

# 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. 04 (FEBRUARY 2012)

1. [9th Annual Army Global Information Operations Conference](#)
2. [China Seeks to Vigorously Develop Battlefield Network Warfare Capacity](#)
3. [The Future of Influence in Warfare](#)
4. [Cloud computing to integrate with current Army system](#)
5. [Report: Army network tests failed to adequately assess mobile operations](#)
6. [Plant DNA Helps the Pentagon Identify Fake Electronic Components](#)
7. [Chinese Communists Influence U.S. Policy Through Ex-Military Officials](#)
8. [Malaysia's Islamic Party Hails Iran's Progress in Electronic Warfare](#)
9. [Is China a Paper Tiger in Cyberspace?](#)
10. [U.S. Could Maintain Virtual Presence in Syria](#)
11. [Battle for Syria Rages across the Internet](#)
12. [Iran – Death for Blogging](#)
13. [A Fatal Tweet](#)
14. [A Primer of Copyright Rules, Regulations, and Risks in Writing for Information Operations Publications](#)
15. [The 50 Ruble Army](#)
16. [Jihadi Information Warfare: The Next Wave](#)
17. [DIA Director Reveals China's Villainous Capabilities In Space](#)
18. [In Attack on Vatican Web Site, a Glimpse of Hackers' Tactics](#)
19. [Anonymous, It Could Become a Cyber Weapon](#)
20. [Report: Internet Radicalizes U.S. Muslims Quickly](#)
21. [When Is A Cyberattack A Matter Of Defense?](#)
22. [Quran Burning a PSYOP Failure in Afghanistan](#)
23. [Psychological Warfare Must Precede Strike on Iran](#)
24. [U.S. Should Not Follow China's Example in Merging Cyber and Electronic Warfare Efforts](#)

## 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 9<sup>th</sup> 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](mailto:scott.janzen@us.army.mil); and Mr. Jose Carrington, 719-554-8880, [jose.carrington@us.army.mil](mailto:jose.carrington@us.army.mil).

[Table of Contents](#)

## China Seeks to Vigorously Develop Battlefield Network Warfare Capacity

Yuan Yi, Peng Moxin, Xu Wenhua; [PLA Daily](#) (via DefPro), 30 January 2012

Currently, the world's military powers are vigorously developing the capacity for battlefield network warfare, and have made a figure in several recent local wars.

On September 6, 2007, Israel adopted the Suter network attack system of the U.S. military and succeeded in escaping from the air defense network that the Syrian armed forces had painstakingly built up for years and destroying Syrian nuclear facilities in the depth, indicating that the network warfare weapons in laboratories have been applied in battlefields with increasingly high degree of practicality and actual combat, and have constituted a substantial threat to such battlefield networks as the command and control network, the reconnaissance and early warning network, the battlefield communication network and the comprehensive support network.

As the battlefield networks play a key supporting role for the entire combat system, it is necessary to be fully aware of the serious impact of the threat upon the combat command and the actions of troop units under informationization conditions and continually strengthen the awareness of the power of controlling the Internet and the awareness of network management, control and protection.

The battlefield network threat is a newly emerging thing in the era of informationization warfare. Some people still have vague ideas for it, and some even confuse the battlefield network threat with the Internet network threat, which just reflects that the current theoretical research on the battlefield network threat is still relatively weak.

Therefore, it is imperative to fundamentally make sense of the connotation, characteristics, regular patterns and other theoretical issues of battlefield network threat, grasp its basic information such as mechanism, origin and type, and thoroughly analyze the impact on tactical and technical performance of weapons and equipment, on combat command, control and coordination, and on commanders' decision and officers and men's mentality when the battlefield network is under cyber attack, thus providing theoretical guidance to military training under the circumstance of battlefield network threat.

We need to actively develop network countermeasure simulation software and equipment, simulation systems that have the effect similar to "blank shell" of removing failure mechanism and retaining infection mechanism, and network countermeasure simulation training systems that have the function of displaying network situation and assessing counterwork result.

We must strengthen network defense construction and depend on large comprehensive training base to create vivid environment with battlefield network threat, thus providing material conditions for military training under the circumstance of battlefield network threat.

We should vigorously launch battlefield network defense training, popularize basic network security knowledge such as flaws, internet virus, Trojan virus and hackers so that officers and men can understand basic theories

of cyber warfare and enhance network security attainment. We should also do a good job in skill training for all kinds of network operational personnel.

We should also enrich the background of battlefield network threat in various military drills, find and remedy flaws and weaknesses of our own battlefield network, and improve our capability of handling emergencies when our battlefield network is attacked, so as to ensure the stability, reliability, security and confidentiality of our battlefield network.

[Table of Contents](#)

## The Future of Influence in Warfare

By Dennis M. Murphy, [Joint Forces Quarterly 64](#), January 2012

### Abstract

Enemies realize the potency of influence and will increasingly bend information to sway both friendly and hostile publics. To prevail in future conflicts, the Nation must not only be more adroit at telling its own story but also predictive about adversary inclinations and methods of using misinformation. We have progressed since 9/11, but the need remains to more fully exploit the tools of influence, especially through focused intelligence support. General Stanley McChrystal called strategic communication vital to securing the operational center of gravity in Afghanistan, which he identified as popular support. There as elsewhere, success comes through changing behavior through influence; thus, Americans must understand the environments they operate in as well as the thinking of enemies and host populations.

Information plays a prominent role in the history of U.S. warfare. From Winfield Scott's courting of the Catholic Church in Veracruz in 1847 to George Creel's Committee on Public Information in World War I, military and civilian leaders have long understood that information, and the influence it produces, can significantly enable the success of military operations. That is no different today. In fact, it is apparent from both current military operations and the environment in which they occur that information and influence as applied to military success will become increasingly important while significantly more complex in the future.

First, consider importance. It seems clear that success in Afghanistan hinges on the ability to change behavior through influence. General Stanley McChrystal's initial assessment of the situation there, published in August 2009, stated, "Strategic Communication makes a vital contribution to the overall effort [battle of perceptions] and more specifically to the operational center of gravity: the continued support of the Afghan population."<sup>1</sup> The transparency of the information environment and increasing access to information through any number of means, from satellite television to the Internet, portend that military operations will not only have the ability to shape the information environment, but also in turn risk being shaped by it.

