatened spaces -- there may be another harbor metaphor that does much more good. This one comes from World War II as well and has to do with the harbor lights of the Eastern seaboard cities. Very soon after Germany declared war on the United States -- in the immediate aftermath of Pearl Harbor -- U-boats were dispatched to attack shipping on our side of the Atlantic. German submarine skippers were assisted in their task by the failure of President Franklin Delano Roosevelt to order a blackout along the coast. And so the U-boats had what their crews called "the happy time," teeing up targets for night attacks because they were illuminated against the backdrop of blazing city and harbor lights.

For several months in 1942, mayors of coastal cities resisted pressure to enforce blackouts because of the loss of business they feared would ensue, plunging an economy still not fully recovered from the Depression into a new downward spiral. It was only when shipping losses grew dangerously high -- over a million tons were sunk in the first four months of 1942 -- that a blackout was finally put in place and merchant ships began to move in escorted convoys. This didn't put an end to the U-boat menace, but did bring it under control.

Today, the "harbor lights" are on all over cyberspace. A wide range of targets is well illuminated, highly vulnerable to all manner of cyber mischief. Our armed services, increasingly dependent upon their connectivity, can be virtually crippled in the field by disruptive attacks on the infrastructure upon which they depend -- but which are not even government-owned. Leading commercial enterprises hemorrhage intellectual property to cyber snoops every day -- a point Governor Romney made twice in his debates with President Obama. And countless thousands of Americans, having had their personal security hacked, are now serving unwillingly and unknowingly as drones or zombies, pressed into service in the robot networks, or "botnets," of master hackers.

Why do the harbor lights remain on in cyberspace? Because, rather than focusing on security, information technology manufacturers and software developers have been driven for decades by market forces that impel them to seek greater speed and efficiency -- at the most competitive prices. In short, the virtual harbor lights stay on because the perceived economic cost of improved security -- that is, of enforcing a blackout, in metaphorical terms -- is seen as too high. And, just like FDR, American political leaders have shied away from forcing their hand.

Where the metaphor breaks down -- no metaphor can address every aspect of a problem -- is in its invisibility. Mass ship sinkings in the early months of 1942 were tangible events that horrified the nation. Today, the ongoing compromise of sensitive military information systems, the theft of intellectual property, and the recruitment of men, women, and children into zombie armies, all these pass largely beneath our levels of awareness. Cyberwarfare is a lot like Carl Sandburg's fog, coming in on "little cat feet."

To be sure, senior civil and military leaders know the gravity of the situation. A deeply alarming study of our cyber vulnerabilities by the National Academies was just declassified; it makes quite clear the grave nature of the threat. At the same time, word of a new presidential decision directive (PD-20) about responding aggressively to the cyber threat has leaked out. Reporting about the still-classified directive suggests that it follows the line of Secretary Panetta's comments in recent weeks about taking pre-emptive action against cyber threats.

All this implies clear awareness of the problem, but the pro-active recommendation to seek out and "attack the attackers" is problematic, given how well-hidden so many of them remain. Eleven years after the Code Red and Nimda computer viruses were unleashed -- shortly after 9/11 -- the identity of the perpetrators remains unknown. And this is true of many, perhaps most, cyber attacks. Digital warriors and terrorists today hide in the virtual ocean of cyberspace as well as U-boat skippers did during their "happy time" along the Atlantic seaboard 70 years ago. And efforts to track them in advance of their attacks, to hearken yet again to the harbor lights metaphor, will be as fruitless as the U.S. Navy's original strategy in 1942 of sending out hunter-killer squadrons to search the ocean for the U-boats.

Back then, the right answer from the start was to black out coastal cities at night. Then, when ships sailed, they were evasively routed and escorted by anti-submarine vessels. Losses still occurred, but soon fell to acceptable levels. This is the lesson of the "harbor lights" metaphor. In cyberspace, the analogous approach would consist of far greater use of strong encryption and "evasive routing" of data via the Cloud, making it much harder for the virtual U-boat wolf packs that stalk them to find their targets.

