

INFORMATION OPERATIONS NEWSLETTER



Compiled by: [Mr. Jeff Harley](#)
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 OSS.NET](#)

[ARSTRAT IO NEWSLETTER AT JOINT TRAINING INTEGRATION GROUP FOR INFORMATION OPERATIONS \(JTIG-IO\) -
INFORMATION OPERATIONS \(IO\) TRAINING PORTAL](#)

TABLE OF CONTENTS

VOL. 12, NO. 03 (DECEMBER 2011/JANUARY 2012)

1. [9th Annual Army Global Information Operations Conference](#)
2. [A Speed Bump for Pentagon's Information Ops](#)
3. [Special Forces Get Social in New Psychological Operation Plan](#)
4. [Hazards of Perception Management](#)
5. [Does Social Media Help or Hurt Terrorism?](#)
6. [All Quiet on the Western Front](#)
7. [Who sent a false text message saying cash benefits will no longer be paid to Iranians?](#)
8. [Cyberspat Erupts As Baku-Tehran Relations Become Increasingly Strained](#)
9. [SPAWAR Recognizes Space Cadre at Information Dominance Warfare Officer Pinning Ceremony](#)
10. [In the Middle East, Cyberattacks Are Flavored with Political Rhetoric](#)
11. [SCADA Systems in Railways Vulnerable to Attack](#)
12. [Twitter Able To Censor Tweets in Individual Countries](#)
13. [Taliban Folklore in Pakistani Media](#)
14. [Iran Mounts New Web Crackdown](#)
15. [Call For Cyberwar 'Peacekeepers'](#)
16. [The Strategic Communication of Unmanned Warfare](#)
17. [57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report](#)
18. [In Battle for Hearts And Minds, Taliban Turn To CDs](#)
19. [Can U.S. Deter Cyber War?](#)
20. [Supremacy in cyberspace: Obama's 'Star Wars'?](#)
21. [Chinese Tech Giant Aids Iran](#)
22. [China Likely to Go Asymmetric if Conflict Breaks out with United States](#)

9th Annual Army Global Information Operations Conference

The US Army Space and Missile Defense Command/Army Forces Strategic Command (USASMDC/ARSTRAT) G-39 will be hosting the 9th annual Army Global Information Conference 16-20 April 2012 at Peterson AFB, CO. This conference provides a forum for the IO community of professionals, including Army, Joint and interagency, to improve Army operational support to USSTRATCOM and Combatant Commands. The objectives for this conference are:

- Discuss full-spectrum Information Operations activities in support of USSTRATCOM and other Combatant Commands.
- Inform the IO community of interest of current operational best practices, lessons learned, and tactics, techniques and procedures.
- Address the integration of traditional and emerging IO doctrine and practice, components, enablers and organization of the Mission Command Warfighting Function.
- Discuss Army IO way ahead: doctrine, resources, structure and capabilities.

Points of contact are Scott Janzen, 719-554-6421, scott.janzen@us.army.mil; and Mr. Jose Carrington, 719-554-8880, jose.carrington@us.army.mil.

[Table of Contents](#)

A Speed Bump for Pentagon's Information Ops

By Walter Pincus, [Washington Post](#), 12/06/2011

The Pentagon may have hit a speed bump in the expansion of its growing worldwide information operations.

The Senate Armed Services Committee has asked Defense Secretary Leon Panetta to assess the effectiveness of a series of news and information Web sites that have been initiated by U.S. Special Operations Command (SOCOM) in recent years in a bid to counter extremist messaging. The so-called "influence Web sites" are maintained by various overseas commands and operated by defense contractors.

For fiscal 2012, SOCOM sought \$22.6 million in the Overseas Contingency Operations account — primarily intended to fund the wars in Afghanistan and Iraq — for the initiative.

Congress, over the past few years, has been pressing the Pentagon to justify the hundreds of millions of dollars spent overseas under various headings such as "strategic communications" and "information operations."

In the latest challenge, the Senate Armed Services Committee noted in a legislative report that information ops Web sites "have become a significant and costly component" of U.S. military commands' campaigns to counter violent extremism, "despite there being limited information to demonstrate ... [they] are reaching or appropriately influencing their intended target audience in support of U.S. national security objectives."

Among the Web sites are Magharebia, which covers North Africa and is operated under U.S. Africa Command; Central Asia Online, under U.S. Central Command, which covers countries such as Uzbekistan, Kyrgyzstan, and Kazakhstan; and the Southeast European Times, under U.S. European Command, which covers the Balkans, Greece and Turkey.

While the committee said it supports the objectives of the program, it wants more specifics — including a determination on whether the sites are reaching audiences in areas where Internet access is "readily available" and where "U.S. national security interests are of immediate concern."

For now, the panel recommended cutting the funds by 50 percent, to \$11.3 million, and then holding that amount until Panetta certifies the effectiveness of the program. The recommendation was made as part of the fiscal 2012 defense authorization legislation, which was recently passed by the Senate but that may draw a veto from the administration.

[Table of Contents](#)

Special Forces Get Social in New Psychological Operation Plan

By Noah Shachtman, [Wired](#), January 20, 2012

The elite forces of the U.S. military think they've found a new way to sway opinion in the Pentagon's preferred directions: a voice-based social networking app that's a cross between talk radio and Twitter.

The American intelligence and defense communities have become enthralled by the possibilities of social media. They're looking to use the networks to forecast political unrest, spread friendly messages, spot emerging terror groups — and even predict the next natural disaster. But these efforts have generally tried to leverage existing, and already popular, civilian social networks.

A new project from U.S. Special Operations Command, on the other hand, looks to create something brand new: a "user-generated social media radio application powered by the human voice, available on the PC, Mac, Android, iPhone, and Nokia smart phones, that lets users share their thoughts and experiences." And this voice-activated SOCOM network is being billed explicitly as a tool for "military information support operations" — shaping public attitudes. That's what the Pentagon used to call "psychological operations."

Earlier this month, SOCOM released its wishlist for technologies it would like in the new year. Items included chemical dyes to track the unsuspecting; hackers' tools for "data infiltration and exfiltration"; and heap of gadgets to move hearts and minds — including this social media app.

"The command is investigating ideas and technologies that can replace traditional methods of information dissemination like face-to-face or handing out leaflets," SOCOM spokesperson Col. Edward "Tim" Nye tells Danger Room. "We are looking at ways to get instantaneous feedback from television and radio broadcasts in a virtual world. We are looking for ways to allow audiences to comment or interact with the U.S. government in an environment that ranges from limited individual engagement to a much larger audience. We are soliciting ideas that capitalize on the innovative technologies that incorporate the newest dissemination methods through computers and smart phones."

When asked if people should trust this app, given that's its a tool for psychological operators, Nye answered, "That question of trust is no different for this potential dissemination method than any other dissemination method."

On the network — which SOCOM sees as almost as a friends-enabled, military-grade Shoutcast — "users should be able to make their own long-form radio shows, by dialing in with a free phone number. This should allow a person's interest in sports, music, news, culture to be aired. Users are to be kept entertained while sharing the things that matter to them the most."

"A cellular device should serve as a broadcast tower, a DJ/moderator booth, and a radio receiver," the SOCOM call request for proposals adds. "Individuals can host their own call-in show using industry best practices or just listen in to others expressing their opinions freely without the fear of traceability. Participants must feel the available content is powerful, addictive, informative, and capturing social experience through their collective insight, passion, and involvement."

SOCOM was unable to respond for calls to comment on this story. But, in some ways, the command appears to be following the lead of the U.S. State Department, which years ago declared that "the very existence of social networks is a net good" — and distributed tools to promote the existence of those networks. The idea was that open communication would inevitably lead to more democratic sentiment, which would inevitably redound to America's benefit. (Theorists like Evgeny Morozov, in contrast, have argued digital communication is easier to track and trace — which makes the networks ideal tools for social control.)

And since America's special operations forces tend to work in parts of the world where the technological infrastructure is the most threadbare, SOCOM is looking to buy up a heap of "air-droppable scatterable electronic media" that it can litter over a remote battlefield. Those gadgets include "AM/FM broadcast transmitters; miniaturized loudspeakers; entertainment devices; game device technologies; [and] greeting cards."

That's right, greeting cards. American military's psychological operators may be looking at new ways to persuade. But that doesn't mean they're giving up the tried and true.

[Table of Contents](#)

Hazards of Perception Management

By Momin Iftikhar, [The Nation \(Pakistan\)](#), January 23, 2012

As the US contemplates its moves to make a clean break and leave behind the quagmire of Afghanistan in a manageable state, the issue of perception management has begun to register a sharp rise on the scale of its vital priorities. Despite the blood of thousands of innocent civilians on their hands [call it collateral damage, if you please] the Americans remain steadfastly committed to burnish the perception of their benign image and moral authority, defined by an overwhelming respect for human rights, universal compassion and love for humanity. This is easier said than done and a recent video, gone viral on the internet, showing four US marines desecrating the dead bodies of Taliban explains the US dilemma as to why despite investing heavily

into the business of positive perception management, the Americans find themselves a much reviled nation. Nowhere is this exercise in diminishing returns more evident than in Afghanistan and Pakistan where despite considerable US investment to turn the tide of an abysmal anti-US public opinion, the results reflect a resounding failure.

Information Operations, which encompass the cultivation of a positive image for the US damage intensive and disproportionate application of firepower, are since 90s, a part of the official American military treatise. This innovative doctrine harnesses the phenomenal advances in information and communication technologies and integrates their tentacles into an overall military strategy; primed not only to achieve unchallenged military supremacy, but also to win an unassailable moral high ground by winning the battle of hearts and minds in and around the devastated theatre of operations. In a nutshell, the ultimate objective is not only to win militarily, but also convincingly win the propaganda war. Conceptually, this idea is seamless, but when exposed to the fog of war and the ground realities, presents a true dilemma for the US military, CIA and State Department strategists, who at best are not working in tandem, but at worst seem to be pulling away at cross purposes.

An image is worth a thousand words and a video with the cast of genuine characters spells out a credibility and authenticity that spin doctors find difficult, if not impossible, to handle. Technically, it is extremely easy to make a live video and uplink to internet - a process that is beyond the best military or civil censorship regime to preclude or predict. This means that the inhumanity ingrained in the ruthlessness of US operations can no longer be concealed and ultimately adds up to neutralise the impact of information warfare segment of the operations seeking a positive projection of its military. In such an environment, frequent surfacing of offensive videos [urinating marines - Afghanistan] and images [Abu Ghraib - Iraq] exponentially add to latent fires of anti-American hostility and backlash towards the US operations and forces.

The paradox emerges because the US military operations are increasingly getting on a tangent to the professed strategy for winning the battle for hearts and minds. As made evident by the "urinating episode", it seems that the US officers and men have little, if any, comprehension of local traditions, despite senior commanders making much fuss about their understanding of local customs enshrined in the Pakhtunwali. Nor the military chain of command seems to be particularly keen to drill the necessity of discipline and the need to show respect for the enemy dead; part of the honour code of fighting men the world over. One wonders as to what kind of perception management will be needed to heal the wounds to the Pashtun pride caused by the senseless conduct of the marines, who seemed to have been left to themselves by the chain of command in satiating their animal instincts. Similarly, what kind of respect and cooperation would be forthcoming to the US military from Pakistan whose loss of scores of its sons on the Salalah ridge has not elicited a corresponding response of guilt and remorse from the Obama administration or the military, who have even failed to share the contents of the inquiry into the lamentable event.

Acutely aware that despite widespread operations for reaching the hearts and minds of the Pakistani public and intelligentsia, its desired objectives to soften up the American image remain elusive; the CIA run perception building operations have acquired a new urgency. The footprints of this ambitious campaign are clearly visible in the fields of education, agriculture and social welfare projects. The USAID logo is sprouting all over like wild shrubs in monsoons in the Pakistani landscape, yet the American effort remains most noticeable by its concerted attempts to make ingress in the dynamic and evolving realm of Pakistani media.

The attempted penetration of all genres of local media mediums by the US financed journalism is developing dangerous trajectories of its own. If Information warfare has become a veritable implement of the US military and CIA run strategy, causing death and destruction among the militants' ranks and the local population without distinction, then individuals serving and promoting the US cause in the local media are bound to become a pawn in the insurgents' crossfire in the battle for winning perceptions.

The recent and deplorable assassination of Mukarram Khan Atif in a Shabqadar Mosque by Taliban militants is indicative of the perils faced by the local journalists, who are lured in by attractions of the American financed media services. It was the first death of a journalist in Pakistan, which was claimed by a militant group. According to the New York Times, Atif worked for Deewa Radio, a voice of America service that was set up in 2006 for making Pashto broadcast into the FATA region. The radio has an annual budget of \$1 million with about 25 local employees for whom the salaries are lucrative, considering the meagreness of local standards. Apart from Deewa, there is Radio Mashaal, also financed by the US and the BBC Pashto Service that keep spreading the message of their respective governments into a sensitive area where drone attacks are a routine and xenophobia rampant.

Atif's tragic killing has underscored the perils caused to the media men by their fatal attraction to the lure of American-sponsored journalism, which according to the US doctrine is closely perceived to be linked to its military objectives in the region. His death calls for a serious introspection on part of the American planners of

the battle for hearts and mind, who are putting scores of Pakistani journalists in the harm's way by recruiting them to inadvertently play a role in the US-led battle for a positive perception management in FATA and elsewhere.

[Table of Contents](#)

Does Social Media Help or Hurt Terrorism?

From [Voice of America](#), 21 January 2012

The recent headlines were enough to concern even the most cynical reader. "Terrorist groups recruiting through social media," blared the headline at the [CBC's website](#). "Social Media Gave Terrorist Groups Second Wind," read the report at [pixelsandpolicy.com](#). "Terrorists making 'friends' on Facebook," topped the [Digital Journal](#) story, underscored by an image of a masked person brandishing an automatic weapon.