Next, consider complexity. In a recent *Small Wars Journal* article, Lee Rowland and Steve Tatham, in their presentation on target audience analysis (TAA) and measures of effectiveness, make a strong case that influence operations are a complex business: "TAA— when undertaken properly—is an extremely complex process and whilst its methodology is comparatively simple, its implementation is most certainly not."<sup>2</sup> A discussion of the human behavior model in an article published in early 2010 in *Parameters* concludes the same: "A deep understanding of the human behavior model, specifically culture and how it informs emotion, is critical to obtaining behavior change that is driven by perception and attitude."<sup>3</sup> Noted communication researcher Steven Corman joins the chorus when he describes a shift in academic thought on influence from one of "simplistic . . . to pragmatic complexity."<sup>4</sup>

The U.S. Government, and the military in particular, has gradually recognized the value and urgency of information to affect national security since the attacks of September 11, 2001. Significant debate since then has informed the evolution and viability of concepts such as information operations (IO), strategic communications (SC), and public diplomacy.<sup>5</sup> In fact, the military has moved beyond the apprentice stage to what could arguably be termed journeyman status as it relates to applying information to enable achievement of its objectives. But the importance and complexity of future influence operations will require master status. The U.S. military will achieve such mastery by getting its doctrine right; by building its intelligence capability to focus on enemy use of information as a weapon of choice; and, most importantly, by creating an organizational culture that embraces the criticality of using information to influence across the spectrum of future conflict.

### Getting Doctrine Right

The concepts of IO and SC (the primary military influence processes) and their application have evolved in fits and starts over the past 10 years. Much debate in the midst of conflict has surrounded the meaning of these terms, the similarities and differences between them, and the responsibilities for each beyond theory and in practice.<sup>6</sup> Add to this the recent emergence of cyberspace operations, and the confusion is understandable.

Still, progress, while appearing glacial to many, is occurring. A new and clearer definition of information operations has been approved by the Department of Defense. A "Strategic Communication Capabilities Based Assessment" has been completed.<sup>7</sup> Both of these efforts will lead to military doctrinal publications and directives that afford the opportunity to provide clarity and, more importantly, move these concepts to an understanding that enables mastery of the craft of applying information in order to influence.

An example of progress was reflected in the theme of the 2010 Worldwide Information Operations Conference: "Mainstreaming Information Operations, Normalizing Doctrine and Operations."<sup>8</sup> In other words, how do you take IO out of the ether, where it appears as a new, bright, shiny object, and place it squarely into the realm of routine and recurring military operations? The same challenge exists for strategic communications and cyberspace operations. The answer to that question lies squarely in getting the doctrine right. In fact, if the military does not get the next iteration of influence-related doctrine correct over the next 2 years, the progress previously described will be significantly muted.

Doctrine is what drives the conduct of military operations. It is guidance that (as noted on the inside cover of all joint doctrine publications) "is authoritative [and] as such will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise."<sup>9</sup> Once doctrine is written and codified, Soldiers, Sailors, Marines, and Airmen read it and follow it. It becomes "truth." Given that this is the case, defining the correct audience for the doctrine is critical since the future of information in warfare should focus on movement to mastery of the concept. One may understandably default to the influence practitioner as the obvious audience for this doctrine. But the most important audience is the commander. The progress previously described is reflective of IO or SC staffs who really understand how to achieve effects in the information environment after 10 years of practice in war. What is lacking, however, are commanders who understand the concept sufficiently to provide appropriate guidance, resources, and advocacy for those same IO staffs, which makes all the difference in the world.<sup>10</sup>

First, the focus of commander-oriented doctrine must be on information effects, not IO or SC. Both are integrating processes that are often misunderstood and confused with the individual capabilities that they integrate. Adding further confusion are related processes and capabilities like the newly minted cyberspace operations. Information effects, on the other hand, are clearly understood by commanders. Effect is a doctrinally accepted term, a part of operational design.<sup>11</sup> Commanders know that they must achieve information effects to enable achievement of military objectives. However, they may not understand the nuances of IO or the other related but different concepts. In general, doctrine focused on information effects must be incorporated into the currently understood areas of operational art, design, and science.

Second, IO, SC, and cyberspace operations are still terms that will be used. This proposed doctrine need not go into excruciating detail about the specific staff processes that they portend, but it must describe the relationship between them.

Some specific examples of what this doctrine should include are worthy of discussion. First, and arguably foremost, is the importance of considering influence in the development of commander's intent. Commander's intent drives both the planning and execution of military operations. It defines command ownership of the operation. A commander's intent that includes a desired information endstate (a defined attitude or behavior change for critical audiences at the conclusion of the operation) will drive the military course of action development, analysis, and selection. That is, the military actions will be undertaken in a fashion to achieve the standard operational endstate in a way that also allows the desired information-effect endstate to be achieved. Branch planning should also be considered in terms of influence. Branch plans answer the question, "What if?" Given that our enemies routinely use influence to enable success, we should plan for an immediate response to their influence operations through branch planning in order to minimize our reaction time. Additionally, it is important to do a side-by-side comparison of the operational art, design, and science aspects of kinetic operations as compared to influence operations. This should clearly point out the requirement for an information endstate (the art), resources necessary for understanding the complexity of both human behavior and measuring influence effectiveness (the science), and the long-term nature of achieving influence effects (the design).

When the Joint Publication Information Effects in Joint Military Operations is available, it will go a long way toward normalizing future influence operations. It buys informed and educated commanders. That in turn makes the life of the influence staff easier since the commander can now provide appropriate guidance, resources, and advocacy. And that moves information in warfare to a level of mastery not previously seen or practiced. Still, that mastery requires an acute understanding of the enemy, who chooses to vote routinely with information effects as his asymmetric weapon of choice.

## **Know Thine Enemy**

In the apprentice stage of employing influence operations, the commander and staff are proactive in considering the information environment and the required information effects in the planning process. Counterinsurgency, as a population-centric military operation, has driven commanders, over time, to focus on information effects during planning in both Iraq and Afghanistan.