Forget Pearl Harbor. Remember the harbor lights.

Table of Contents

Why Is Israel Tweeting Airstrikes

By Max Fisher, Washington Post, 18 Nov 2012

Governments have always sought to manage public perception in wartime, but the Israel Defense Forces' steady stream of updates on Twitter, YouTube and Facebook since it began airstrikes on the Gaza Strip on Wednesday seems different. Unlike the usual media tactics — leaflets, state-sponsored radio, spokesmen — social media campaigns seek to incorporate themselves into the media we're already consuming, popping into our news feeds, implicitly seeking our participation. Or, in the case of the IDF campaign, sometimes explicitly.

The @IDFSpokesperson Twitter account, encouraging followers to show support for the strikes, tweeted Wednesday: "More than 12,000 rockets hit Israel in the past 12 years. RT if you think #Israel has the right to defend itself." More than 5,500 people have retweeted it. On Facebook, a flier-style image with a similar message has been shared 18,000 times.

But it's hard to measure whether the IDF's campaign is changing minds or just reinforcing existing ideological divides. When Egyptian activists launched a grass-roots social media campaign during the early 2011 Arab Spring protests that culminated in revolution, they used Facebook to organize and Twitter to attract the world's attention and, ultimately, its sympathy. The IDF is plenty organized without social media's help; its campaign has certainly attracted attention, but not necessarily the sort that will further Israel's interests.

An early tweet announced the targeted killing of a senior Hamas military commander, Ahmed al-Jabari, with a headshot, tinged blood-red, bearing bullet points of his terrorist acts and the word "eliminated" stamped in capital letters. As fighting escalated, the IDF tweeted, "We recommend that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead."

Most messages have chronicled Hamas's very real crimes, Israelis' suffering under their rockets and the IDF's strikes. The accounts have mentioned Gazan civilians, though typically alongside reminders that the IDF has dropped fliers warning them to "take responsibility for yourselves and avoid being present in the vicinity of Hamas operatives and facilities."

The campaign has elicited a strong reaction. A significant number of Israelis and Americans (whom one IDF tweet addressed directly) have retweeted, liked, shared and otherwise shown their support for the Israeli military operation, dubbed Pillar of Defense.

Skeptics, particularly in the Arab countries surrounding Israel, have seemed to consider thet weets and posts overly triumphant or insensitive. The IDF's campaign became a heated topic in the larger social media discussion of the military operation. Its official #Pillar Of Defense hashtag has attracted a small fraction of the discussion linked to the Gaza-sympathetic hashtag #Gaza Under Attack.

Hussein Ibish, a D.C.-based senior fellow at the American Task Force on Palestine, tweeted, "This is extremely damning: IDF cheerily live-tweets infanticide." (By the end of the week, the death toll in Gaza had reached 21, including a young child.)

The criticism has not been limited to Middle Easterners. Irish Twitter account @Ard_Macha said of the social media push, "Probably more disturbing than the attack on Gaza is the apparent glee with which the IDF carries out its job."

A polished, edgy campaign can't overturn actual public opinion, which still rules social media. But it can remind people of what they already think, giving them an opportunity to sound off for or against, and to dig up the debates they've been having for years. Like a spree of attack ads in a political campaign, the effect has been polarizing — deepening divides that were already problematic for Israel.

Public opposition to Israel's Gaza policies was already high in neighboring Egypt, for example, where a newly democratic, Muslim Brotherhood-allied government will have to decide how to respond. An attention-grabbing, feather-ruffling campaign risks further inflaming a public opinion that suddenly matters for Egypt's decision-makers in a way that it didn't under Hosni Mubarak's reliably pro-Israel dictatorship.

President Mohamed Morsi isn't going to unilaterally withdraw from the Camp David Accords over a few tweets, but the less pressure he feels from antiIsraeli activists and Muslim Brotherhood factions, the better Israel is likely to be served.

That's the problem with social media. Once you start feeding it posts and images, users can send them swirling just about anywhere. You might think you're just talking to your friends, but you don't really control the conversation, which can take on a breadth and significance you hadn't intended.