Why all the alarm? It turns out these and many similar stories were all prompted by a new study by University of Haifa communications professor Gabriel Weimann. In it, Wiemann asserts that "...90% of terrorist activity on the Internet takes place using social networking tools," a claim also previously made by researcher Evan Kholmann. That terrorists were using the Internet took no one by surprise; that nearly all of their activity takes place in the relative open of social networking did.

"As we know from marketing, there's a distinction between push and pull," Dr. Weimann tells us:

"The pull strategy means you wait in your store and wait for the customers to come, and the push strategy means that you start pushing your product to the customers by knocking on their doors. When it comes to terrorism online, they used to apply a pull strategy; waiting in chat rooms for supporters, interested people, and members of the group to join in. Today, using the social networks, they can actually come to you. That is, using the social nature of Facebook, a page opens to another page, and so on. Friends and friends of friends, like widening circles, all become a huge social web. They can use all that by getting only the first to post the messages they want."

In Weimann's view, terror groups have three goals for using the web: communication, coordination, and recruitment. And it's this last goal – finding new members willing to take arms for their cause – that causes him the most alarm.

"If you're a student, or you're a journalist preparing an article related to a terrorist group, and you use Google search in a very naive way, you may very likely hit on a website which was posted or created by terrorists, without even knowing it. If you're an alienated Arab or Muslim living in Europe or North America, and you're just looking for companion, someone who shares your loneliness and you're looking for social bonding, you may end up with terrorists online without even knowing it. This spread of online propaganda is done in a very smart, concealed way so that sometimes very naive populations may be seduced and tempted."

"That is not a well-founded fear," counters Dr. William McCants, a Middle East and terror researcher at the Center for Naval Analysis (CNA) outside Washington. "The most they've been able to do is perhaps steal some credit cards and blackmail some people, which would definitely be a concern, but it's not as if they're going to shut down a power grid anytime soon," he says. "It's really a coordination tool, and much less a recruitment tool."

McCants readily admits that terror groups are trying to use the web for propaganda purposes. The problem, he says, is that they're just not reaching their target audience.

"If you look at the (the Somali Islamist group) Shabab's Twitter feed, most of their followers are DC area analysts. They're not youth that are interested in the movement. We haven't seen the numbers that would substantiate people saying there are wide swathes of youth who are joining up as a result of reading propaganda online. The numbers of recruits are quite small, estimates both by militants aligned by Al Qaeda and by outside researchers (are) that only .00001 % of people who look at propaganda actually decide to take up arms on behalf of Al Qaeda. That's a vanishingly small number."

So are terrorists winning or losing their wars in the social networking realm? Many researchers say that's simply the wrong question. "Terrorists use the Internet just like anyone else. They use it to communicate, to share ideas, to share tactics and seek out new followers," says McCants. "I think the Internet is particularly effective for finding like-minded people and coordinating with them. But I am very skeptical about its utility in generating new recruits."

Former CIA case officer, and now author, Marc Sageman, sees a landscape composed of fewer disciplined organizations like al Qaida, and more "self-recruited wannabees (hopefuls)" operating alone with only one or two other trusted associates. These solo actors may then likely turn to the Internet primarily for information:

how to construct bombs, monitor security force movements or other tactics honed by jihadists in Afghanistan and Iraq. But this would only happen once the individual had decided on a terrorist course.

Researcher Kholmamn, however, sees the web becoming an ever more potent tool for “soft” psychological warfare – militants boasting of accomplishments and creating the aura of a successful group that others may want to join. For example, while he was alive, American cleric Anwar Al-Awlaki preached heated inducements to jihad from his base in Yemen. His sermons were fiery, exciting, and in English, the language of Colleen LaRose of Pennsburg, Pennsylvania. In time, Colleen became infamous by her new adopted character “Jihad Jane,” and was eventually charged with conspiracy to commit murder and support of terrorists.

It’s those stories, even as few as there are now, that Gabriel Weimann focuses on.

“We have to react. We can’t leave the stage open to the bad guys. There are many ways to fight back but first of all we must be aware of it. We must be aware that online we are now fighting a new type of terrorism. It’s a new type of arena, a new type of war in cyber-space. For this type of war we need a new type of soldiers and weapons. It’s not tanks and it’s not explosives and airplanes and so on. What we need are experienced people who can...either block access to those websites, and can penetrate social networks and post alternative messages and try to compete with the terrorist scenarios of doom, death and destruction with a message of hope, peace and togetherness.”

But CNA’s William McCants says it’s less about war and weapons, and more about understanding the limitations of the Internet:

“I think those terms are the wrong way to think about it. They are not using the Internet as a weapon, that just has not been borne out anywhere. The most they’ve been able to do is perhaps steal some credit cards and blackmail some people, which would definitely be a concern, but it’s not as if they’re going to shut down a power grid anytime soon. It’s really a coordination tool, and much less a recruitment tool.”

Whatever the most accurate view, it’s a fair bet that as long as we have terrorists operating in the real world, they will find their way to cyber-space as well.

[Table of Contents](#)

All Quiet on the Western Front

2012 Challenges and Opportunities in the Five-Year Strategic Plan for U.S. International Broadcasting

By Alan L. Heil Jr., [American Diplomacy](#), December 2011

As the Voice of America marks its 70th anniversary, what lies ahead for all of the world’s publicly-funded overseas networks in the year ahead? For Western broadcasters collectively, 2011 was the most potentially devastating year in more than eight decades on the air. Now, because of fiscal uncertainties in their host countries and rapidly evolving competition from both traditional and new media, they face huge cuts in airtime and operations. Can America step up to help fill the gap? A new strategic plan for U.S.-funded overseas broadcasting charts a possible path.

Over the years, the government networks in Europe and North America have offered a window on the world and a beacon of hope for hundreds of millions of information-denied or impoverished people on the planet. They have done so by offering accurate, in-depth, credible news, ideas, educational and cultural fare, consistent with Western journalistic norms and the free flow of information enshrined in the 1948 U.N. Declaration of Human Rights. The broadcasts have enhanced America’s security, and even saved lives. They helped foster a largely peaceful end to the Cold War.

Consider, then, the events of the year past:

---The BBC World Service, because of resource cuts, has lost five language services (Albanian, English to the Caribbean, Macedonian, Portuguese to Africa and Serbian). Seven more services, including Mandarin Chinese, Russian and Spanish to Cuba, have ended all radio programming, focusing instead, as appropriate, on mobile, television and on-line content and distribution. Over the next five years, World Service projections are a loss of 30 million of its 180 million radio listeners and a reduction of about a quarter of its professional staff. This is the result of a cut in grant-in-aid funding by the United Kingdom’s Foreign and Commonwealth Office.

---Germany’s Deutsche Welle (DW) is also facing substantial reductions. DW discontinued shortwave radio broadcasts in German, Indonesian, Persian and Russian. Chinese will be halved from two hours to an hour daily. As 2012 dawned, Deutsche Welle scheduled reductions in its shortwave broadcasts from 260 to 55 hours each day. It remains on the air on shortwave in English only to Africa.

---Radio Netherlands Worldwide (RNW) is an award-winning network distinguished for its documentary and in-depth cultural and public service broadcasting in English and other languages. But now, RNW funding is being

cut 80 percent, effectively silencing one of the West's most attractive voices of reason to audiences everywhere.

---France's overseas services, Radio France Internationale (RFI), France 24, and TV5, also are in the throes of an existential crisis. RFI and France 24 merger action has resulted in protest demonstrations by staff members affected. Finance ministry auditors in Paris have recommended ending all shortwave and AM radio programming of RFI worldwide to save money. Beginning January 1, shortwave is due to be cut from 102 to 60 hours daily after talks between RFI and TDF, the agency that has managed transmissions for RFI.

---The Voice of America ended its broadcasts in Croatia last November 23. Earlier in the year, the Voice's oversight Broadcasting Board of Governors (BBG) had announced plans to abolish ten hours daily of VOA Chinese Mandarin shortwave broadcasts and an hour daily of TV as well as the Cantonese Service, while investing more in VOA new media services to the PRC. But that decision was wisely modified in the wake of the Arab awakening and expressions of Congressional concern. VOA Director David Ensor and BBG member Victor Ashe recently informed their Chinese Branch colleagues of a commitment to retain a multimedia VOA service to the PRC. Earlier reports were that they would retain some radio and double their TV programming to two hours a day to enter the growing satellite TV market in the PRC. New multimedia tools, such as a VOA Chinese language iPhone app, also are being developed.

Until a few months ago, the West's publicly-funded international broadcasters --- including those of the United States --- together reached at least a third of a billion adults around the world each week. Now, they face the prospect of losing tens of millions in audience share, even with the explosion of social media. All this, as Radio China International (RCI), Radio Russia, Iran's Press TV, and Qatar's Al Jazeera, significantly expand their operations. China, for example, spends two billion dollars a year on external media, about triple the outlay for all five publicly-funded U.S. overseas networks. Ironically, Beijing, Moscow, Tehran and Doha have all ramped up transmissions in English, just as the BBC and VOA have cut theirs back. In December, the five directors of the Western networks meeting in London noted increased jamming of international satellite TV programming in 2011, especially by Iran. They called on the International Telecommunication Union in Geneva to take up the issue at an upcoming meeting. The director generals also appealed to satellite operators and service providers "to recognize the importance of the role they play in ensuring the free flow of information."

MEETING THE CHALLENGES

Given this background, does the United States have a more pressing national and global security responsibility to enhance its overseas media services and the content of those services, given the decline of its Western partners on the world's airwaves? Most assuredly, yes. Can U.S. international broadcasting, using the framework of its newly-announced five year strategic plan, successfully meet and master the challenges? Hopefully, yes. The challenges are:

- 1) Saving money in times of fiscal austerity affecting all the Western government networks
- 2) Modernizing and coordinating delivery systems amid the rapid changes each year in the way people receive and share information in a digital age
- 3) Creating compelling, competitive program content and robust dialogues with influential civil society actors in the increasingly crowded electronic marketplace of traditional and new media
- 4) Retaining a multi-regional presence in VOA English, our own mother tongue and indisputably, the primary world language of commerce, diplomacy, and the Internet.

The relatively new U.S. Broadcasting Board of Governors unveiled a landmark strategic plan last November 1. BBG Chairman Walter Isaacson recently told the Congressional Quarterly Weekly that the plan aims "to consolidate, integrate and streamline" the complex U.S. overseas broadcasting establishment. In addition to VOA, the only full service global network offering a mix of world, U.S. and regional news, there are four other smaller, distinctly separate regionally-targeted networks: Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia (RFA), the Middle East Broadcasting Network (Alhurra and Radio Sawa) and the Office of Cuba Broadcasting (Radio-TV Marti in Spanish).

Kim Andrew Elliott, a pre-eminent Arlington, Virginia, observer and international broadcast research analyst, posed the question as early as 1989: "Too many Voices of America?" A nine-member part-time bipartisan Broadcasting Board of Governors (BBG) was created in 1994 to oversee this conglomerate. It consists of four Democrats and four Republicans, and the Secretary of State as an ex-officio member, usually represented at monthly Board meetings by an Undersecretary for Public Affairs and Public Diplomacy.

On July 29, 2010, an entirely new BBG convened behind closed doors the day after being formally installed at a public session. It was a defining moment. One of the nine governors recalls: "We looked at each other, and everyone agreed: 'This isn't going to work'." They had done their homework and concluded that the five

separate networks, each with a distinct “tribal culture,” had no day-to-day coordinated central management. Moreover, they operated in different institutional frameworks:

---two of them are federal agencies, operating under U.S. government civil service or foreign service rules: VOA, the Martis, and the support agency for both, the International Broadcasting Bureau (IBB). VOA’s Charter (PLs 94-350 and 103-415) requires it to be an accurate and objective source of news about America and the world as well as a conveyor of major U.S. thought, institutions and policies and discussion of these.

---three of the networks are privately-incorporated but fully U.S. government-funded grantees, chartered to be alternative free surrogate media in regions they reach: RFE/RL, RFA, and the Middle East Broadcasting Network Inc. (MBN, like VOA, does provide a mix of area, world, and U.S. news and content to its viewers and listeners). The International Broadcasting Bureau (IBB) is co-located with VOA and the Board offices in southwest Washington, DC. It provides technical distribution, marketing, and program placement services for all the networks. IBB also operates other vital services (human resources, program evaluation, security, contracting, IT) for the federal entities. That makes managing VOA and OCB much more difficult than it was 20 years ago under the now-abolished United States Information Agency. Then the VOA director had under his or her aegis all functions, including that of budgetary and human resources control (now part of the BBG or IBB superstructures).

A MANSION OF MANY MISSIONS?

How did this cumbersome 21st century broadcasting bureaucracy come about? The late Mark Hopkins, a VOA correspondent in Moscow, Belgrade, Munich and Beijing in the 1970s and 1980s, said that over the years, various parties and constituencies felt compelled to add “a cupola here, a porch there” to meet what they saw as national strategic needs of the moment. It was helter skelter. Some steps were taken in the Executive Branch, others by individual members of Congress, and some even by individual networks determined to extend their mandate.

The result: 22 of VOA’s language services have been duplicated in other networks since 1950 (although most of the grantees and VOA also broadcast in unique languages of their own). Perhaps the single most devastating loss for VOA, critics say, was the loss of its half century old Arabic Service in 2002. An earlier BBG removed it from the Voice and privatized it two years later under the latest cupola added in 2004, the Middle East Broadcasting Networks Inc. The Board, on the other hand, points to research indicating substantial viewership of MBN’s Alhurra. Lately, there has been something of a convergence in the increasingly sophisticated content mix of VOA and the grantees, crucial to their credibility. By and large, however, distinct content continues to reflect distinct missions.

THE ROAD AHEAD

This was the situation inherited by the new oversight Broadcasting Board at its inaugural gathering in the summer of 2010. At that session, the seeds were sown for its new strategic plan, “Impact through Innovation and Integration.” The six and a half page document incorporated the views of more than 70 outside specialists. It is based, as well, on a more comprehensive annual BBG language service review. The 2012-2016 strategic forecast calls for:

---Appointment of a day-to-day chief executive officer for all five networks. This role is now filled on an interim basis by the director of the International Broadcasting Bureau, Dick Lobo. He is a federal officer, and the grantees are private corporations, limiting his mandate. But he has improved coordination among the networks and is overseeing a merger of their overseas news bureaus. There have been more joint programming ventures among the five in the past year since Lobo assumed office than in the 70 previous years of U.S. overseas broadcasting --- particularly in coverage of the Arab awakening.