In the journeyman stage, the commander and staff both plan to achieve their own information effects and quickly shift to being “proactively reactive” regarding unpredictable circumstances in the information environment. That is, consideration is also given in the planning process to the fact that unforeseen situations can, and often do, occur that have potentially adverse information effects on coalition forces. (Collateral damage, Abu Ghraib photos, and staged enemy disinformation come to mind.) Recognizing this, the commander and staff develop processes to immediately react to those instances if and when they occur. Information playbooks and battle drills are examples that are prepared to plan for the unforeseen but expected information wildcard as a result of branch planning.<sup>12</sup>

But in order to achieve mastery in influence operations, one must move from being proactively reactive to becoming predictive. This is a critical task, and certainly not an easy one since it speaks to the complexity of the information environment. Consider the importance of being able to predict an information effect planned by the enemy versus reacting to an unanticipated information wildcard employed by the enemy. Rowland and Tatham note that “an unintended incident . . . will have an immediate information effect on [the] target audience and a much slower return to below stasis.”<sup>13</sup> In other words, even if coalition forces are doing a good job achieving planned and intended information effects, the unexpected incident not only adversely impacts operations for the short term, but also never allows a return to the effects achieved before the incident. (One step forward, two steps back.)

So, how does one become predictive in order to cut the legs out from under enemy information effects? The answer lies in the often-overlooked but long-term Achilles’ heel of influence operations: intelligence support. A highly publicized report coauthored by Major General Michael T. Flynn, the North Atlantic Treaty Organization intelligence director in Afghanistan, points out current intelligence flaws: “Our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade.”<sup>14</sup> Only when the Intelligence Community develops the skill sets, a pipeline of experts, and, most importantly, organizational focus toward influence operations will coalition forces have a chance of being predictive regarding enemy use of information. The enemy has a well-established modus operandi (MO) using information as his strategic weapon of choice. In fact, American-born-turned-enemy propagandist Zachary Chesser recently made that MO rather simple to understand by laying out the 10 most effective ways to conduct enemy influence operations.<sup>15</sup> That is not to say that predictive information analysis is always easy. As previously noted, intelligence based on the human behavior model, social psychology, cultural anthropology, and emotion is inherently difficult. But intelligence-gathering and analysis focused on both open sources and traditional and more complex sources will move friendly influence operations from proactively reactive and allow the possibility of being predictive and proactively disruptive before the fact.

The shifts to commander-focused information effects doctrine and intelligence focus on enemy influence operations work hand-in-hand toward forcing a change in organizational culture in support of fully integrated planning and execution of influence operations.

### **Organizational Culture**

In 2009, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen stated, “We have allowed strategic communication to become a thing instead of a process, an abstract thought instead of a way of thinking.”<sup>16</sup> It is this inherent “way of thinking” that defines the organizational culture of the U.S. military today, and in terms of wielding influence through SC, Admiral Mullen sees a basic f law. This is not surprising since researchers note that organizational culture changes in a fairly slow, evolutionary manner.<sup>17</sup> What commander-centric information doctrine and intelligence support to information effects provide, however, are forcing functions to drive an organizational culture that embraces information effects as an inherent part of military planning and execution.

Within military organizations, the commander sets the tone, establishes the command climate, and drives the organizational culture. A commander who embraces and emphasizes the value of information effects to military success will drive the unit to a similar recognition. Doctrine that focuses on and directs commanders to provide initial guidance on desired information effects will result in planning and execution reflective of organizational change. A commander who identifies an information endstate in his intent implies to the staff and subordinates that information effects are important to mission success and must be considered throughout the planning, execution, and assessment processes.

Intelligence support follows this commander-driven change. With an information endstate defined, the intelligence staff determines most likely and most dangerous enemy influence courses of action. The staff then wargames against these scenarios and, in doing so, increases the opportunity to both predict the enemy's use of information and plan to prevent it from ever occurring.

Other standard military decisionmaking processes will follow with a routine consideration of influence on mission accomplishment. Priority Intelligence Requirements will necessarily consider collecting on the environmental factors that portend enemy influence operations. The Commander's Critical Information Requirements will raise time-sensitive influence activities to the commander's level for action, both to exploit friendly effects and blunt enemy effects.

Commander-centric doctrine on information effects, accompanied by intelligence support enabled by appropriate resources and focus on enemy influence activities, will drive organizational culture. If and when that occurs, the military will be well on its way to mastery in planning and executing influence operations and deterring and defeating the primary source of enemy power.

The information environment is a complex system that will become increasingly important to the success or failure of military operations in the future. Progress has been made since 9/11 to both exploit information effects to enable success and to counter enemy asymmetric use of information as a strategic weapon of choice. But the criticality of information as power in future warfare means that if the U.S. military hopes to routinely succeed, it must master influence operations across the spectrum of operations. Commander-centric doctrine will help jump-start that mastery by allowing the commander to provide the appropriate and necessary guidance, resources, and advocacy to influence operations. Intelligence support must simultaneously shift focus from kinetic order-of-battle analysis to a balanced approach that considers collection and analysis of influence-related enemy capabilities as well.

As this command-directed and -focused planning and execution evolve, they will trickle down to the individual Soldier, Sailor, Marine, and Airman. When they inherently and proactively consider any and all of their actions in light of their influence effects, inculcation of the organizational culture toward and true mastery of influence operations will be achieved. In a world where information is ubiquitous and increasingly impacts military success, that cannot happen soon enough. JFQ