Table of Contents

Psychological Warfare on the Digital Battlefield

By Anshel Pfeffer, Haaretz, Nov.19, 2012

Israel's campaign against Hamas in the Gaza Strip is being conducted in the air as well as over the airwaves. But on this front, the Palestinians are fighting with at least one hand tied behind their backs.

There has been no other case in the history of modern warfare where one side controls all the communication infrastructure of the other, as is the case here. All of Gaza's telephone networks and internet servers go through Israel; every phone conversation and email is rooted through Israeli territory and from there sent on through underwater fiber-optic cables to the rest of the world.

Israel hasn't cut Gazans off, technologically, from the outside world for a number of reasons. The official one is to not cause unnecessary harm to the civilian population. Beyond that, the security establishment doesn't want to relinquish the intelligence opportunities from having access to Gaza's communications. Plus, there's the PR consideration to not create a media blackout which would allow rumors of a humanitarian crisis to percolate.

The control over the telephone networks also allows the IDF to issue warnings to specific homes which, according to intelligence, are being used to store arms or serve as local Hamas command posts. Civilians in these homes are called and warned that they are about to be bombed and should leave immediately. From reports in Gaza, these phone-calls were specific and much more focused than in Operation Cast Lead four years ago, when nearly all the civilians in Gaza received phone-calls giving them a general warning not to be caught near Hamas facilities and the firing zone.

The networks in Gaza are managed through the Palestinian Authority's Telecommunications Ministry along with the Israeli Defense Ministry's Coordinator of Government Activities in the Territories and includes allocations of wavelengths to mobile phone operators, radio and television stations. On Sunday, Israel burst into broadcasts of Gazan television and radio, broadcasting warnings in Arabic to residents to avoid Hamas bases and the border area. These interruptions were an addition to the hundreds of thousands leaflets containing similar warnings released from fighter-jets.

"We are busy all the time with psychological warfare of this kind," said a security source who would not add details. This warfare is carried out by the IDF's Intelligence branch which receives information from COGAT and the Shin Bet. The IDF doesn't usually divulge details on psychological warfare that is conducted along with the more open and official media activity.

Security officials insist that there was no intention at any stage to close down Gaza's communication lines, which also remained open during Operation Cast Lead when the blockade on Gaza was much more solid than it is today. Despite this, the international hackers collective Anonymous justified a concerted attack on Israeli websites over the weekend by citing an alleged threat to do so.

No official Israeli spokesman has made such a threat, though Foreign Minister Avigdor Lieberman has advocated a number of times over the last few years that Israel should have a "second disengagement" from Gaza, shutting down all border crossings and cutting off all commercial ties, including also communications infrastructure. Lieberman's ministry was one of the main targets of the hacker attacks. Anonymous claimed to have "wiped out" the Foreign Ministry's database. In reality, the ministry's website was down for a short time from a type of cyber attack that swamps and disables a website but according to ministry sources, "the claim to have wiped out our database is as accurate as Hamas saying it hit the Knesset with a missile."

The directors of the government connectivity unit said today that since the start of the operation in Gaza, there were 44 million cyber attacks on government and security services websites. A few sites went briefly offline but no damage was caused.

The internet is the battlefield of much of the psychological warfare against Israel. Most is even less effective than the cyber attacks. The warfare is mainly in the form of false emails and facebook postings. Over the last few days, many Israelis received a false announcement from "IDF Spokesman" warning them against opening text messages because "when you open the message, terrorists in Gaza can track you and direct their Katyushas to your location!"

At the same time, thousands received emails from one "Moshe Rotoor," using a Russian account, who claims in broken Hebrew that "the military censorship of military intelligence is hiding the information about the attacks on our soldiers on the border of Gaza. See the picture of the field of death in which our soldiers are falling in Gaza." YouTube videos enclosed in the email claim to show an IDF jeep hit by an anti-tank missile. In reality it is a jeep belonging to the Reuters news agency that was hit on the border on Friday.