---Combining the BBG and IBB bureaucracies, which had operated somewhat independently since the Board was established in 1994. The cost of the two organizations in the Administration’s current annual budget proposal is more than a third of the \$767,030,000 requested for all of U.S. international broadcasting. Appropriators in both the House and Senate prescribed substantial cuts in the IBB in separate reports approved last summer. One way to achieve this would be by consolidating the BBG and IBB support staffs. The merger became official on January 15, 2012 and consolidated various BBG/IBB operations to create units for Communications and External Relations, Strategy and Development, and Digital and Design Innovation.

---Consolidating administrative support for the privately-incorporated grantees (RFE/RL, RFA, and MBN). Deloitte, a consulting agency hired to examine the feasibility of the strategic plan, says that combining the financial management, technical staffs, and purchasing power pools for equipment and services of the three entities might yield annual savings of between \$9,000,000 and \$14,000,000. These savings, the consultant adds, “could be redeployed toward journalistic initiatives that advance the Board’s strategic vision.” Deloitte quoted grantee executives as conceding that the present structure was haphazardly built over time, and

"would not be the logical approach if one were starting fresh." Deloitte agreed. It endorsed the concept of grantee administrative consolidation.

---De-federalizing the government agencies: VOA, IBB, and the Martis. The advantage of privatizing the three departments is that they would be on the same basis, administratively, as the three grantees. This could pave the way for streamlined, common, presumably cost saving procedures across all of U. S. international broadcasting. A single consolidated, publicly-funded, private corporation likely would be easier to manage. Its output might be perceived by users as less subject to U.S. government interference, although journalistic content "firewall" procedures have been pretty effectively enforced by successive Boards since 1995.

Deloitte, while endorsing the Board's proposal to merge the grantees, is still looking at de-federalization of VOA and Martis. The consultant suggests that a feasibility study include: 1) Partial integration in 2012 of a few VOA and Marti administrative operations with those of the grantees, short of full-scale privatization that would require new legislation, and 2) A longer term look into the feasibility of full-scale de-federalization of those two networks and IBB, including benefits, risks, and financial impact. De-federalization, however, faces opposition by those in Congress who view the flagship VOA and its support organization as vital to the nation's security.

---Repealing the clause of the 1948 Smith-Mundt Act that prohibits the dissemination of BBG materials within the United States. Congress is actively considering repeal, led by Representatives Mac Thornberry (R-Texas) and Adam Smith (D-Washington). For the first time, both the State Department and the BBG have actively supported a change in the old law and proposed language to abolish the prohibition. (The original legislation was passed shortly after World War II to prevent any sitting administration from using U.S. government media to influence the American public. But in the 21st century, all five overseas networks have websites and content easily accessible to millions of Americans, making the original legislation outdated).

---Abolishing duplicated language services in the five networks. Advocates of ending overlap among VOA on one hand and RFE/RL, RFA, MBN and the Martis on the other, say it is high time to trim the many "voices of America." Yet a spot check of their respective websites shows surprisingly little content duplication on any given day. VOA and MBN cover world, regional and U.S. news. RFE/RL, RFA and the Martis focus largely on events in regions they reach. Influential users of all ages likely channel surf a combination of the U.S media over time, finding them for most part complementary in the news, information and ideas they seek and share.

Rationalizing which languages to cut in U.S. international broadcasting at which networks likely will be the most contentious issue confronting the Board in 2012 and 2013. Many services have champions on Capitol Hill. Services broadcasting the U.N. official languages and several key strategic ones such as Persian and the Afghan languages should have both full service content and full service distribution in today's highly competitive 21st century communications environment. Sufficient staffs are required to build new and social media platforms in these languages for the burgeoning younger generation around the globe inspired by the Arab pro-democracy uprisings. Better to cut bulging support bureaucracies than frontline journalists, editors, video producers, and webmasters. As one knowledgeable professional international broadcaster put it: "Heavens, yes."

In key languages particularly, cross-streaming of content is essential across platforms (radio, television, and a variety of social media channels). BBC Director General Mark Thompson told a London conference shortly after the massive BBC World Service cuts were announced: "The future of news and information is intrinsically multi-platform, multi-device and multi-media. No one medium, neither TV, nor radio, nor print, nor even the web are sufficient in themselves." Those players with multiple platforms, he added, "are capturing the highest amount of news consumption."

---Creation of a Global News Network (GNN) pooling the best journalism and on-scene reporting of all five U.S-funded overseas networks. This may be essential to meet the most ambitious goal of the BBG's strategic plan: expansion of the networks' combined reach from 165 million in 2010 to 216 million in 2016. The GNN, expected to take shape soon, will draw on the reportorial resources of VOA, RFE/RL, RFA, MBN and the Martis. Collectively, they have hundreds of correspondents and contract reporters filing in 58 languages around the world.

Pilot prototypes of the GNN have already been produced, and skeletal approximation of a future combined news roundup appears daily on the main page at the BBG website, www.bbg.gov. A logical site for assembling a more robust GNN is the VOA newsroom in southwest Washington, where space is adequate, English scripts are produced and where the Board's and IBB headquarters are located. A logical state of the art distribution system is used by RFE/RL in Prague. It is now being installed at the other networks to ease transfer among them of audio, video and website content. GNN, the BBG strategic plan has said, will retain the well-established brand names by the originating networks, as warranted --- an indispensable asset.

THE WEST REACHING THE REST?

Just a few days after the BBG's strategic plan was released, a fresh tally of the current audience for U.S. government funded international broadcasting was firmed up and made public in mid-November. The claimed global reach on all global media this past year surged from 165,000,000 to 187,000,000 adults weekly. Significant increases were registered in Indonesian (VOA), Pashto and Dari to Afghanistan (RFE/RL and VOA), Arabic in Egypt (MBN), and Hausa to Nigeria and Niger (VOA). Radio Free Asia audiences to several southeast Asian countries (11,900,000) were counted for the first time. There were declines in VOA Persian News Network viewing in Iran despite the popularity of its satire program Parazit, and in VOA's reach in Pakistan, the Board said, due to a growth in competition by new local outlets.

Three elements stood out in this latest research overview:

- 1) The astonishing growth of the VOA Indonesian audience, largely on television, from 25 to 38 million
- 2) The predominance of the Voice in the final cumulative total: 141 million out of the 187 million listeners/viewers/Internet/short messaging users (about 75 per cent)
- 3) the way people still get information worldwide, 103 million on radio, 97 million on TV, and 10 million via the new media[1]

All silent on the Western front, informationally? Hardly. The United States does have an opportunity to fill in gaps, if it does so wisely within fiscal constraints. Despite massive cuts in shortwave transmission facilities by the U.S. over the past nine years and plans to do so by all of the so-called Big Five governmental international broadcasters of the West between now and 2016, caution is advised. Despite cuts in relay facilities, radio audiences are more than holding their own, in U.S. international broadcasting, an 8.7 per cent increase (9.5 million) between 2010 and 2011. (TV viewing did even better: a 22 per cent increase (17.5 million viewers), compared with one million more for the Internet this past year (11 per cent).

As Secretary of State Clinton, an ex-officio member of the BBG, told the Senate Foreign Relations Committee in February: "Even though we're pushing on-line, we can't forget TV and radio because most people still get their news from TV and radio."

Radio World editor Paul McLane recently wrote: "These totals and percentages suggest to me that radio's role as part of Uncle Sam's face to the international community is understated and underappreciated." In the U.S. commercial radio industry, McLane adds, it is much the same and "radio continues to post total listening statistics (241 million weekly listeners) that other media envy. Radio is the media's best kept secret!" Only a year ago, BBC research and transmission specialists had estimated the World Service's shortwave radio audience at 85 million. Silencing shortwave or radio relays via FM stations too early, before new social media are better established, would carry real risks (see No. 3 above).

Building and deploying new media, to be sure, are essential in making hard choices because the way people consume and share information is changing with lightning speed. The BBG, VOA and the social media platform Citizen Global this year began collaborating on providing multiple channels (TV, Internet, and audio streams) to enable women in central Africa's conflict zones to share their stories with others. Some interact on line with those who hear their grim accounts of rape and pillaging, a sort of "iMovie in the cloud." Recently, VOA's Afghan Service program, Radio Ashna reported a deadly Taliban suicide bombing in Kandahar and an appeal for blood donations to help the victims. A number of donors responded. A VOA English website (<http://middleeastvoices.com>) focuses on Arab world events and combines radio, TV and text in a daily Syria Report that recently interviewed the commander of the Syrian Free Army. A new VOA daily shortwave radio program on refugee relief in Somali and Amharic to famine-stricken Horn of Africa has helped thousands gain access to lifesaving food and water and even stay in touch with lost family members. And VOA Development Office trainers in Hong Kong met a number of journalists from mainland China this past year to share ideas with each other about how accurate, reliable, information can empower readers, listeners, viewers and bloggers alike.

Content is king, and credibility will continue to be the North Star of U.S. international broadcasting program producers and reporters in every region of the world and in the United States. As the strategic plan shows, the Board can supply an overarching policy framework. But accurate, objective journalism produced at the broadcaster level is what matters most and empowers listeners in a wide range of settings, from refugee camps in Africa, Tibetan monasteries in India, to large communities of social media consumers in the cities of China, Russia, the Arab world, Iran, North Korea, and in an awakening Burma. Although choices will be painful for all the broadcasters of the West in the years ahead, progress in 2011 toward synergies in America's world services augur well. Congress, after all, has termed U.S. international broadcasting a national security function. It, along with the administration, the BBG, and the networks themselves, can and must master the

challenges. As Edward R. Murrow once said: "Our task is formidable and difficult. But difficulty is one excuse history has never accepted."

[1] The totals add up to more than the worldwide cumulative of 187 million because a listener/viewer/netizen who uses more than one U.S. government medium or delivery system, counts only once.

[Table of Contents](#)

Who sent a false text message saying cash benefits will no longer be paid to Iranians?

From [Spotlight on Iran](#) (Week of January 11-18, 2012)

A text message sent this week to Iranian citizens, claiming that cash benefits will no longer be paid under the subsidy policy reform, caused a public uproar and media frenzy.

Earlier this week Iran's media reported that in the last several days a number of citizens have received a text message from an unknown source stating that, since they own a car and an apartment, as of this month they are no longer eligible to receive the cash benefits paid by the government to Iranian citizens. An Iranian who received the text message told the Qods newspaper that the message is a source of great concern for his family, since they depend on the cash benefits. So far the authorities have been unable to discover who is responsible for sending the text message.

The text message drew considerable interest since it was sent shortly after government officials announced that, as part of the second stage of the reform plan, the government intends to stop paying the cash benefits to more than 10 million Iranians whose monthly income ranks in the top three deciles.

Following the media frenzy sparked by the text message, Behrouz Moradi, chairman of the organization in charge of implementing the subsidy policy reform, said that the text message was fabricated. He asked the legal authorities to check who is responsible for sending it, and said that a lawsuit will be filed against those individuals. Moradi said that the text message was part of a plot designed to spread lies, raise concerns among the public, hit the economy, and undermine the government's success in implementing justice and the subsidy reform (Mehr, January 16).

Top officials in the reform organization stressed that the fabricated text message has nothing to do with the government's plans with regard to the second stage of the subsidy policy reform. They noted that, at first, people who earn a high income will be sent a letter asking them to remove themselves from the list of cash benefit recipients on their own initiative. It is only then that the government will intervene, and, at any rate, no text message has been sent about the issue. The officials noted that the fabricated text message was also sent to low-income families, ones that are not supposed to be on the list of families which will stop receiving the cash benefits (Kalemeh, January 16).

[Table of Contents](#)

Cyberspat Erupts As Baku-Tehran Relations Become Increasingly Strained

From [RFE/RL](#), January 17, 2012

BAKU -- Iranian-Azerbaijani tensions -- which have been escalating for weeks -- have apparently erupted into a cyberskirmish that has affected dozens of websites in both countries.

Meanwhile, a meeting between Azerbaijani, Iranian, and Turkish foreign ministers scheduled for January 17 was suddenly canceled.

The official reason cited was that Turkish Foreign Minister Ahmet Davutoglu must attend the funeral of Turkish Cypriot leader Rauf Denkash.

On the same day the meeting was supposed to have taken place, a group calling itself the "Real Azerbaijani Cyberarmy" launched a cyberstrike against dozens of Iranian sites, making them inaccessible.

These attacks are apparently a response to a similar attack on January 16, in which about a dozen official Azerbaijani sites, including those of President Ilham Aliyev, the ruling New Azerbaijan Party, the Constitutional Court, and the Interior and Communications Ministry were inaccessible.

Visitors were greeted by claims of responsibility from the "AzerianCyberArmy" and assertions that the government in Baku is "serving Jews."

The same day, several websites in Israel -- including the sites of the El Al airline and the Tel Aviv stock exchange -- were attacked.

Communications Minister Mushfiq Amirov said on January 17 that the attacks against Azerbaijani sites have been traced to several "geographical locations," but he declined to specify where and did not attribute blame for the attacks.

The Azerbaijani sites were promptly restored and analysts downplayed the significance of the cyberassault.

"This cannot be considered a full-scale cyberattack," said Azerbaijani cybersecurity expert Rashad Aliyev. "They gained access to the sites' servers, threw a shell program over them, and changed the indices without damaging the databases, but they have changed some files.

"It shows the programming of the sites is weak. If you can break a door with a stone and enter, [it shows] the site could be exposed to bigger attacks. One or two hours was required to return the sites to their previous state."

Months Of Tension

Relations between Azerbaijan and Iran have been particularly strained in recent months.