---

## Notes

1. Stanley A. McChrystal, Headquarters, International Security Assistance Force Memorandum, "COMISAF's Initial Assessment," Kabul, Afghanistan, August 30, 2009, D-1.
2. Lee Rowland and Steve Tatham, "Strategic Communication and Influence Operations: Do We Really Get 'It'?" Small Wars Journal, August 3, 2010, available at <<http://smallwarsjournal.com/blog/journal/docs-temp/483-tathamrowland.pdf>>.
3. Dennis M. Murphy, "In Search of the Art and Science of Strategic Communication," Parameters 34, no. 4 (Winter 2009/2010), 111.
4. Steven R. Corman, Angela Trethewey, and Bud Goodall, "A 21st Century Model for Communication in the Global War of Ideas," Consortium for Strategic Communication, Report #0701, April 3, 2007, 9.
5. Information operations, strategic communications, and public diplomacy are related concepts that all in some way focus on informing, educating, and influencing audiences. Still, their nuanced differences remain difficult for the nonpractitioner to grasp, as evidenced by a U.S. Department of Defense front-end analysis in summer 2010, examining the lexicon and definitions of information operations and strategic communication, among others.
6. See Dennis M. Murphy, "The Trouble with Strategic Communication(s)," IOSphere (Winter 2008) for a detailed explanation of the lexicon and comparison of the terms information operations (IO) and strategic communication (SC).
7. The new definition of IO is an outcome of the Department of Defense front-end analysis (see note 5). The "Strategic Communication Capabilities Based Assessment" was conducted by U.S. Strategic Command during 2009-2010 and considered SC from doctrinal, personnel, and organizational perspectives, among other considerations.
8. The Worldwide Information Operations Conference is an annual event bringing together an international audience of approximately 500 IO practitioners, academics, and contractors to focus on both the progress and future of IO.
9. See Joint Chiefs of Staff, Joint Publication 3-13, Information Operations (Washington, DC: Joint Chiefs of Staff, February 13, 2006), i, among others.
10. The author has taught on the topics of IO and SC at the U.S. Army War College for the past 6 years. Over that period, senior military leader-students have increasingly recognized the importance of information effects to warfighting success. However, they anecdotally offer that even with successive tours of duty in combat zones, it takes an initial 4 months, on average, for commanders to put into place effective tactics, techniques, and procedures to compete in the information environment.
11. Joint Chiefs of Staff, Joint Publication 5-0, Joint Operation Planning (Washington, DC: Joint Chiefs of Staff, August 11, 2011), III-18.
12. Again, this should be planned using current military paradigms. In this example, branch planning is the appropriate mechanism. A branch answers the question "What if?" in military plans. See Joint Publication 5-0, II-18.
13. Rowland and Tatham, 6.
14. Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security Working Paper, January 4, 2010.
15. Jared Brachman, "The Internet Jihad," Foreign Policy, available at <[www.foreignpolicy.com/articles/2010/10/11/the\\_internet\\_jihad](http://www.foreignpolicy.com/articles/2010/10/11/the_internet_jihad)>.

16. Michael G. Mullen, "Strategic Communication: Getting Back to Basics," Joint Force Quarterly 55 (4th Quarter 2009), 2.
17. Christine A.R. MacNulty, Transformation from the Outside In or the Inside Out (Carlisle, PA: U.S. Army War College Center for Strategic Leadership, 2008), 22.

-----  
About the Author

Professor Dennis M. Murphy serves as the Director of the Information in Warfare Group in the [Center for Strategic Leadership](#) at the U.S. Army War College.

[Table of Contents](#)

## Cloud computing to integrate with current Army system

By Kristen Kushiyama, [CERDEC](#), February 1, 2012

ABERDEEN PROVING GROUND, Md. (Feb. 1, 2012) -- The U.S. Army's Research, Development and Engineering Command's communications-electronics center, or CERDEC, hosted an Industry Day Jan. 10-12, to inform potential technology development partners of new capabilities that support Army cloud computing development efforts and hear what potential partners could contribute to those efforts.

The CERDEC Intelligence and Information Warfare Directorate's Tactical Cloud Integration Laboratory, or I2WD TCIL, focuses on developing and integrating new capabilities by "bridging" developers, vendors and solutions with operational users in a cohesive, isolated environment, said Kesny Parent, CERDEC I2WD TCIL Program Management Office.

"PM DCGS-A (Program Manager Distributed Common Ground System-Army) has identified the need to establish operational clouds at fixed sites and at regional nodes to support Army intelligence data collection and analytics capabilities," said Parent.

In order to fulfill that need, CERDEC I2WD asked industry, academia and other government organizations to submit proposals for capabilities such as multi-intelligence, all-source analysis correlation; platform and resource allocation and optimization algorithms, predictive analysis tools; language translation services; still image and graphic processing capabilities; advanced human intelligence exploitation; and advanced visualization and conceptualization tools.

All proposals were to assist in an effort to establish an infrastructure that supports the storage and management of multi-intelligence data and provides a computational framework that brings analytics to that data.

CERDEC and PM DCGS-A, an entity of Program Executive Office Intelligence Electronic Warfare & Sensors, added another day to the original two-day event to accommodate 48 respondents, said Michael Hinman, system engineer technical assistant and TCIL support Project Manager.

"We are being open and accommodating, because the proposals can be interesting," said Hinman.

Not only did potential government contractors have the opportunity to present possible solutions to the Army's cloud computing gaps, but the event gave government personnel the chance to tell industry where the Army's focus is related to current and future forces, said Mark Kitz, technical director of PM DCGS-A.

Developing cloud technology is important to the intelligence community as a component of DCGS-A, which is the Army's core intelligence, surveillance and reconnaissance enterprise system, said Kitz.

"It uses the latest in cloud technology to rapidly gather, collaborate and share intelligence data from multiple sources to deliver a common operating picture. DCGS-A is able to rapidly adapt to changing operational environments by leveraging an iterative development model and open architecture allowing for collaboration with multiple government, industry and academic partners," said Kitz.

As part of cloud technology advancements for DCGS-A, CERDEC I2WD was chosen to host the TCIL because of the organization's expertise in science and technology for the intelligence community, which made for a natural partnership from a PEO perspective, said Kitz.

"The timeline for TCIL is driven by maturity. This Industry Day is the initial opportunity, and we would like to do yearly engagements to perform an assessment of industry and communicate where we would like to see resource go to solve problems," said Kitz.

The intent of TCIL is to have neutral ground and a government proponent for vetting technologies and having an independent, government assessment of capabilities, said Upesh Patel, CERDEC I2WD TCIL technical director.

The ultimate objective is to get technology out to Soldiers by maturing the capabilities and getting it to the DCGS Standard Cloud, said Patel.

"This is a continuous process evolving over time, not a one shot deal. Requirements change and involve user driven- mission input," said Patel.

[Table of Contents](#)

## **Report: Army network tests failed to adequately assess mobile operations**

By Bob Brewin, [NextGov](#), 02/03/2012

Large-scale Army battlefield network tests last summer did not include mobile operation scenarios and did not feature robust attacks against the networks, the Defense Department's test organization said in its annual report to Congress.