On the web someone who claims to belong to the Al-Qassam Battalions claims to be holding the personal details of 5,000 "Israeli officers" and to have hacked their mobile phones. He threatens to disclose their details online over the next few days. The source of these threats and "reports" is not clear.

"We don't see this as a serious threat," says a security source. "It hasn't fooled people or caused panic."

Gal Ilan, the spokesperson of the Information Ministry is slightly more concerned. "It is happening from a lot of direction. There are entire groups attacking Facebook pages with swastikas. We have mobilized many civil PR resources with volunteers at the ministry and universities and the Jewish community in New York."

The civil and military media operations are pleased with the online responses to their efforts to support the military operation on social networks through footage of IDF strikes and videos such as "the ten lies of Hamas," but there are reservations.

Senior officials in the government PR operation demanded that the IDF Spokesman tone down the boisterous tweets on the IDF official Twitter account. Complaints came over some of the more exuberant "bumper sticker" tweets including the one featuring assassinated Hamas military chief Ahmad Jabari with the word "ELIMINATED" written over his face, and a photograph of a destroyed Gaza home accompanied by the caption, "Would you raise your child in this neighborhood?" After a senior IDF Spokesman officer stepped in, the tweets over the last few days have been more sober.

Table of Contents

Testing Novel Effects of Ad Redesign on Customer Willingness to Pay

By Steven G. Shenouda, Ph.D., MBA Class of 2013, MIT | Sloan School of Management

Consumer behavior is an immense field. Customer willingness to pay and vendor ability to influence willingness to pay are important notions in marketing. Causal factors are beginning to be better understood in different literatures, from psychology to neuroscience. The literature reviewed in section 2 suggests that we can understand and influence willingness to pay. Section 3 presents the details of the present study, designed and executed to help fill the gap in the knowledge about practical implementation of influencing willingness to pay through robust mechanisms. Section 4 presents the results. Specifically, Chi Square tests were computed to examine the differences in willingness to pay for treatment and control groups for a national sample of 242 male and female participants. Additionally, demand curves and price elasticities were computed to assess relative strengths of any effects. Finally, a summary of the rationale, method, and results are presented in section 5. General implications of the results are presented. Possible future studies are proposed and limitations to the present study are discussed.

shenouda_mkt15052012.pdf

Table of Contents

Taipei’s Cyberwarfare Gambit

By Paul Nash, Diplomatic Courier, 28 November 2012

When it comes to questions of territorial sovereignty, Taiwan has never been shy about making bold, even antagonistic accusations against the Chinese mainland. Cyber territory is no exception. According to a report lately published by Taiwan’s National Security Bureau, the PRC is behind a growing number of cyberintrusions targeting its government and corporate networks—more than a million during the first half of this year alone.

To many, the accusations are not surprising. It is well known that China has been aggressively evolving its Integrated Network Electronic Warfare strategy for over a decade now. The People’s Liberation Army (PLA) created a sizable cyberwarfare unit in the mid 1990s. Since then, it has purportedly used computer hacking and viruses to target political, economic and military assets in Taiwan and a host of other countries, including the United States. A report prepared for the U.S.-China Security Review Commission by Northrop Grumman claims that Chinese state-affiliated and state-sponsored entities appear to be responsible for a growing number of cyberintrusions in the United States. According to the defense contractor, numerous intrusions seem to be probing for vulnerabilities in America’s telecommunications supply chain and critical infrastructure systems.

Taiwan’s Ministry of National Defense has taken note. While making deep cuts to other programs, it has proposed a plan in its 2013 budget recommendation, sent to the Legislative Yuan for approval, that would see its information warfare strategy expanded over the next five years. The plan calls for the Communication Electronics and Information Bureau to be augmented by a new special task force able to prevent and control malicious attacks on military and civilian networks. The task force would be set up and trained in an experimental facility that simulates cyberattacks on the nation’s critical infrastructure: its electrical power grid, natural gas and petroleum pipelines, nuclear power facilities, water treatment plants, railways, and highways.