Tehran has criticized Baku's close relations with Israel, which regards Azerbaijan as a key friend among Muslim countries. Azerbaijani supplies account for about one-fifth of Israel's oil stocks.

Azerbaijan is also currently a nonpermanent member of the UN Security Council, which regularly discusses Iran's controversial nuclear program.

President Aliyev's government is staunchly secular, and it has recently cracked down on pro-Iranian groups and mosques in Azerbaijan.

In November, prominent Azerbaijani writer Rafiq Tagi was killed in an attack widely seen as retaliation for an anti-Iranian article he had published.

Although Tehran has denied any involvement in Tagi's killing, he was targeted in a 2007 fatwa by Iranian cleric Grand Ayatollah Fazel Lankarani.

In December, Azerbaijani Deputy Foreign Minister Araz Azimov, speaking in Washington, D.C., accused Iran of "vigorously and economically cooperating with Armenia," noting that "Iran has many more agreements with Armenia than with Azerbaijan."

He said Iranian support helps Armenia maintain its "occupation" of the disputed Azerbaijani region of Nagorno-Karabakh.

Cyberattacks are notoriously difficult to attribute. A New Azerbaijan Party spokesperson claims the attack on the party's website was traced back to Iran.

However, hacker groups in Armenia and Azerbaijan have traded similar attacks in the past.

Azerbaijan Internet Forum President Osman Gunduz said the attacks represent a declaration of "cyberwar." He called on the authorities to investigate the security lapses that left the websites vulnerable.

[Table of Contents](#)

SPAWAR Recognizes Space Cadre at Information Dominance Warfare Officer Pinning Ceremony

By Tina Stillions, [Space and Naval Warfare Systems Command](#), 20 January 2012

CHANTILLY, Va. -- Space and Naval Warfare Systems Command (SPAWAR) held an Information Dominance Warfare Officer pinning ceremony to recognize more than 60 Navy active duty and reserve officers Jan. 19.

Held at the National Reconnaissance Office (NRO) here, the event highlighted the SPAWAR Space Field Activity's contribution to the Information Dominance Corps and was presided by Deputy Chief of Naval Operations for Information Dominance Vice Adm. Kendall Card.

Rear Adm. James Rodman, SPAWAR chief engineer, received his pin during the ceremony and provided opening remarks before introducing Card.

"Just as the armored tank transformed land warfare and the aircraft carrier sea warfare, our networks and our ability to use information will transform the estate known as cyber warfare," said Rodman. "If Gen. Patton were alive today, he'd probably trade in his pearl handed six shooters for a smartphone and an iPad."

Rodman discussed the importance of information as the Navy's newest warfare domain. Information Dominance requires speed to identify, process and correlate data into a recognizable whole so that it can be used as an asymmetric warfighting advantage.

"The electromagnetic world has become the real world and we have to dominate it," said Rodman. "That's a huge sea state change for our doctrine, our weapons and our people."

The Information Dominance Warfare pin is given to a select group of skilled individuals with expertise in intelligence, information warfare, oceanography, meteorology and space. Those who receive the designation must complete a rigorous training and qualification process before being awarded the insignia.

Card stressed the importance of bringing members of the space cadre into the fold and solidifying a vital link in the Information Dominance Corps architecture.

"The warfare pin represents a common warfighter identity for the Information Dominance Corps and I'm here to welcome you to your community," said Card. "The qualification represents the significant gains we have made toward establishing the IDC as a key warfighting capability of the U.S. Navy."

The SPAWAR SSFA cadre is the Navy's presence at the NRO and also serves the Program Executive Office for Space Systems, which coordinates all Department of Navy space research, development and acquisition activities.

As the Navy's Information Dominance systems command, SPAWAR designs, develops and deploys advanced communications and information capabilities. With more than 8,900 active duty military and civil service professionals located around the world and close to the fleet, SPAWAR is at the forefront of research, engineering, acquisition and support services that provide vital decision superiority to our forces at the right time and for the right cost.

[Table of Contents](#)

In the Middle East, Cyberattacks Are Flavored with Political Rhetoric

Published January 24, 2012 in Arabic [Knowledge@Wharton](#)

In the beginning of January, a self-described Saudi Arabian hacker known only by the handle OxOmar claimed he had posted details of 400,000 Israeli credit cards online. The target was commercial assets, but the message of the attack was political: In online statements he stated that he belonged to "the largest Wahhabi hacker group of Saudi Arabia," that counted among its targets credit card accounts used to donate to "Israeli Zionist Rabbis." It was the first salvo in a series of attacks the regional press has come to describe as "cyber warfare" between Arab and Israeli hackers this month.

Days after his first leak, OxOmar posted online another information batch of 11,000 Israeli credit cardholders, though Israeli banks said altogether only 20,000 credit card accounts had been compromised. Soon after, an Israeli hacker calling himself 'OxOmer' went online to announce he had posted names, email addresses, phone numbers and credit information of 217 Saudi Arabian credit cardholders. OxOmar promptly released online the information of another 200 Israeli cardholders, and upped his rhetoric.

More Arab credit card accounts were posted online in response, and the hacking then moved on to larger commercial targets, as the websites of the Tel Aviv Stock Exchange, El Al Airlines and several Israeli banks were disrupted. Israeli hackers responded, attacking the Abu Dhabi Securities Exchange and Tadawul, Saudi Arabia's exchange, then the United Arab Emirates' Central Bank website and that of the Arab Bank Palestine. The Israeli hackers said their actions were also politically motivated. "You can call this a Zionist revenge," the hackers told Israeli newspaper Yedioth Ahronoth.

The incidents highlight the ability of cyber criminals to carry out attacks across borders, even when corporations are aware of their threats. They also demonstrate how digital disruptions could become a tool in state conflict. The Middle East is considered a boom market for cyber security; according to RNCOS research, the regional market for IT security software is expected to grow at a CAGR of over 34% from 2010 to 2013. But the mixing of historical political disputes with cybercrime and cyber vandalism gives online threats in the region a distinct tinge.

"The question that then arises is how can organizations and individuals protect themselves," says Gurpreet Dhillon, professor of information security at Virginia Commonwealth University. "It is no longer the question of buying an ever so complex lock. It is more about ensuring that the key to the lock is not compromised. Part of the exercise is about awareness. Many of the social engineering attacks go unnoticed because individuals do not know about the nature and scope of the attack. Many organizations are also ill-prepared to deal with cyber threats."

A Binary Explosion

Former Central Intelligence Agency and National Security Agency director Michael Hayden was the main guest speaker at a recent conference on cyber security in the United Arab Emirates capital of Abu Dhabi. He too noted how forces from the online world had intertwined themselves with the region's politics, reflecting on the experience of Egypt's social media-fueled protests that led to the ouster of then-President Hosni Mubarak.

"Omar Suleman [the former head of the Egyptian intelligence service] was a very good intelligence officer," Hayden said. "Omar Suleman was so good at his job that he was able to keep Mubarak in power against all opposition for more than three decades. And yet, the immolation of a fruit merchant in a small Tunisian city set in motion a revolution enabled by the cyber world, enabled by social media.

"A few weeks later there were a million people in Tahrir Square in Cairo, calling for the overthrow of the Egyptian government. In other words, all of Omar's skills he used to maintain support for Mubarak were insufficient to meet the volume, and the velocity of what was coming at him, enabled by this domain."

In the modern world, Hayden said, few countries don't perform espionage. And the role of the NSA, he said, was to do that electronically. "It's the American intelligence organization that does what we call computer network exploitation. Which means, getting on someone else's network where we are not welcome and extracting information from that network."

"I can tell you American policy. We steal secrets, you bet. But we steal secrets essential for American security, safety and liberty. We don't steal secrets for American commerce, for American profit. There are many other countries around the world, that do not self-limit so."

Hayden dwelled upon another instance of cyber subterfuge coupling with real world politics in the Middle East -- the development of the Stuxnet computer virus in 2010, which was allegedly deployed by the U.S. and Israel to hobble Iran's nuclear weapons program, crashing entire cascades of uranium enriched centrifuges.

"Someone, almost certainly a nation state, felt it was a legitimate act of self-defense or counter-proliferation, to use a cyber weapon to create physical destruction in something that another nation would almost certainly describe as their critical infrastructure.

"A cyber weapon was used to destroy a nation's critical infrastructure. That's a big deal. To use an example from history, that's an army crossing the Rubicon. That's a legion on the wrong side of the river. Our world is different now. Someone just moved us into a new era. Someone just used ones and zeros to make something go bang."

Still Cyber Thieves

Computer security experts and analysts say that despite the politics on display with many of these cyber threats in the region, the goal for many attacks is still simple thievery. Getting a handle on how much is going on varies wildly. According to the United Nations Interregional Crime and Justice Research Institute (UNICRI), cyber criminals netted an estimated US\$240 million globally in 2007. But Symantec, the publishers of the Norton security software, released a report last September pegging the cost of global cyber crime at US\$114 billion a year.

Nevertheless, organized crime has adopted the technique for its operations, and the online threat to businesses and individuals will continue its sophistication, says Francesca Bosco, project officer with UNICRI. "Cyber crime is very profitable, with low infrastructure costs, and readily available attack tools," she says. "Cyber crime has become an integral part of the transnational threat landscape."

Bosco notes that cyber thieves around the world largely engaged in the sort of information theft displayed by the Arab and Israeli hackers in their online battles. An entire online underground has spawned, she said, devoted to selling clusters of data such as credit card numbers, or Facebook accounts. "If you steal money, once its spent, its gone," she says. "But data can be used and reused in so many different ways."

VCU's Dhillon says hacking tools are as easy to acquire, so much so that even governments have taken avail of them. "For instance [one website] sells password "cracking" services for major email services for as little as US\$150," he says. "Many nation states systematically make use of such like services. A Paris court [last November] fined the French energy giant, Électricité de France, nearly US\$1.9 million for directing a hack into Greenpeace computers."

Middle East malware (malicious software) authors know that most countries in the region filter websites based on religious content and pornography, says Christian Beek, principal consultant at McAfee Foundstone Services EMEA. Instead, he says, malware in the region is largely spread through file sharing and USB drives. He pointed out that Microsoft online security analysts had discovered over 60% of every 1,000 computers in Qatar had been infected with malware, a rate far higher than anywhere else in the world.

For these reasons and others, Middle East consumers remain wary of going online to make purchases. According to a recent survey of e-commerce in the Middle East by online payment service OneCard, fraud and theft of personal information is still the biggest concern preventing more regional customers from making purchases online.

Caution is warranted, says Ken Baylor of Gladius Consulting. Cyber thieves regularly exploit seemingly secure financial transactions even in the U.S., he said. "It's an innovation battle between banks and criminals," he notes.

Baylor has worked on a number of online security issues for banks, and says that cyber criminals largely relied on software that hid itself in other programs, and allowed them remote access to a user's sensitive information on their computer, such as their bank account, often without their knowledge. Such programs, referred to as 'Trojans,' have become harder to detect, and more complex over time, he says.

One such type of cyber attack being perpetrated increasingly in the Middle East, according to KCS Group, an international security firm, in an interview with Abu Dhabi-based newspaper The National, is the technique of holding bank account access for ransom, where users or institutions are told by cyber criminals to pay up or see sensitive information about them published online.

But so much information is readily available online without requiring any sophisticated tools to access it, said web security professional and blogger Jamal Bandukwala. Instead, it's just a matter of knowing where to look. "It's a good idea to see what information your company is putting out there," Bandukwala said.

A number of government intelligence agencies have already caught onto the fact, Bandukwala noted, and cull the Internet for data in a method he called 'open source intelligence.' By constantly collecting sources of information online, he said, including media, web content, satellite imaging, public documents and academic journals, governments can search the web very deeply. "It's all fair game," he said.

One of the sites favored for trading information, he added, started out as a simple tool for developers to share source code online via text snippets. "Now it is used to leak information anonymously," Bandukwala said. A quick run through the site reveals credit card numbers, leaked databases, compromised websites, employee lists, even passport numbers and travel itineraries that were electronically intercepted and posted. The same website, incidentally, is used by OxOmar and his Israeli opponents to post their latest hacks.

"In spite of decades' worth of work, organizational security policies still represent reactions to the latest slew of attacks; reactive approaches do not work," Dhillon adds. "As a society we need to understand the limits of technological advances and its appropriate uses. Just like one would not hand out the key to the house to a stranger, similarly sharing passwords or using a credit card in an untrusting environment should be avoided."

[Table of Contents](#)

SCADA Systems in Railways Vulnerable to Attack

By Fahmida Y. Rashid, [eWeek](#), 2012-01-25

Government officials initially believed railway signal disruptions in December were tied to a cyber-attack against a Northwest rail company in December, Nextgov reported. But government and railway officials later denied that a U.S. railroad had actually been hit by a cyber-attack.

"There was no targeted computer-based attack on a railroad," said Holly Arthur, a spokeswoman for the Association of American Railroads.

While an attack has been ruled out, the incident highlights the dangers of industrial control systems controlling critical infrastructure.

Train service on the unnamed railway was "slowed for a short while" and schedules delayed for 15 minutes on Dec. 1, according to a Transportation Security Administration memo obtained by Nextgov. A "second event" occurred just before rush hour the next day, but it did not affect schedules, according to the Dec. 20 memo, which summarized the agency's outreach efforts to share threat intelligence with the transportation sector.

"Amtrak and the freight rails needed to have context regarding their information technical centers," the memo said, adding that rail operators were not focused on cyber-threats.

TSA investigators discovered two IP addresses for the intruders associated with the Dec. 1 incident and another for Dec. 2. Investigators considered the possibility of the attackers being based overseas, but did not specify the suspected country, Nextgov reported. Alerts listing the three IP addresses were sent to several hundred railroad firms and public transportation agencies.

Officials at the Department of Homeland Security, which oversees the TSA, told Nextgov on Jan. 23 that further investigation showed it may not have been a targeted attack, but did not explain what may have caused the "anomalous activity."