The ambitious six-week Army network integration evaluation at White Sands Missile Range, N.M., last summer, which had 3,800 soldiers from the 1st Armored Division's 2nd Brigade Combat Team put battlefield systems through their paces, cost \$67 million, or roughly six times more than previous tests. The benefits from the larger tests remain unclear, said Michael Gilmore, the Defense Department's director of operational test and evaluation, in his annual test report submitted to Congress in January.

The report said the Army tested 25 experimental systems in the summer of 2011, the expense of which stressed the service's evaluation capacity.

In addition, the Army should develop operational scenarios in future evaluations, the report said. Last summer, brigade and battalion tactical operations centers and company command posts operated from fixed sites and were dependent on a fixed-aerial tier of 100-foot towers and aerostats to establish network connectivity.

In future tests, the Army should place a greater emphasis on scenarios that require commands to move around the battlefield and establish and maintain mobile, ad hoc networks. "Both of these are desired Army network characteristics that have not been demonstrated to date," the report said.

And while the summer 2011 evaluation did involve tests of electronic warfare and computer attacks, the report said future tests should include a "robust information operations opposing force."

Paul Mehney, a spokesman for the Army system of systems integration directorate, said in an email that the service cut the number of systems it plans to evaluate at another network integration evaluation this spring, which in turn will reduce overall test costs.

The May 2012 evaluation also will focus on mission command-on-the-move capability and include a large number of mobile communication equipment, including systems in the aerial tier, routers and multichannel radios. More than one third of the testing priorities will concentrate on mobile operations and soldier connectivity, Mehney said.

[Table of Contents](#)

## **Plant DNA Helps the Pentagon Identify Fake Electronic Components**

From Our Bureau, [DefenseWorld.net](#), Feb 8, 2012

Fake components have been used to build U.S. submarines, missile defense system and aircrafts such as the Boeing C-17 and the Lockheed Martin C-130J "Super Hercules". The Pentagon has now turned to plant DNA to help identify fake electronic components with a high success rate.

According to a 2011 report by the US Senate Armed Services Committee, 1800 cases were found in which the Pentagon had acquired counterfeit electronics. To combat the rising number of counterfeits, the Pentagon along with Applied DNA Sciences have taken to imprinting weapons, micro chips with plant DNA to help weed out fakes.

SigNature DNA, as the new tech is called, is being used by the U.S. Department of Defense to authenticate microchips headed for the military supply chain.

"Our mark is simple and portable, can be scanned at any node in the supply chain, and if suspected, a part can be submitted for forensic examination in a lab, just as law enforcement can legally ID people using DNA", said Dr Jim Hayward, CEO of ADNAS.

Since the pilot testing began 18 months ago, ADNAS has marked upwards of 20,000 chips so far, in live process tests in the factories and assembly venues, with an authentication success rate of 100%, so far.

This also means bad news for contractors who sell fakes to the Pentagon, according to the Levin-McCain Amendment contractors who supply counterfeit material will be held responsible and thus punishable.

In seven out of 10 cases, the fake parts originated in China where microchips are often smuggled out of factories, or burned off old computer circuit boards before having their identifying marks sanded off and repainted as new.

In Chinese bazaars, "military grade" microchips are openly advertised, although these chips are often commercial chips that have been modified and relabeled.

The problem, however, is not new. During the Clinton Administration, the Pentagon has been buying "off-the-shelf" electronics, rather than designing its own systems in an effort to cut costs.

[Table of Contents](#)

## **Chinese Communists Influence U.S. Policy Through Ex-Military Officials**

By Bill Gertz, [Free Beacon](#), 6 Feb 2012

China's intelligence services are using a private exchange program for retired U.S. and Chinese generals to influence the U.S. government and downplay Beijing's large-scale military buildup, according to a congressional report.

The Sanya Initiative launched in 2008 with support from retired Adm. Bill Owens, a former vice chairman of the Joint Chiefs of Staff, and the China Association for International Friendly Contact (CAIFC), a Chinese military front organization, the report said.

"Institutions and persons affiliated with [People's Liberation Army] military intelligence entities play a prominent role in the Sanya Initiative," the report by Congress' U.S.-China Economic and Security Review Commission [1] said.

The intelligence and influence effort was outlined in a late draft of the commission's 2011 annual report. However, the section containing details of the intelligence links was left out of the commission's final report [2] made public in November.

A U.S. official said the passage's deletion occurred because some of Sanya's U.S. participants and senior commission members were concerned about portraying the exchange program negatively. The Washington Free Beacon obtained a copy of the omitted material.

William Reinsch, China commission chairman for the 2011 cycle, did not disclose why the material was excised. In an email he wrote, "While I supported the action taken, I was neither the lead nor sole proponent of it."

According to the report, "the leading Chinese figure in the PLA delegations participating in the first two rounds of Sanya Initiative dialogues was retired Gen. Xiong Guangkai, the former deputy chief of the PLA general staff who was director of PLA Intelligence."

Xiong "has remained active in public affairs since his retirement in 2007, serving as chairman of the Chinese Institute of International Strategic Studies, a think tank directly affiliated with PLA intelligence," the report said.

### **PLA uses retired military for influence**

The PLA influence operation used the retired military officers to convey Chinese propaganda and policy messages to Congress and the Pentagon, including during meetings in 2009 with then-Chairman of the Joint Chiefs of Staff Adm. Mike Mullen, briefings to the Pentagon's advisory Defense Policy Board, and lobbying against the annual Pentagon report on China's military.

The Chinese sponsor of Sanya, CAIFC, worked closely with the Chinese military's Foreign Affairs Office "to raise the idea and secure the necessary approvals" for the exchange program.

"While nominally a civic organization promoting international exchanges, the China Association for International Friendly Contact is actually a front organization for the International Liaison Department of the PLA General Political Department," the report said.

According to the report, the PLA uses CAIFC as a cover name for carrying out "ideological and political work on foreign armies, [to] explain China's policies, and [to] disintegrate enemy armies by dampening their morale."

The report also said the Chinese sponsor of Sanya "is linked to the Intelligence Bureau of the Liaison Department of the PLA's General Political Department ... [with additional] ties to both the Ministry of State Security and the Ministry of Foreign Affairs." The Ministry of State Security is China's civilian intelligence service. The Liaison Department of the PLA is in charge of "conducting propaganda and psychological operations directed at other militaries."