It remains unclear to what extent the PLA or ministries of the Chinese government are behind the rising incidents of hacking in Taiwan and other countries. The U.S. National Counterintelligence Executive says that “Chinese actors are the world’s most active and persistent perpetrators of economic espionage” via the internet, and that the U.S. has been subjected to an “onslaught of computer network intrusions that have originated in China.” Google, Lockheed, DuPont, and several major multinational oil companies believe they have fallen victim to Chinese hacking and lost valuable technological, scientific, and trade secrets as a result.

But much of the evidence implicating the Chinese government—the evidence made public, at least—remains circumstantial. Establishing linkages between network intrusions and a Chinese state-sanctioned directive is difficult, even when intrusions are detected and monitored. Identifying a perpetrator is becoming more elusive with the proliferation of civilian hacker groups in China, the world’s biggest cybercommunity, and also with the advent of increasingly sophisticated portable IT devices that make it harder to pinpoint the source of an attack. In 2009, researchers from the Munk Institute in Toronto, Canada, released a report in which they claim to have discovered a large-scale international hacking operation with apparent—though not conclusive—connections to PLA command and control. Beijing denies any involvement, calling such accusations unfounded and attributing China-based cyberattacks to civilian “hacktivists” or American propaganda.

Industrial cyberespionage, of course, is not the same thing as cyberwarfare. Nevertheless, observers feel that China’s movements on this field are a good gauge of its cyberwarfare capabilities and intentions. Not only do the two share similar technical foundations, but China seems to have decidedly integrated cyberwarfare into its economic development program. Economic development is itself considered a key component in the PRC’s longer-term national defense strategy, a deterrent to foreign encroachment on its territorial claims and global economic interests, as well as a way to legitimize and sustain one-party rule.

Taiwan’s cyberwarfare plan follows in the footsteps of additional funding that the U.S. has earmarked for military, intelligence, and homeland security programs set up to counter a perceived threat from China. It is also part of a broader push to modernize Taiwan’s military by enhancing asymmetrical warfare capabilities. These capabilities include improved all-frequency electronic detection, mobile land-based long-range surface-to-surface and ballistic missiles redesigned for enhanced precision, and a new generation of attack helicopters for littoral and beachhead defense. They also include multi-functional unmanned aerial vehicles (UAV) built in response to China’s new Yilong UAV, which the PLA claims is superior to the U.S. Predator. Taiwan flew a drone aircraft for the first time earlier this year on the Hualien coast during an electronic warfare exercise.

Taiwan’s foray into cyberwarfare is meant to alter the risk calculus of any future conventional cross-Strait conflict. When Taiwan announced in 1999 that it had established a committee to examine the concept of information warfare, some four years after Beijing deployed its cyber task force, it stated that it would not use cyberattack capabilities to initiate an offensive. These capabilities would serve only as a balance-of-power deterrent, conceptualized (too optimistically, perhaps) within the doctrinal framework of something akin to mutually assured destruction.

The thinking among military strategists in Beijing is quite different. Some see a cyberattack against the “renegade province” as a potential instrument of precipitating a national crisis in Taiwan that would open up an opportunity to prosecute a more efficient invasion using conventional forces, thereby bringing about the island’s political reunification with the mainland.

It remains to be seen how Taiwan’s cyberwarfare gambit might affect political and economic relations with the PRC. Members of Taiwan’s opposition Democratic Progressive Party are drawing political capital from the National Security Bureau’s report already, claiming it proves that Beijing is actively preparing for a military strike. But Beijing’s relations with Taipei have stabilized somewhat since Ma Ying-jeou of the Kuomintang party came to power in 2008 on a platform of improving trade, investment, and tourism with the mainland. Ma’s re-election in January for a second four-year term suggests that the Taiwanese electorate presently has a diminished desire to see its government take a politically provocative stance towards China.

Taiwan, of course, may have to reconsider opening up core telecommunications services to investment from the mainland in light of this damning report. Ironically, however, it makes little difference whether or not legislators in Taipei entertain the question of integrating cyberwarfare into the nation’s overall strategy of information warfare. The initiation of public debate on the issue has already, unintentionally or by design, made it part of Taiwan’s information warfare campaign.

Table of Contents