The railway incident is similar to what happened at an Illinois utility last fall. A government fusion center claimed Russian attackers had remotely destroyed the facility's water pump, but the DHS on further

investigation claimed it was not an attack. It later turned out the intrusion had been an American contractor remotely logging in to perform some maintenance tasks.

However, the TSA's railway memo highlights how vulnerable the railways are to an attack on supervisory control and data acquisition (SCADA) systems, according to experts from Casaba Security, a security analysis and consulting company. Just about anything in the railway infrastructure could be controlled by SCADA systems, including track switches, signal and crossing lights, transformers, weather and track sensors, engine monitors, railway car sensors, electronic signs and even turnstiles, said Samuel Bucholtz, Casaba's co-founder. Most of these systems are connected to the network so that they can obtain data collected by the sensors.

"A sensor that can detect the position of a track switch is not helpful unless it can pass that data to an operations center hundreds of miles away," Bucholtz said.

Connecting SCADA systems to the Internet puts the infrastructure at risk because it opens up the possibility of intruders finding a way into the network. However, many organizations take that risk to save money, simplify the infrastructure and ease maintenance. It is usually cheaper to transmit data over the Internet instead of investing in dedicated lines or wireless frequency space, according to Bucholtz.

"The benefit of SCADA being 'online' is that the Internet is cheap, robust, standardized and easily accessible," Bucholtz said.

The downside is that without proper protections, the infrastructure is wide open to anyone looking. Cambridge University researcher Eireann Leverett developed a tool that mapped more than 10,000 industrial control systems accessible from the Internet, including water and sewage plants. While some of the systems could have been demo systems or used in places that wouldn't count as critical infrastructure, such as the heating system in office buildings, some were active systems in water facilities in Ireland and sewage facilities in California.

Only 17 percent of the systems mapped asked for authorization to connect, suggesting that administrators either weren't aware the systems were online or had not installed secure gateways, Leverett said. Leverett, a computer science doctoral student at Cambridge, presented the findings at the S4 conference in Miami.

Administrators need to set up secure and isolated networks and use Secure Sockets Layer or a virtual private network to restrict who can talk to the controllers, according to John Michener, chief scientist at Casaba. Since SCADA systems will likely be Internet-accessible, administrators should focus on putting them behind a secure gateway. "Increasingly all the communications are over the Net, so being on the Net is all but inescapable," Michener said.

[Table of Contents](#)

Twitter Able To Censor Tweets in Individual Countries

From The [Guardian](#), 26 January 2012

Twitter: tweets containing content breaking a law in one country can now be taken down there but still be seen elsewhere. Photograph: Jonathan Hordle / Rex Features

Twitter has refined its technology so it can censor messages on a country-by-country basis.

The additional flexibility announced on Thursday is likely to raise fears that Twitter's commitment to free speech may be weakening as the short-messaging company expands into new countries in an attempt to broaden its audience and make more money.

But Twitter sees the censorship tool as a way to ensure individual messages, or tweets, remain available to as many people as possible while it navigates a gauntlet of different laws around the world.

Before, when Twitter erased a tweet it disappeared throughout the world. Now, a tweet containing content breaking a law in one country can be taken down there and still be seen elsewhere.

Twitter will post a censorship notice whenever a tweet is removed. That is similar to what internet search engine Google has been doing for years when a law in a country where its service operates requires a search result to be removed.

Like Google, Twitter also plans to share the removal requests it receives from governments, companies and individuals at the [chillingeffects.org](#) website.

The similarity to Google's policy is not coincidental. Twitter's general counsel is Alexander Macgillivray, who helped Google draw up its censorship policies while he was working at that company.

"One of our core values as a company is to defend and respect each user's voice," Twitter wrote in a blogpost. "We try to keep content up wherever and whenever we can, and we will be transparent with users when we

can't. The tweets must continue to flow."

Twitter, which is based in San Francisco, is tweaking its approach now that its nearly six-year-old service has established itself as one of the world's most powerful megaphones. Daisy chains of tweets already have played instrumental roles in political protests throughout the world, most notably in the uprising that overthrew Egypt's government a year ago.

It's a role that Twitter has embraced, but the company came up with the filtering technology in recognition that it will likely be forced to censor more tweets as it pursues an ambitious agenda. Among other things, Twitter wants to expand its audience from about 100 million active uses to more than 1 billion.

Reaching that goal will require expanding into more countries, which will mean Twitter will be more likely to have to submit to laws that run counter to the free-expression protections guaranteed under the first amendment in the US.

If Twitter defies a law in a country where it has employees, those people could be arrested. That's one reason Twitter is unlikely to try to enter China, where its service is blocked. For several years Google agreed to censor its search results in China to gain better access to the country's vast population, but stopped that practice two years after engaging in a high-profile showdown with China's government. Google now routes its Chinese search results through Hong Kong, where the censorship rules are less restrictive.

In its Thursday blogpost, Twitter said it had not yet used its ability to wipe out tweets in an individual country. All the tweets it has previously censored were wiped out throughout the world. Most of those included links to child pornography.

[Table of Contents](#)

Taliban Folklore in Pakistani Media

By Abbas Daiyar, the [Friday Times](#), January 27 - February 02, 2012 - Vol. XXIII, No. 50

The dominant discourse in mainstream Pakistani media on issues of foreign policy and national security has always been based on the narrative of the military establishment. Most Pakistani analysts, both right-wing and liberal, believe the Taliban is a nationalist movement motivated by Pashtun alienation in Afghanistan.

This narrative is a product of the Pakistani military establishment's 'strategic depth' policy, and was propagated internationally by former military dictator Pervez Musharraf. Addressing the European Union parliament in September 2006, he said the Taliban represent Pashtuns and they could spark a 'national war' in Afghanistan. Domestically, opinion makers say in TV talkshows that the Afghan Taliban are representatives of the Pashtun.

They say the Afghan Taliban have grassroots support in the south and southeast, and the movement is a reaction to the lack of Pashtun representation. But they also say the Afghan Taliban are a genuine resistance force fighting an ideological war against foreign invasion. The two views do not coincide.

The central leadership of all major insurgent factions is based in Pakistan, be it the Quetta Shura of Kandahari Taliban, the Haqqani Network in Waziristan, or the Hizb-e-Islami of Hekmatyar

They would never say Tehreek-e-Taliban Pakistan represents all Pashtuns of FATA, or that the insurgency is a nationalist movement motivated by the grievances of the tribes. They call TTP a terrorist organization. And this is where the contradictory notion of good Taliban and bad Taliban comes into play. The Afghan Taliban are a resistance force representing Pashtuns, while their ideological brothers TTP, who also claim allegiance to Mullah Omar, are terrorists.

Ironically, those who claim that the Afghan Taliban are a Pashtun nationalist movement are not Pashtuns. Pashtun intellectuals and journalists, both liberal and conservative, and even Pashtuns who have been part of the military establishment, deny that.

The folklore of Taliban nostalgia prevailing in mainstream Pakistani media that Mullah Omar had brought peace to Afghanistan is also not shared by the Afghans. The Taliban killed thousands of people until there were no rivals and no one to resist their brutality, and there was rejoice in Kabul after their government was toppled in 2001.

Non-Pashtun ethnic politicians complain that Pashtuns hold most key ministries in President Karzai's administration

Afghans do not see the Taliban as a nationalist movement based on the Pashtunwali code, but influenced by Deobandi madrassas in Pakistan. They are not even a unified group. Not even all Afghan Taliban call themselves Pashtun nationalists. Although they are predominately Pashtun, many among them are from other ethnic groups, particularly in Northern Afghanistan. Local insurgent groups have multiple motivations. Some

join the resistance against the perceived foreign invaders, while others fight for local purposes, such as clan rivalries and personal interests. Then there are those who fight for money.

Working on a research project in Northern Afghanistan in August last year, I met some insurgents who were not ethnic Pashtuns, but Turkmen. They told me they were paid \$500 to \$600 a month by a Taliban commander in Mazar-e-Sharif. That is more than what some of my colleagues were being paid by an NGO. Some of the Taliban men are opportunists who benefit from the narcotics industry and seek Taliban's shelter.

"Unlike the late 70s and 80s when Afghanistan experienced a national resistance movement against the Soviet occupation, the Taliban's claim for Jihad against Americans does not resonate with a majority of Pashtuns," according to Afghan political activist and former chief of staff at Foreign Ministry Wahid Munawar.

The central leadership of all major insurgent factions is based in Pakistan, be it the Quetta Shura of Kandahari Taliban, the Haqqani Network in Waziristan, or the Hizb-e-Islami of Hekmatyar. The commanding cadres of the movement have gone to madrassas in Khyber Pakhtunkhwa, Southern Punjab or Karachi. Balochistan and the tribal areas are recruiting centers for Afghan Taliban. While traveling on the two borders, I regularly meet Taliban who are on their way to Quetta for rest, after a month or two of fighting in Helmand or Uruzgan. Majority of the suicide bombers in Afghanistan are traced to the tribal areas or Balochistan. What cultural or political grievances can they have about the Pashtuns of Afghanistan? The Taliban have destroyed the very foundations of centuries old Pashtun customs such as respect for tribal elders and the Jirga system.

"Taliban draw their support mostly from a tiny minority of Pashtun partly based on ideological grounds," says Rafi Fazil, an Afghan student and activist. "There is also an element of fear - given the vacuum created by the absence of government in Taliban controlled areas - that plays a key role. Not every Pashtun who sympathises with the Taliban actually subscribes to their violent ideology. Those who do, and are prepared to take part in violence, constitute a tiny minority."

If there are free elections, the Pashtuns of Afghanistan would reject the Taliban, like Pakistani Pashtuns vote for the liberal Awami National Party.

President Hamid Karzai received a large number of votes from the Pashtun south and southeast. The nationalist Afghan Mellat is a popular party among urban Pashtuns. There is no truth to the statement that Pashtuns lack representation in the current power structure in Afghanistan. In fact, non-Pashtun ethnic politicians complain of the opposite - that Pashtuns hold most key ministries in President Karzai's administration.

[Table of Contents](#)

Iran Mounts New Web Crackdown

By Farnaz Fassihi, [Wall Street Journal](#), 6 Jan 2012

Iran is mounting new clampdowns on Internet expression, including rules that will impose layers of surveillance in the country's popular Internet cafes, as Tehran's political establishment comes under increasing strains from economic turmoil and threats of more international sanctions.

In the most sweeping move, Iran issued regulations giving Internet cafes 15 days to install security cameras, start collecting detailed personal information on customers and document users' online footprints.

Until now, Iran's cybercafes have been a youth-culture mainstay of most towns and neighborhoods, used not only by activists but also by other Iranians who believe the security of their home computers is already compromised.

Iranian users also have reported more blocked sites this week, as well as new barriers to accessing social-networking services. Internet connections, too, have bogged down.

The network slowdown likely heralds the arrival of an initiative Iran has been readying—a "halal" domestic intranet that it has said will insulate its citizens from Western ideology and un-Islamic culture, and eventually replace the Internet. This week's slowdown came amid tests of the Iranian intranet, according to domestic media reports that cited a spokesman for a union of computer-systems firms. He said the intranet is set to go live within a few weeks.

Taken together, the moves represent Iran's boldest attempts to control flows of online information—a persistent thorn in the side of Tehran's political establishment since activists used the Internet to plan and document mass protests against what they said was a rigged election that returned President Mahmoud Ahmadinejad to office in 2009.

The video surveillance brings Iran further into the vanguard of nations that have sought to keep tabs on Internet use. Libya under Moammar Gadhafi ran extensive web-monitoring operations. China has

sophisticated website filtering and an army of censors patrolling chat rooms. China and Cuba require Internet-cafe users to present identification.

Tehran is imposing the crackdown amid a politically fraught run-up to Iran's March 2 parliamentary elections. Reformist political parties have already boycotted the vote. Meanwhile, Iran faces deepening economic pressures. International sanctions have crimped foreign sales and investments, inflation has been steep and the currency has dropped 40% against the U.S. dollar since late December.

The rial's record lows have come in part as the European Union and U.S. have threatened to place sanctions on Iran's central bank and impose an embargo on Iranian crude for what they allege is Iran's pursuit of nuclear weapons, a charge Tehran denies. A recent rhetorical battle between Iranian and U.S. military officials about access to waters of the Persian Gulf—through which one-fifth of the world's oil passes daily—raised fears of a possible military confrontation.

With the latest moves, the government is aiming to sow fear ahead of elections and curtail planned protests, say activists and observers in Iran and abroad. The Iranian judiciary announced last week that any calls to boycott elections, delivered on social-networking sites or by email, would be considered crimes against national security.

"They want to execute a plan where no one has protection, so they can trace whoever is involved in what they perceive as antigovernment activity at any given moment and at any location," said Ehsan Norouzi, an Iranian cybersecurity expert who left Iran after 2009 and now lives in Germany.

Tehran hasn't directly commented on the measures. The Islamic Republic, however, has long battled the Internet's influence and tried to filter access to sites, such as pornography or even fashion, that didn't fit within the norms of a conservative Islamic society. Since 2009, Iranian officials have widened their Internet monitoring to fight what they say is a "soft war" of culture and ideology against it. That year they formed the Cyber Police, a task force drawn from various security arms, which the government says has trained some 250,000 members.

In the past week, Iranian Internet users say the government has blocked access to VPNs—secure Internet networks that are located abroad—and foiled one of the ways users have attempted to gain entry to closed websites such as Facebook, Twitter and YouTube. In recent weeks the government also has targeted a popular currency-tracking site and pages belonging to prominent politicians, among others.

"They are closing in on us, and we are already feeling the dire impact of these announcements. Everyone is afraid," a prominent student activist said in an email exchange from Iran. "It will make it very difficult for us to tell the world what's happening here."

The new rules on cybercafes, issued by the Cyber Police and published Wednesday in several Iranian newspapers, require customers at the cafes to provide their name, father's name, address, telephone and national identification numbers before logging on.

The venues must install security cameras that will let the government match users to the computer they used. They also must log each user's browsing history, including the IP addresses of every Internet page visited. This data, along with the video images, must be saved for six months and provided to the Cyber Police on demand, according to the regulation.