"The Liaison Department conducts its perception management operations in accordance with centrally determined [Chinese Communist Party] propaganda messages," the report said, quoting a Defense Intelligence Agency analyst as saying that propaganda programs are implemented through PLA public and intelligence channels under the direction of political commissars.

In 2009 the office of the Director of National Intelligence identified the Chinese liaison office as a "major collector" of intelligence against U.S. interests, the report said.

Larry Wortzel, a U.S.-China Economic and Security Review Commission member, told the Free Beacon that the Chinese military skillfully uses political and intelligence units to cultivate relationships with retired U.S. and other foreign military officers.

"One way it has done this is by using the China Association for International Friendly Contact," he said. "Its programs have sought to invite retired US officers to China as well as to cultivate representatives of U.S. defense industries. My experience in contact with groups brought to China by CAIFC shows that often the U.S. visitors are offered business or partnership opportunities in China."

Kenneth E. deGraffenreid, formerly a senior U.S. counterintelligence policymaker, said in an interview that the retired officers' effort highlights the Chinese government's roots in the communist movement. "Subversion-the technical term-is their foremost stock in trade," he said. "The regimes of this movement employ a number of political warfare/influence operation techniques which mislead the West because they are used as weapons, not as a means of cooperative relations."

Western states regard exchanges and meetings as part of free, informed, open discussions while the Chinese regard them as part of a political warfare struggle, he said.

"Many in the West have been, and are being yet again, duped just as they were when the PRC and the late Soviets used them in the 20th century," Mr. deGraffenreid said, noting that the FBI has been "gun shy" in using its counterintelligence operations to halt the activities as a result of poor counter-spying and strong political reactions from the pro-China lobby in the United States.

"The role of PRC military intelligence entities in the Sanya exchanges, and the consistency of messages from the Chinese participants with official PRC narratives, both strongly suggest that the Chinese government has intended the exchanges as a channel for communicating to the U.S. policy community the [Chinese Communist Party's] preferred narratives on national security issues," the report said.

Owens was quoted in the report as saying a central goal of Sanya is to "convey accurate and relevant information to key decision makers and national leaders in China and [the United States]," the report said.

"U.S. participants in the Sanya Initiative have made a number of proposals and recommendations on U.S.-China policy that closely parallel themes emerging from their meetings with PLA counterparts," the report said.

For example, Owens told a conference in Washington in 2008 that China's policy was peaceful; that China did not seek to be a superpower; and that "China's intentions toward its neighbors are peaceful and neither irredentist or hegemonic." All those themes have been identified as Chinese propaganda messages.

Retired Air Force Gen. Ronald Fogleman, a former Air Force chief of staff, was also identified as a Sanya participant who echoed PLA propaganda themes at the same meeting. Fogleman "warned that the United States risked making China into an adversary through the U.S.'s own actions," the report said.

The report said Owens also has repeated China policy themes in op-ed articles in newspapers, and in one called for the United States to review the 1979 Taiwan Relations Act because it is the basis for selling arms to Taiwan and "is not in our best interest."

China's government and military has said repeatedly that the United States must not sell arms to Taiwan, which the Chinese regard independent as a breakaway province.

The Sanya Initiative has also targeted the annual Pentagon report to Congress on China's military, a report frequently criticized by the PRC as an exaggeration of China's military intentions. The congressional report stated that U.S. members of Sanya were "asked by their PLA counterparts ... to use their influence to press for a delay in the publication of the Pentagon's 'Military Power of the People's Republic of China' report to Congress." It said Fogelman had contacted U.S. government officials to propose this but was not successful.

Congress changed the name of the annual Pentagon report from the "Military Power of the People's Republic of China," to the "Military and Security Developments Involving the People's Republic of China," in 2010, however. Some congressional aides said this was an effort by Congress to soften the report.

## **Initiative launched in 2008**

Sanya launched in February 2008 after Owens and CAIFC hosted a series of meetings in Beijing and the city of Sanya on Hainan Island in the South China Sea.

In addition to Owens and Fogleman, U.S. participants have included retired Army Gen. John M. Keane, former Army vice chief of staff, and retired Marine Corps Gen. General Charles E. Wilhelm, former commander of U.S. Southern Command. Chinese participants have included Xiong and four other retired PLA generals.

A 2008 report produced by Sanya listed "key outcomes" of the first meeting. Included on the list was that "American and Chinese Generals agree that they are in an excellent position to convey information to key decision makers and national leaders."

According to Sanya report, "all four American generals have already begun to discuss writing op-ed pieces to provide a counterpoint to the current writing about China's military, for example that of Bill Gertz...."

Owens, since retiring from the military, has been engaged in business in China, where government connections with Chinese leaders is considered essential to success.

A spokeswoman for Owens had no immediate comment. However, last year he responded to written questions, saying that he started Sanya based on his belief that the initiative would serve U.S. interests for retired U.S. and Chinese generals to meet once a year for discussions about military relations.

"This project has the full knowledge and support of senior government officials, and the work that I do has been conducted in close consultation with the U.S. Embassy and policy makers in Washington," Owens said. "It has been undertaken with clear attention to America's security and best interests."

Regarding his contacts with Xiong, the former PLA intelligence chief, Owens said the retired Chinese general was his counterpart for the first two Sanya meetings and is no longer involved.

"Regarding the Pentagon's annual report on China's military build-up, the Chinese raised it in the first Sanya Initiative meeting two years ago, but I have never worked on my own or with the Sanya Initiative to lobby Congress or the executive branch to change this report," he said.

Asked about reports that he had earned as much as \$100 million through investments and businesses based in Hong Kong, Owens declined to comment on his personal finances.

Fogleman and Wilhelm could not be reached for comment and Keane said he has not been associated with the group since 2008.

Other Sanya participants have included retired Adm. Joseph Prueher, a former U.S. Pacific Command commander and former ambassador to China, and retired Adm. Timothy Keating, another former Pacific Command leader, according to the report.

Prueher headed an academic commission on China at the University of Virginia that produced a report in April 2011 that sought to play down the threat emanating from China's development, the report said.

That commission's recommendations closely aligned with Chinese propaganda from the Sanya program on Taiwan in opposing U.S. arms sales to Taiwan and reviewing U.S. policy on the transfers, according to the U.S.-China Economic and Security Review Commission's report.

The congressional report said Prueher's commission played down "the Communist identity of China's ruling party-a staple of PRC messages to foreign audiences" and made the questionable assertion that "it is accurate for Americans to view and interpret China as 'Chinese' rather than as 'Communist,' as they are pragmatically, rather than philosophically, driven."

The Sanya group met in 2008 in China, in 2009 in Hawaii, New York, and Washington, and in Beijing in 2010. The 2010 session was hosted by Chinese Gen. Xu Caihou, vice chairman of the Chinese Central Military Commission, China's highest organ of power, and by Gen. Liu Zhenqi, deputy director of the PLA General Political Department.

The report said that during the meeting Xu called on the United States to "'to respect and accommodate China's core interests and major concerns' in order to further bilateral military ties."

The Pentagon has tried for the past decade to develop closer military relations with the PLA. But China's military continues to view the Pentagon as its main enemy and relations and exchanges have been stymied. Beijing cut off the military exchanges twice in recent years to protest U.S. arms sales to Taiwan.

The report also asserted that the United States is wrong to seek a democratic government in China because "a complete democracy is not necessarily the best model for the Chinese at this time."

[Table of Contents](#)

## Malaysia's Islamic Party Hails Iran's Progress in Electronic Warfare

From [FARS News Agency](#), 8 Feb 2012

TEHRAN (FNA)- Malaysia's Islamic Party appreciated the Iranian scientists and engineers for their great achievements in aerospace and electronic warfare, calling it a challenge to the US.

Pointing to the launching of Navid satellite by Iran, Malaysia's Islamic Party website noted that the Islamic Republic managed to develop its own spaceship and thus challenge the US monopoly of space technologies.

It reiterated that the satellite is fully designed and engineered by the Iranian scientists and experts.

It further said that Iran's achievements are not limited only to space technology but rather the country has managed to make remarkable progress in electronic war as well.

Iran on Friday successfully launched the 'Navid-e Elm-o Sana'at' satellite into the orbit.

The satellite was sent to space following a decree by Iranian President Mahmoud Ahmadinejad on Friday morning via videoconference.

Foreign Minister Ali Akbar Salehi, Minister of Science, Research and Technology Kamran Daneshjou and Head of State Spatial Organization Hamid Fazeli attended the control panel for the launch of the satellite.

The satellite, which is completely designed and built by Iranian experts, was blasted into orbit on the occasion of the 10-Day Dawn celebrations, marking the 33rd anniversary of the victory of Iran's Islamic Revolution in 1979.

The 50-kilogram orbiter lifted off into space with an orbital angle of 55 degrees on the Iranian-made Safir satellite-carrier.

Head of Iran Space Agency (ISA) Hamid Fazeli said the domestically-built Navid satellite will circle the Earth at altitudes between 250 and 370 kilometers.

Navid-e Elm-o Sana'at is a telecom, measurement and scientific satellite whose records could be used in a wide range of fields.

Iran has already sent small animals into space - a rat, turtles and worms - aboard a capsule carried by its Kavoshgar-3 rocket in 2010.

The Islamic republic, which first put a satellite into orbit in 2009, has outlined an ambitious space program and has, thus far, made giant progress in the field despite western sanctions and pressures against its advancement

[Table of Contents](#)

## Is China a Paper Tiger in Cyberspace?

By Adam Segal, [Council of Foreign Relations](#), February 8, 2012

Two recent studies of national cyber power have placed China near the bottom of the table. China is [number 13](#) on the EUI-Booz Allen Hamilton Cyber Power Index, behind Argentina, Mexico, and Brazil but better off than Russia, Turkey, South Africa, and India (the United Kingdom, United States, and Australia are the top three). The Brussels-based [Security & Defence Agenda](#) groups [China with Italy, Russia, and Poland](#) in the fifth tier (the U.S. and the UK are in the third tier, below Finland, Sweden, and Israel; the top group is empty).

These are very subjective studies based on interviews, surveys, and vague metrics. Still, they cut against the grain of popular perceptions. If you were just paying attention to the almost weekly reporting in the Western press about alleged Chinese cyber espionage, you could be forgiven for thinking that China ruled the cyber waves. Yet recent writings in the Chinese press have more of a "China is vulnerable" flavor and suggest that analysts, if not characterizing the country's cyber strategy as weak, think there is a great deal of work that remains to be done.

The work ahead is both defensive and offensive, technical and strategic. Zhang Yongfu, a professor at the PLA's [Information Engineering University](#), told the [PLA Daily](#) that the "cybersecurity situation" was in its early stages. As with every other country, deciding which bureaucracies should be involved in defense and coordinating among them is difficult; cyber management, in Zhang's words, is fragmented and ineffective. Since a cyber event could develop over hours if not minutes, policymakers must seriously wonder if the People's Liberation Army, Ministry of Public Security, Ministry of State Security, and Ministry of Industry and Information Technology can successfully coordinate their roles during a crisis.

Chinese analysts are also grasping with the conundrum that if you wait until you see a problem in your networks, it may already be too late. The Pentagon's [Strategy for Operating in Cyberspace](#) says it will employ "active defense"— "synchronized, real-time capability to discover, detect, analyze, and mitigate threats and

vulnerabilities." Former Deputy Secretary of Defense William Lynn III compared this to combining a sentry and a sharpshooter. This article on China National Defense News also uses the concept of active defense (积极防御), involving a reliance on cyber reconnaissance and surveillance as well as the realization that defense must be conducted at "all times and all places", which could be read to mean "defense" in other countries' networks.

As with most articles about cyberspace, there is a fear that China could lose control over information "nodes and infrastructure" and outside powers could distribute rumors that mislead the public. The growing dependence of the military on networks is a new vulnerability as other powers are preparing to sabotage network command, control, communications, and intelligence systems. Technology is a big concern in all of these articles: the United States has it, [China does not](#). There are also discussions about how the PLA and others can attract and retain hacking talent.

What to make of these assessments? Someone is bound to find a quote from Sun Tzu (Here's an easy one: "All warfare is based on deception; when we are able to attack, we must seem unable") and suggest that these articles are meant to confuse, mislead, and lull the United States into a false sense of security. Maybe these articles are primarily focused on domestic audiences, signaling to the Chinese public that the leadership is not standing still while the United States develops a cyber strategy, or perhaps to various domestic institutions and actors that they need to get on board with the emerging strategy.