"These rules are aimed at promoting transparency and organization for Internet businesses and offer more protection against online abuse," according to the text of the regulation.

Internet cafe owners in Tehran expressed anger at the rules, saying they would cause customers to shun their establishments, forcing them to close. "Do they think I'm running a security shop, to ask people for their ID number and put a guard above their head to monitor their Web activity? Are they insane?" the owner of a well-known Tehran Internet cafe said by telephone.

Separately, Iran's government appears to have enlisted an army of users to promote it on the Internet.

A conservative cleric blogger based in the holy Shiite city of Qum, Ahmad Najimi, said in his blog last week that the government was paying hackers hired in the network known as the "Cyber Army" the equivalent of \$7 per hour to swarm the Web with positive comments about the Islamic Republic and post negative comments against dissidents.

That is consistent with comments from the Revolutionary Guards Corps' commander in Tehran, General Hossein Hamedani, who in October announced the creation of two Cyber War centers in the capital. Gen. Hamedani said some 2,000 bloggers had been recruited and trained as Cyber Army staff.

"In the soft war against Iran, there is an opportunity for everyone to be present and we have to be ready for widespread counterattacks," Mr. Hamedani said, according to the semi-official Fars News Agency.

Iran announced in March 2011 that it was funding a multimillion-dollar project to build an Iranian intranet—a necessity, its telecommunications ministry said, to offer Iranians an alternative to the un-Islamic and corrupt content on the World Wide Web. An economic affairs official called it "a genuinely halal network, aimed at Muslims on an ethical and moral level."

An Iranian newspaper this week cited Payam Karbasi, the spokesman for Corporate Computer Systems of Iran, a professional union, as saying the network would be launched in coming weeks.

The network would first run parallel to the global Internet, Iranian telecommunications officials have said, with banks, government ministries and big industries allowed to access the global Internet.

But eventually, officials have said, the entire country—which the government estimates has some 23 million Internet users—would switch over. But many experts are skeptical that Iran could pull off such a project, saying the economy would suffer if its commercial entities are closed off.

[Table of Contents](#)

Call for Cyberwar 'Peacekeepers'

By Susan Watts, [BBC](#), 26 Jan 2012

The US Army's Cyber Command is recruiting.

Its mission? To create "a world class cyberwarrior force", and to develop cyberspace as an "active domain".

That's according to Lieutenant General Rhett Hernandez, Arcyber commander, speaking at a London conference on cyber defence this week.

He spoke of the explosive complexity of living in a digital age, and a cyber threat that was "growing, evolving and sophisticated".

Newsnight was invited to listen in at the conference,

Overall, the US military aims to recruit 10,000 "cyber warriors", and is apparently prepared to relax the usual entry criteria. They will accept long hair, even someone who can't run too well.

But there is a minimum requirement. Recruits will naturally be at the top of their field. They will be "a professional elite... trusted and disciplined, and precise... collateral damage is not acceptable," Lt Gen Hernandez told delegates.

Recruits will be trained using cyber challenge scenarios, for what is widely acknowledged as setting the cyber threat apart is not just its scale but its unpredictable and all-pervasive nature, posing a risk to critical national infrastructure such as power grids and water supplies, as well as the financial sector, individual companies and citizens.

'A huge issue'

Newsnight spoke to Sir John Scarlett about the nature of the cyber threat.

He was head of MI6 from 2004 to 2009, and chairman of the Cabinet Office Joint Intelligence Committee before that.

Earlier this month, Sir John became chairman of the Bletchley Park Trust.

In his first television interview since that appointment, he told us that Bletchley Park, and its famous wartime codebreaking success, held a special place in the history of cyberwarfare.

"Bletchley Park is at the very centre of this whole issue. In the Second World War, this was a state-to-state matter, and it was states grappling with each other... and so all the issues around cyber communications and their vulnerability were in that context.

"It was super secret. It didn't impact on people's everyday lives, and the whole issue of cyber communications, or machine communications didn't impact on people's everyday lives. Now it's into everything and everybody is affected by it.

"We have to worry about crime, we have to worry about terrorism, we have to worry about state activity, and we have to worry about what's called hacktivists...people with missions of one kind or another."

There seems little doubt in his mind that what he calls the "state-to-state issue", and the threat from the most capable states in this area, "remains a huge issue"

'Virtual peacekeeping force'

John Bumgarner, from the US Cyber Consequences Unit in Washington, would agree. His research organisation describes him as an "uber-hacker" with 18 years of service in special operations and intelligence.

He goes further. He told Newsnight there will soon be a need for a virtual UN peacekeeping force - in cyberspace.

"We've seen cyber incidents between Russia and Georgia, and that's ongoing. We've seen incidents between Pakistan and India and that's ongoing. We've seen stuff between China and India... between Israel and other Middle Eastern states. The UN needs to figure out how they can deploy peace keepers in the digital borders of a nation, virtual peacekeepers that would protect the peace."

Sir John thinks the cyber threat is growing by definition because use of the internet is growing. But he sees this as more than a purely military domain.

"There's quite a lot of talk about cyber warfare, and cyber attacks as if this is a military issue. Of course there are military aspects to it and military infrastructure aspects to it, and in the event of some future state-to-state conflict undoubtedly this would be a huge feature. But in the immediate term this is something which is happening now, the attacks and the downloading and the theft and the invasion of privacy are happening now on a day-by-day basis."

Computer security company Sophos confirms that the scale of attacks is growing, significantly.

Its teams constantly monitor computers infected with malicious code - often designed to send out Spam designed to trick users into giving away personal information that's valuable to organised crime. The company sells software to protect against such attacks.

"Here at Sophos we see 180,000 new pieces of "malware", that's malicious code, every single day. That compares with 1500 a day when I joined Sophos 6 years ago," said Mark Harris, VP SophosLabs & Global Engineering Operations.

'Cyber law'

And there are complaints that our laws are struggling to keep pace.

Stewart Room of Field Fisher Waterhouse said there was now a need for an amnesty - instead of punishment - for companies that suffered a data loss or cyber-attack.

An amnesty, he argued, would help to encourage companies to come forward and discuss what went wrong - so that others could learn, fast.

He is also calling for a new "cyber law", to formalise best practice.

"A good idea within legislation would be to introduce a requirement that companies need to state in their annual reports exactly what they've done to protect our security and our information that year. In the same way that annual reports contain statements about environmental issues such as CO2 emissions. If we were to deal with security in that way, shareholders would engage with the matter and so would the public generally and that would improve security."

Headlines about cyber attacks pop up almost daily now. One of the most startling was the attack on the global intelligence firm Stratfor over Christmas, for which members of the loose-knit hacker group Anonymous claimed responsibility.

John Bumgarner analysed the data released for the Guardian newspaper and concluded that thousands of British email addresses and passwords - including those of defence, intelligence and police officials as well as politicians and Nato advisers - had been revealed.

Mr Bumgarner chuckled when we asked if the Stratfor release might dent people's confidence in the ability of even the most security-conscious of organisations to keep data safe.

"We're taking it on blind faith... really when you give your information out as a private citizen to a corporation you're praying that that corporation will protect your data... as much as possible, but they can only do so much."

This week, the Republican presidential hopeful Newt Gingrich has been citing cyberwar on the campaign trail, reportedly saying that the appropriate response to countries that target US corporate or government information systems is to "create a level of pain which teaches people not to do it".

But how far can we trust what we're being told about the scale of the threat? I asked Sir John why anyone should take seriously his warnings about the threats to cyber security, given the track record - some might say failings - of British intelligence on Iraqi weapons of mass destruction.

"I think people have to judge what's being said here, make their judgements, apply their commons sense, and then just think it through and say: Well, is this a serious and believable and realistic issue, or is it not?"

At this week's London conference, delegates were reassured that technology would allow us to adapt to the cyber threat.

"We once thought of Aids as an existential threat, now we live with it," Major General Jonathan Shaw, commander of UK Cyber Policy at the Ministry of Defence told the audience.

"Our reaction today is similarly out of balance.... we're never going to cure it, we have to live with it... But how much intellectual property will we have left by the time we get it right?"

[Table of Contents](#)

The Strategic Communication of Unmanned Warfare

By Matt Armstrong, [MountainRunner](#), June 2008

Modern conflict is increasingly a struggle for strategic influence above territory. This struggle is, at its essence, a battle over perceptions and narratives within a psychological terrain under the influence of local and global pressures. One of the unspoken lessons embedded in the Counterinsurgency Manual (FM3-24) is that we risk strategic success relying on a lawyerly conduct of war that rests on finely tuned arguments of why and why not. When too much defense and too much offense can be detrimental, we must consider the impact of our actions, the information effects. The propaganda of the deed must match the propaganda of the word.

Giulio Douhet wrote in 1928,

"A man who wants to make a good instrument must first have a precise understanding of what the instrument is to be used for; and he who intends to build a good instrument of war must first ask himself what the next war will be like."

Secretary of Defense Robert M. Gates has said that there is too much spending geared toward the wrong way of war. I find this to be particularly true in area of battlefield robots. Much (if not all) of the unmanned systems planning and discussion, especially with regards to unmanned ground combat vehicles, is not taking into account the nature of the next war, let alone the current conflict.

Last year I posted an unscientific survey that explored how a ground combat robot operating away from humans (remote controlled or autonomous) might shape the opinions of the local host family. The survey also explored the propaganda value of these systems to the enemy, in the media markets of our allies, Muslim countries, and here in the United States. The survey results weren't surprising.

Serviam Magazine just published what could be construed as an executive summary of a larger paper of mine to be published by [Proteus](#) later this year. That paper is about four times longer and [adds a few points](#) with more details. In the meantime, my article that appeared in Serviam, Combat Robots and Perception Management, is below.

Also of interest: [Unintended Consequences of Armed Robots in Modern Conflict](#) and, for a different kind of unmanned warfare, see [For Official Secret Squirrel Use Only: the ACORN](#)

Combat Robots and Perception Management by Matt Armstrong (the below article originally appeared in the magazine Serviam and is based on a paper and presentation I gave at the U.S. Army War College):

Robots will figure prominently in the future of warfare, whether we like it or not. They will provide perimeter security, logistics, surveillance, explosive ordinance disposal, and more because they fit strategic, operational, and tactical requirements for both the irregular and "traditional" warfare of the future. While American policymakers have finally realized that the so-called "war on terror" is a war of ideas and a war of information, virtually all reports on unmanned systems ignore the substantial impact that "warbots" will have on strategic communications, from public diplomacy to psychological operations. It is imperative that the U.S. military and civilian leadership discuss, anticipate, and plan for each robot to be a real strategic corporal (or "strategic captain," if you consider their role as a coordinating hub).

As unmanned systems mature, ground systems operating among and interacting with foreign populations will substantially affect perceptions of our mission, both at home and abroad. Robots will exert significant influence in three overlapping information domains. The first domain is the change on the calculus of foreign engagement as the public, Congress, and future administrations perceive a reduction in the human cost of war (on our side). The second domain is the psychological struggle of the local populations in conflict and postconflict zones, and the third is the overarching global information environment.

The first domain and the most touted benefit of robots is their ability to reduce the exposure and vulnerability of America's warfighters. The Defense Department's Unmanned Systems Roadmap 2007-2032, approved in December 2007, leads with this point and repeatedly emphasizes it. Unlike President Clinton's lobbying cruise missiles against Al-Qaeda in Sudan and Afghanistan, a future president will be able to deploy remote-controlled and autonomous robots to accomplish the same mission with greater precision. However, few have considered the true cost of lowering the bar for kinetic action in a world of instant communications. There are

parallels here between outsourcing to machines and outsourcing to private military contractors that circumvent public and congressional oversight by avoiding the use of uniformed soldiers.

The second critical domain is in the psychological struggle for the minds and hearts of the men and women in conflict and postconflict zones. There is a real risk of undoing the lessons learned on the importance of personal contact with local populations that was earned at such a high price in Iraq and Afghanistan. Mapping the human terrain becomes, by implication at least, not only unnecessary but impossible in the sterility of robot-human interfaces.

In 2007, Lieutenant General Raymond Odierno issued guidance emphasizing the importance of engaging the local population and building a “feel” for the street. This guidance instructed Coalition forces to “get out and walk” and noted that an up-armored Humvee limits “situational awareness and insulates us from the Iraqi people we intend to secure.” Criticism of mine-resistant ambush-protected vehicles that prevent local engagement are just as applicable to robots operating in the sea of the people.

If deployments are not accompanied by intelligent and constant two-way conversations with the people and the media, the propaganda about our deeds becomes how the United States is not willing to risk lives for the mission or the host population. The media must not create the idea that the mission is not important enough to sacrifice our own men and women, lest the local population wonder why they should sacrifice theirs. The result may be more than replaying improvised explosive device attacks against robots on YouTube; it may lead to a modern propaganda contest and an escalation of spectacular attacks to reach humans in order to influence U.S. public opinion and increase extraregional sympathy for the insurgents.

The third domain is the discourse in the global media, both formal and informal, with foes and their base, allies, “swing voters,” and our own public. This discourse includes not only justifying actions but also containing and managing failures. On the former, work is under way today to formulate rules of engagement for robots designed around Western notions of an ethical practice of war codified in the laws of war. But the collapse of traditional concepts of time and space by new media prevents consideration of information by consumers and reporters. The noble pursuit of “lawfare,” of knowing the truth through careful reflection and analysis to validate Western-justified ends and means, just does not work. Attempting to justify acts based on what can be done according to Western laws actually permits an engagement model that is too permissive and ultimately detrimental to a mission where, as Lieutenant General James Mattis put it, “ideas are more important than [artillery] rounds.” In other words, international law may permit firing into a house with women and children, but the blowback will be significant. Further, if private military contractors are perceived as skirting the laws of war, then the application of those laws to a robot and its human handler (if one exists) is even more unclear.

Without capable information management from the strategic to the tactical level, accidents and failures of unmanned systems will receive harsh treatment in the global media, amplifying an endemic view in the Middle East and elsewhere that the United States commoditizes death. The United States cannot afford technological failures or induced failures (i.e., hacking) that kill civilians. The U.S. military can blame “out-of-control” human contractors, even if they were operating under the rules of engagement set by their government clients, but the principal is absolved from responsibility to a much lesser degree if the agent is a machine. Previous incidents of “technical failure” causing civilian deaths, including the USS Vincennes shutdown of Iran Air Flight 655 in 1988, are examples of a strategic communications apparatus that cannot handle technical failure.

It is essential that the information effects of what we do be considered from the outset, including the impact of information campaigns. Strategic communicators, public diplomats, and information operators must be involved from the inception of unmanned warfare, but they are not. Conversations with proponents of unmanned systems in the Defense Department and think-tanks make it clear the U.S. military has yet to understand that deploying robots to augment the human warfighter is not the same as changing out the M-16 for the M-4 carbine. The uniformed warfighters the robots will replace reflect the country’s commitment to the mission, shaping local and global opinions that garner or destroy support for the mission. Robots, regardless of their real or perceived autonomy, will also represent, reflect, and shape these opinions. The informational effect of robots is substantial, but little research has been done on the subject. Failing to recognize the effect that unmanned systems may have on the struggle for the minds and wills of men and women will have tragic unintended consequences.

[Table of Contents](#)

57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report

By the Security & Defence Agenda (SDA), [MarketWatch](#), 30 Jan 2012

BRUSSELS & WASHINGTON, Jan 30, 2012 (BUSINESS WIRE) -- McAfee and the Security & Defence Agenda (SDA) today revealed the findings from a report; Cyber-security: The Vexed Question of Global Rules that paints, for the first time, a global snapshot of current thinking about the cyber-threat and the measures that should be taken to defend against them, and assesses the way ahead. The SDA, the leading defense and security think-tank in Brussels, interviewed leading global security experts to ensure that findings would offer usable recommendations and actions. The report was created to identify key debate areas and trends and to help to governments and organizations understand how their cyber defense posture compares to those of other countries and organizations.

Here are some noted findings:

- 57% of global experts believe that an arms race is taking place in cyber space.
- 36% believe cyber-security is more important than missile defense.
- 43% identified damage or disruption to critical infrastructure as the greatest single threat posed by cyber-attacks with wide economic consequences (up from 37% in McAfee's 2010 Critical Infrastructure Report).
- 45% of respondents believe that cyber-security is as important as border security.
- The state of cyber-readiness of the United States, Australia, UK, China and Germany all ranked behind smaller countries such as Israel, Sweden and Finland (23 countries ranked in report).

McAfee asked the SDA, as an independent think-tank, to produce the most informed report on global cyber defense available. The SDA had in-depth interviews with some 80 world-leading policy-makers and cyber-security experts in government, business and academia in 27 countries and anonymously surveyed 250 world leaders in 35 countries. As the only specialist security and defense think-tank in Brussels, SDA has become one of the world's leading forums for the discussion of international defense and security policies. The methodology used for rating various countries' state of cyber-readiness is that developed by Robert Lentz, President of Cyber Security Strategies and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. [see here for infographic on rankings]

Top 6 Actions Cited in Report

- Real-time global information sharing required
- Financial incentives for critical improvements in security for both private and public sectors
- Give more power to law enforcement to combat cross-border cyber crime
- Best practice-led international security standards need to be developed
- Diplomatic challenges facing global cyber treaties need to be addressed
- Public awareness campaigns that go beyond current programs to help citizens

Real-time sharing of global intelligence was a core recommendation of the report, citing the building of trust between industry stakeholders by setting up bodies to share information and best practices, like the Common Assurance Maturity Model (CMM) and the Cloud Security Alliance (CSA). "The core problem is that the cyber criminal has greater agility, given large funding streams and no legal boundaries to sharing information, and can thus choreograph well-orchestrated attacks into systems," says Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector, McAfee. "Until we can pool our data and equip our people and machines with intelligence, we are playing chess with only half the pieces."

Experts interviewed also agreed that developments like smart phones and cloud computing mean we are seeing a whole new set of problems linked to inter-connectivity and sovereignty that require new regulations and new thinking. Last year, McAfee issued a Q3 threat report that stated that the total amount of malware targeted at Android devices jumped 76 percent from Q2 of 2010 to Q2 of last year, to become the most attacked mobile operating system.

Other key report findings from the SDA report include the following:

- Need to address expected shortage of cyber workforce: More than half (56%) of the respondents highlight a coming skills shortage.
- Low level of preparedness for cyber attacks: China, Russia, Italy and Poland fall behind Finland, Israel, Sweden, Denmark, Estonia, France, Germany, Netherlands, UK, Spain and the United States.

-- Cyber-security exercises are not receiving strong participation from industry: Although almost everyone believes that exercises are important, only 20% of those surveyed in the private sector have taken part in such exercises.

-- Risk assessment: Prioritize information protection, knowing that no one size fits all. The three key goals that need to be achieved are confidentiality, integration and availability in different doses according to the situation.

-- Balance between security and privacy: Improve attribution capability by selectively reducing anonymity without sacrificing the privacy rights.

While many respondents believed that global treaties were an essential factor in the development of sound policy, some also suggested the establishment of cyber-confidence building measures as alternatives to global treaties, or as a stopgap measure, since treaties are seen as unverifiable, unenforceable and impractical. Stewart Barker, the former Assistant Secretary of Homeland Security under President George W. Bush, stated that treaties "delude western countries into thinking they have some protection against tactics that have been unilaterally abandoned by other treaty signatories."

About the report:

McAfee asked the Security & Defence Agenda (SDA) as an independent think-tank to produce the most extensive report on Cyber Defense. The report stack ranks the degree to which governments are prepared to withstand cyber attacks. This SDA report sets out to reflect the many different views on what cyber-security means, and how to move towards it. To build up a multi-faceted picture of opinion worldwide, SDA interviewed world leaders to highlight what they see as the key issues.

To download "The Cyber Defense Report" report please visit www.mcafee.com/

[Table of Contents](#)

In Battle for Hearts and Minds, Taliban Turn To CDs

By Ahmad Shafi, [NPR](#), January 23, 2012

January 23, 2012 When the Taliban controlled Afghanistan from 1996 to 2001, their hard-line policies included a ban on music tapes and videos.

Yet now, the Taliban are producing their own CDs in an attempt to win the hearts and minds of Afghans.

In bustling downtown Kabul, Mustafa, 22, works in an electronics store selling music CDs to 20-something customers.

But not all of Mustafa's customers are looking for the latest Afghan, Indian or Western pop songs. He says he has customers who only look for Taliban songs — a sort of hypnotic chanting of religious and nationalistic poems unaccompanied by music. He clicks on one the audio files.

In Pashto, one of the two main languages of Afghanistan, the song calls for a holy war against the "infidels." Its says the fight will continue until corruption is wiped out and the Taliban's version of Islamic law is restored.

Mustafa says someone brings him the Taliban CDs that he suspects have probably been downloaded from the Internet. He sells 50 songs for about a dollar.

Since 2005, the Taliban have been mass producing CDs and DVDs featuring footage of alleged NATO atrocities and clips of insurgents battling NATO forces.

The CDs and DVDs are readily available in Kabul and other major cities. In some rural areas, the Taliban operate pirate radio transmitters, with the militants broadcasting warnings to local residents and Afghan government officials.

Taliban Radio Broadcasts

Bilal Sarwary, a BBC reporter, recently visited his native Kunar province, on the border with Pakistan, and heard the Taliban broadcasts on a local radio station.

"They were calling the Afghan National Police national traitors," Sarwary said. "They were naming some people and warning them not to work with the Americans and the Afghan government or else they would be killed."

Sarwary says the Taliban broadcasts referred to the impending withdrawal of NATO troops, scheduled for the end of 2014, as a sign of victory for the insurgents.

"There was a Taliban commentator, and he said, 'Look, conduct however many special forces operations you want, you will not scare the Taliban. NATO is leaving. NATO is losing. NATO cannot fight us.'"

NATO has been using social media sites such as Twitter to try to counter the Taliban's propaganda. However, only a small percentage of Afghans have access to the Internet.

NATO has also been supporting some local radio and TV stations, but the Taliban has also shifted tactics, assassinating radio personalities who oppose them. This month, they killed a prominent tribal leader in Kandahar who used his radio station to preach against the Taliban.

In the battle for psychological advantage, many analysts believe ISAF, the acronym for the US-led NATO mission in Afghanistan, has largely failed to deliver its message.

Candace Rondeaux from the International Crisis Group says the Taliban, on the other hand, has improved its propaganda machine over the years.

"In the meantime, you know ISAF kind of sat silently. Or they frequently put out these sort of propaganda videos or commercials or radio statements that don't really connect with Afghan realities at all," she said.

[Table of Contents](#)

Can U.S. Deter Cyber War?

By Adam Segal, the [Diplomat](#), January 12, 2012

There has been a great deal of thinking and writing about why deterrence is difficult in cyberspace. Attacks can be masked, or routed through another country's networks. And even if you know for sure the attack came from a computer in country X, you can't be sure the government was behind it. All of this creates the attribution problem: It's hard to deter if you can't punish, and you can't punish without knowing who is behind an attack. Moreover, much of the cyber activity is espionage, and it's hard to imagine a government threatening military action for the theft of data.

[China Defense Daily](#) lays out some of the reasons why Chinese experts think deterrence is hard, or to be more specific, why the U.S. military will have difficulty achieving its deterrence aims. First, though, the article addresses all the "advantages" the United States brings to the table: resources (10 of the world's 13 root servers are in the United States); technology (operating systems, databases, processors, microchips, network switching, and other core technology are all "in the hands of American companies"); power (there is a large gap between the United States and others in the development of weapons, investment, the training of talent, and the scale of armed forces).

Despite these strengths, the article sees the U.S. as being unable to secure its networks. The announcement of the Defense Department's [Strategy for Operating in Cyberspace](#), in the Chinese view, encouraged other countries to develop their own offensive capabilities. Attribution is hard, and providing proof of who is behind an attack that would convince others is still extremely difficult. Detection and monitoring capabilities in cyberspace are underdeveloped, so it's a real question whether the U.S. military can detect, provide warning of, and deter an attack before it happens. Finally, if the United States decides to retaliate through offensive cyber attacks, it can have no certainty about the outcomes. The impacts on networks are often limited and can be quickly recovered from.

U.S. intelligence officials are going to AP and The [Wall Street Journal](#) and telling them they have identified the specific Chinese groups behind attacks on Google, RSA, and other companies in an attempt to diminish Chinese confidence that they can remain hidden and, thus, strengthen deterrence. Going further down the hall of mirrors, it may be that the purpose of the article in China Defense Daily is to undermine these U.S. efforts. Can Washington believe that it has achieved a credible deterrent if the potential adversary keeps saying it's not possible?

What deterrence is in cyberspace and how it is achieved is exactly the type of discussion the United States needs to be having with China. This article's use of deterrence (威慑, wei she) is reflective of the Chinese [definition](#), which can be more expansive and normative than the American use, encompassing threat or menace. As far as I can tell, cyber security discussions have only (officially) been happening once a year at the [U.S.-China Strategic and Economic Dialogue](#).

Cyberspaces are of course a strategic and economic issue, so it makes sense to have a whole government approach. Still, given the distance between Washington and Beijing, and the speed at which the issue is developing, the Pentagon and the People's Liberation Army should be speaking as frequently, and in as many fora, as possible.

[Table of Contents](#)

Supremacy in cyberspace: Obama's 'Star Wars'?

By Igor Panarin, [Russia Today](#), 11 January, 2012

US President Obama delivered a public address in the Pentagon on 5 January this year introducing the "defense strategic review." Writer and political analyst Igor Panarin believes Washington's new military doctrine will focus on cyberspace supremacy.

In the article below, Panarin explains his view.-

The United States was first to approach cyberspace as a new sphere of military action, along with the existing military domains such as land, sea, air and space. The concept dates back to 1998, but it was only interpreted into a concrete action plan following the war in South Ossetia in August 2008, which did not play out well for the US and its Georgian proxy.

Late in May 2009, President Barack Obama instituted the post of Cyberspace Coordinator within his administration, with the coordinator sitting on both the National Security Council and the National Economic Council. The same month saw the establishment of the US Cyber Command, headquartered at Fort Meade, Maryland, and headed by Army General Keith Alexander, who also happens to be the head of the National Security Agency, America's most powerful intelligence service.

The National Security Agency/Central Security Service (NSA/CSS) is the United States' centermost intelligence agency. It was formally established on 4 November 1952. The agency is responsible for the collection of foreign communications and signals intelligence, employing the Echelon eavesdropping system as its key technical asset. The NSA performs clandestine surveillance of Russia's electronic communications through Echelon elements stationed in Norway, Cyprus, Kyrgyzstan and the Baltic states.

The US Cyber Command, aka CYBERCOM, plans to employ cyber warfare for purposes of land-based, naval and aerial military operations. Special information and cyber warfare units and command structures have been set up within the US armed forces, including the Army Cyber Command/Second Army. Naval cyber warfare is to be directed through the Fleet Cyber Command, based on the once-disbanded and specially reestablished US 10th Fleet. The air force component of CYBERCOM is the 24th Air Force, aka Air Forces Cyber. The US Marine Corps also has its own Cyberspace Command.

The US Department of Defense's technical research branch, the Defense Advanced Research Projects Agency (DARPA) is currently finalizing its National Cyber Range: a miniature version of the internet meant as a testing ground for cyber intelligence and warfare. The Cyber Range is intended for testing new tactics and techniques through cyber war games, as well as for training cyber troops. The new strategy also includes developing new cyber weapons and tools, such as passive viruses, cyber beacons, etc.

US lawmakers have already developed new legislation regulating government and military activities aimed at securing America's cyberspace supremacy. One of the notable trends is simplified decision making for offensive cyber warfare operations and activities. In the past, launching a cyber attack required stage-by-stage authorization from the Joint Chiefs of Staff, then the defense secretary, and then the US president. Under the new rules, decision making on such an action will take no more than 10 minutes. This primarily concerns psychological operations targeting any specific audience of Internet users.

CYBERCOM held a simulation exercise early in December 2011, which eventually earned praise from Gen. Alexander. The exercise involved 300 cyber specialists designated respectively as CYBERCOM elements and "the enemy," practicing offensive and defensive tactics and coordination. The simulated US cyber defense operation was centered at the Air Force's Nevada Test and Training Range at Nellis, Nevada, while the designated aggressors sought to penetrate the American cyber network from remote locations.

In just over a week, both sides sought to win initiative and counter each other's moves, analyzing their own progress and performance through daily operational briefings. The exercise served to try out various real-time scenarios based on the probable action and counter-action of a potential adversary. DoD officials commended the exercise as highly successful, complementing CYBERCOM specialists for their proficiency and excellent teamwork.

Rather mysteriously, the CYBERCOM exercise took place at the same time as Russia experienced an unprecedented surge in street protests following its parliamentary election last December. It seems rather telling that the protest rallies that drew thousands of people in some of Russia's major cities were mainly organized and dispatched through web-based social networks such as Facebook.

Finally, on 5 January 2012 President Obama and the DoD released a defense strategic guidance titled "Sustaining US Global Leadership: Priorities for 21st-century Defense." The document formulates the United States' top strategic priority as securing the nation's global dominance through aggressive action in

cyberspace. Herein, the White House and the Pentagon explicitly state their intention to enhance America's global posture by securing its domination in cyberspace through information and cyber warfare tactics.

Thus, the Obama administration is laying out its own ambitious global-domination project, superseding Ronald Reagan's "Star Wars" and George Bush Junior's "War on Terror": a global war in cyberspace.

[Table of Contents](#)

Chinese Tech Giant Aids Iran

By Steve Stecklow, Farnaz Fassihi, and Loretta Chao, [Wall Street Journal](#), 27 Oct 2011

When Western companies pulled back from Iran after the government's bloody crackdown on its citizens two years ago, a Chinese telecom giant filled the vacuum.

Huawei Technologies Co. now dominates Iran's government-controlled mobile-phone industry. In doing so, it plays a role in enabling Iran's state security network.

Huawei recently signed a contract to install equipment for a system at Iran's largest mobile-phone operator that allows police to track people based on the locations of their cellphones, according to interviews with telecom employees both in Iran and abroad, and corporate bidding documents reviewed by The Wall Street Journal. It also has provided support for similar services at Iran's second-largest mobile-phone provider. Huawei notes that nearly all countries require police access to cell networks, including the U.S.

Huawei's role in Iran demonstrates the ease with which countries can obtain foreign technology that can be used to stifle dissent through censorship or surveillance. Many of the technologies Huawei supports in Iran—such as location services—are available on Western networks as well. The difference is that, in the hands of repressive regimes, it can be a critical tool in helping to quash dissent.

Last year, Egyptian state security intercepted conversations among pro-democracy activists over Skype using a system provided by a British company. In Libya, agents working for Moammar Gadhafi spied on emails and chat messages using technology from a French firm. Unlike in Egypt and Libya, where the governments this year were overthrown, Iran's sophisticated spying network remains intact.

In Iran, three student activists described in interviews being arrested shortly after turning on their phones. Iran's government didn't respond to requests for comment.

Iran beefed up surveillance of its citizens after a controversial 2009 election spawned the nation's broadest antigovernment uprising in decades. Authorities launched a major crackdown on personal freedom and dissent. More than 6,000 people have been arrested and hundreds remain in jail, according to Iranian human-rights organizations.

This year Huawei made a pitch to Iranian government officials to sell equipment for a mobile news service on Iran's second-largest mobile-phone operator, MTN Irancell. According to a person who attended the meeting, Huawei representatives emphasized that, being from China, they had expertise censoring the news.

The company won the contract and the operator rolled out the service, according to this person. MTN Irancell made no reference to censorship in its announcement about its "mobile newspaper" service. But Iran routinely censors the Internet using sophisticated filtering technology. The Journal reported in June that Iran was planning to create its own domestic Internet to combat Western ideas, culture and influence.

In winning Iranian contracts, Huawei has sometimes partnered with Zaeim Electronic Industries Co., an Iranian electronics firm whose website says its clients include the intelligence and defense ministries, as well as the country's elite special-forces unit, the Islamic Revolutionary Guards Corps. This month the U.S. accused a branch of the Revolutionary Guards of plotting to kill Saudi Arabia's ambassador to the U.S. Iran denies the claim.

Huawei's chief spokesman, Ross Gan, said, "It is our corporate commitment to comply strictly with all U.N. economic sanctions, Chinese regulations and applicable national regulations on export control. We believe our business operations in Iran fully meet all of these relevant regulations."

William Plummer, Huawei's vice president of external affairs in Washington, said the company's location-based-service offerings comply with "global specifications" that require lawful-interception capabilities. "What we're doing in Iran is the same as what we're doing in any market," he said. "Our goal is to enrich people's lives through communications."

Huawei has about 1,000 employees in Iran, according to people familiar with its Iran operations. In an interview in China, a Huawei executive played down the company's activities in Iran's mobile-phone industry, saying its technicians only service Huawei equipment, primarily routers.

But a person familiar with Huawei's Mideast operations says the company's role is considerably greater, and includes a contract for "managed services"—overseeing parts of the network—at MTN Irancell, which is majority owned by the government. During 2009's demonstrations, this person said, Huawei carried out government orders on behalf of its client, MTN Irancell, that MTN and other carriers had received to suspend text messaging and block the Internet phone service, Skype, which is popular among dissidents. Huawei's Mr. Plummer disputed that the company blocked such services.

Huawei, one of the world's top makers of telecom equipment, has been trying to expand in the U.S. It has met resistance because of concerns it could be tied to the Chinese government and military, which the company denies.

Last month the U.S. Commerce Department barred Huawei from participating in the development of a national wireless emergency network for police, fire and medical personnel because of "national security concerns." A Commerce Department official declined to elaborate.

In February, Huawei withdrew its attempt to win U.S. approval for acquiring assets and server technology from 3Leaf Systems Inc. of California, citing opposition by the Committee on Foreign Investment in the United States. The panel reviews U.S. acquisitions by foreign companies that may have national-security implications. Last year, Sprint Nextel Corp. excluded Huawei from a multibillion-dollar contract because of national-security concerns in Washington, according to people familiar with the matter.

Huawei has operated in Iran's telecommunications industry since 1999, according to China's embassy in Tehran. Prior to Iran's political unrest in 2009, Huawei was already a major supplier to Iran's mobile-phone networks, along with Telefon AB L.M. Ericsson and Nokia Siemens Networks, a joint venture between Nokia Corp. and Siemens AG, according to MTN Irancell documents.

Iran's telecom market, which generated an estimated \$9.1 billion in revenue last year, has been growing significantly, especially its mobile-phone business. As of last year, Iran had about 66 million mobile-phone subscribers covering about 70% of the population, according to Pyramid Research in Cambridge, Mass. In contrast, about 36% of Iranians had fixed-line phones.

As a result, mobile phones provide Iran's police network with far more opportunity for monitoring and tracking people. Iranian human-rights organizations outside Iran say there are dozens of documented cases in which dissidents were traced and arrested through the government's ability to track the location of their cellphones.

Many dissidents in Iran believe they are being tracked by their cellphones. Abbas Hakimzadeh, a 27-year-old student activist on a committee that published an article questioning the actions of Iran's president, said he expected to be arrested in late 2009 after several of his friends were jailed. Worried he could be tracked by his mobile phone, he says he turned it off, removed the battery and left Tehran to hide at his father's house in the northeastern city of Mashhad.

A month later, he turned his cellphone back on. Within 24 hours, he says, authorities arrested him at his father's house. "The interrogators were holding my phone records, SMS and emails," he said.

He eventually was released and later fled to Turkey where he is seeking asylum. In interviews with the Journal, two other student activists who were arrested said they also believe authorities found them in hiding via the location of their cellphones.

In early 2009, Siemens disclosed that its joint venture with Nokia, NSN, had provided Iran's largest telecom, government-owned Telecommunications Company of Iran, with a monitoring center capable of intercepting and recording voice calls on its mobile networks. It wasn't capable of location tracking. NSN also had provided network equipment to TCI's mobile-phone operator, as well as MTN Irancell, that permitted interception. Like most countries, Iran requires phone networks to allow police to monitor conversations for crime prevention.

NSN sold its global monitoring-center business in March 2009. The company says it hasn't sought new business in Iran and has established a human-rights policy to reduce the potential for abuse of its products.

A spokesman for Ericsson said it delivered "standard" equipment to Iranian telecom companies until 2008, which included built-in lawful-interception capabilities. "Products can be used in a way that was not the intention of the manufacturer," the spokesman said. He said Ericsson began decreasing its business in Iran as a result of the 2009 political upheaval and now doesn't seek any new contracts.

As NSN and Ericsson pulled back, Huawei's business grew. In August 2009, two months after mass protests began, the website of China's embassy in Tehran reprinted a local article under the headline, "Huawei Plans Takeover of Iran's Telecom Market." The article said the company "has gained the trust and alliance of major governmental and private entities within a short period," and that its clients included "military industries."

The same month the Chinese embassy posted the article, Creativity Software, a British company that specializes in "location-based services," announced it had won a contract to supply a system to MTN Irancell.

"Creativity Software has worked in partnership with Huawei, where they will provide first and second level support to the operator," the company said.

The announcement said the system would enable "Home Zone Billing"—which encourages people to use their cellphones at home (and give up their land lines) by offering low rates—as well as other consumer and business applications that track user locations. In a description of the service, Creativity Software says its technology also enables mobile-phone operators to "comply with lawful-intercept government legislation," which gives police access to communications and location information.

A former telecommunications engineer at MTN Irancell said the company grew more interested in location-based services during the antigovernment protests. He said a team from the government's telecom-monitoring center routinely visited the operator to verify the government had access to people's location data. The engineer said location tracking has expanded greatly since the system first was installed.

An official with Creativity Software confirmed that MTN Irancell is a customer and said the company couldn't comment because of "contractual confidentiality."

A spokesman for MTN Group Ltd., a South African company that owns 49% of the Iranian operator, declined to answer questions, writing in an email, "The majority of MTN Irancell is owned by the government of Iran." He referred questions to the telecommunications regulator, which didn't respond.

In 2008, the Iranian government began soliciting bids for location-based services for the largest mobile operator, TCI's Mobile Communication Co. of Iran, or MCCI. A copy of the bidding requirements, reviewed by the Journal, says the contractor "shall support and deliver offline and real-time lawful interception." It also states that for "public security," the service must allow "tracking a specified phone/subscriber on map."

Ericsson participated in the early stages of the bidding process, a spokesman said. Internal company documents reviewed by the Journal show Ericsson was partnering with an Estonian company, Reach-U, to provide a "security solution" that included "Monitor Security—application for security agencies for locating and tracking suspects."

The Ericsson spokesman says its offering didn't meet the operator's requirements so it dropped out. An executive with Reach-U said, "Yes, we made an offer but this ended nowhere."

One of the ultimate winners: Huawei. According to a Huawei manager in Tehran, the company signed a contract this year to provide equipment for location-based services to MCCI in the south of Iran and is now ramping up hiring for the project.

One local Iranian company Huawei has done considerable business with is Zaeim Electronic Industries. "Zaeim is the security and intelligence wing of every telecom bid," said an engineer who worked on several projects with Zaeim inside the telecom ministry. Internal Ericsson records show that Zaeim was handling the "security part" of the lawful-interception capabilities of the location-based services contract for MCCI.

On its Persian-language website, Zaeim says it launched its telecommunications division in 2000 in partnership with Huawei, and that they have completed 46 telecommunications projects together. It says they now are working on the country's largest fiber-optic transfer network for Iran's telecom ministry, which will enable simultaneous data, voice and video services.

Zaeim's website lists clients including major government branches such as the ministries of intelligence and defense. Also listed are the Revolutionary Guard and the president's office.

Mr. Gan, the Huawei spokesman, said: "We provide Zaeim with commercial public use products and services." Zaeim didn't respond to requests for comment.

[Table of Contents](#)

China Likely to Go Asymmetric if Conflict Breaks out with United States

By Robert K. Ackerman, [SIGNAL Scape](#), 26 Jan 2012

The United States cannot expect to fight on its own terms if it finds itself in an armed conflict with China. The Asian power is likely to resort to unconventional or even asymmetric operations to deny U.S. forces their strong points, offered China experts in a panel at West 2012 in San Diego.

Dr. Alan J. Vick, senior political scientist at Rand Corporation, noted that the recent U.S. conflicts all started at a time and in a manner of U.S. choosing, and this followed a rapid deployment of U.S. forces to forward basing locations. China would not permit that, he said. It would argue that deploying forces to forward bases is an aggressive action, so it would feel free to launch pre-emptive strikes using its newly incorporated tactical ballistic missile strike capability.

Lt. Gen. Wallace Gregson, USMC (Ret.), principal, WC Gregson & Associates, Inc., and former assistant secretary of defense for Asian and Pacific security affairs, warned that the United States should investigate space/counterspace capabilities and cyber. A Chinese cyber weapon can attack from its sanctuary without warning, and it could cripple or shut down essential networks in the United States.

Vick called for new infrastructure investments—base hardening and active defense; long-range strike aircraft and missiles; longer range stealthy cruise missiles; and improved stealthy intelligence, surveillance and intelligence. Gregson said that U.S. forces must learn how to do without their —exquisite communicationsll even they are disabled or modified just a little bit.

Vick pointed out that Chinese and U.S. military forces could confront one another in a number of potential situations, and China is the only country that could do that. Potential flashpoints include Taiwan, the Philippines, and Japan. He added that a North Korean implosion may be more risky than an invasion of the South by the North. China fears that U.S. forces may wind up on their border if the North collapses.

[Table of Contents](#)