Perhaps the simplest explanation is that Chinese policymakers fear that they really are at the bottom of the table. Despite outside perceptions of the coherence and efficacy of Chinese cyber strategy, Chinese analysts are feeling increasingly vulnerable in cyberspace.

[Table of Contents](#)

## U.S. Could Maintain Virtual Presence in Syria

By Joseph Marks, [NextGov.com](#), 02/06/2012

The closing of the U.S. embassy in Damascus on Monday in response to escalating violence may not mean an end to the State Department's virtual ties with Syria, experts told Nextgov.

Even from outside the country, State officials could continue to interact with Syrian citizens on Facebook and Twitter, they said, and to update postings on the embassy's English and Arabic-language websites.

"There's no magic bullet that's going to take the place of having people on the ground in the country," said Sheldon Himelfarb, who researches conflict, media and technology at the United States Institute of Peace. "But, absolutely, social media allows us to continue to reach out to activists and civil society and ordinary citizens regardless of the embassy doors being open."

The State Department hasn't announced any specific plans to maintain its social media presence in Syria and declined to comment on the issue Monday.

Embassy staff regularly used social media before the evacuation and Ambassador Robert Ford often answered questions from Syrian citizens on Facebook.

As of Monday evening, officials had posted a note to the embassy's website saying they had suspended embassy operations but had not noted the closure on the embassy's Facebook and Twitter pages.

One of the most ambitious attempts at virtual diplomacy in recent years was the December launch of the State Department's "virtual embassy" for Tehran, essentially a standard U.S. embassy website without a physical embassy standing behind it. The United States has not had diplomatic relations with Iran since that nation's 1979 Islamic revolution and the ensuing crisis during which embassy officials were held hostage for more than a year.

Posts on the virtual Tehran embassy site include some stock notices about statements by Secretary Hillary Clinton but also include some unique posts clearly aimed at drawing in average Iranians. One recent post honors World Wetlands Day, created by a United Nations Convention signed in the Iranian town of Ramsar in 1971.

The site also includes information about U.S. visas and studying in the United States. Because the Iranian government blocks the embassy site, Iranians can only reach it using circumvention tools.

The two-month-old embassy site is often derided or goes unnoticed in Iranian social media, but a few approving links to embassy pages have begun popping up too, especially to things like the wetlands post that don't tout U.S. foreign policy, said Collin Anderson, an independent researcher who has worked with Iranian and Syrian social media activists and studied the embassy site's reach.

It's difficult to measure how much effect sites like the virtual embassy have, Anderson said, but ideally they can present a clearer vision of U.S. society, culture and policy than what's portrayed in Iranian state media.

"It's basically the hearts and minds things," he said.

The Damascus embassy's website could easily be transitioned into something like the Tehran website, Anderson said, but would be stymied by a lower level of tech savvy in Syria.

About 20 percent of Syrians are online compared with about 30 percent of Iranians, according to the OpenNet Initiative, a joint project by Harvard, the University of Toronto and the SecDev Group, a Canadian security and development company. Syrian Internet is significantly less developed and more regulated, though, according to ONI.

A more important diplomatic tool than maintaining the website, Anderson said, will be maintaining a U.S. presence in social media. Ambassador Ford's Facebook chats, for instance, could be done just as easily from Washington as from Damascus and would reach a wider audience.

"The power of social media is that it's an audience that's not necessarily going to already be sold on an issue," he said. "With the virtual embassy, you have to go there with intent...To get a large audience requires a platform where people are sharing pictures of their dogs and grandkids and then sometimes in your feed there will be some U.S. response to the crackdown in Homs. That's what you get out of social media."

[Table of Contents](#)

## Battle for Syria Rages across the Internet

By Abigail Fielding-Smith, [Financial Times](#), 8 Feb 2012

As a live, online video-stream broadcast the terrifying sounds of Syrian president Bashar al-Assad's forces pounding opposition strongholds in Homs yesterday, another battle was raging on an instant-messaging forum.

As people expressed their horror at what was happening and typed in the opposition battle cry —Allahu Akbar!!, a pro-regime user weighed in with —May Bashar [sic] army kick your asses!! The other users responded with a volley of expletives. The loyalist retorted: —Be prepared we are coming FOR U.!!`

The conflict between supporters and opponents of the regime of Mr Assad is being fought just as urgently in the cybersphere as on the streets of Homs, and goes far beyond trading insults. Two shadowy transnational armies slug it out on a daily basis for control not of streets and neighbourhoods but of websites and information caches.

—It's a real war between us,!! says one so-called hacktivist on the opposition side, who calls himself Abdul Hak (servant of truth). —Sometimes they win a battle, sometimes they lose.!!

It has been a good week for the anti-regime side, which succeeded in not only hacking the text message news service of the pro-regime TV station Addounia, but, through the hacker group Anonymous, releasing what are claimed to be private email correspondence of Mr Assad's advisers.

Much like the 'real-world' Syrian opposition, the cyber-activists are a disparate mixture of individuals and groups in and outside Syria. According to Abdul Hak, groups inside will often do what is known as —hardware hacking!!, such as disrupting wires. Opposition cyber activists are said to communicate with each other via Skype, internet relay chat, disposable email addresses and sometimes even the comments sections of random websites.

Their enemy, however, is not to be underestimated. The so-called Syrian Electronic Army, a group of pro-government hackers whom activists allege have received professional help and training, are believed to have hacked the websites of Harvard university and broadcaster Al Jazeera. Others have sought to neutralise Twitter as a tool for mobilising the opposition by using their favoured hashtags such as —16 March!! (the day of the first protests) and flooding them with links to porn sites or pictures of Syria in a glow of tranquility.

The cyber war may seem like a side-show compared with the struggles between protesters, armed insurgents and government forces going on every day inside Syria but, according to Wissam Tarif, a researcher with the campaign group Avaaz, it can have life and death consequences.

—Three months ago, I got a PDF file on my email with more than 40,000 names of people they have detained, and that file came from activists who hacked in to interior ministry website,!! he says.

Moreover, with a situation of near stalemate on the ground, control of the narrative is key for either side to move forward. With the state having controlled the public sphere for so long, the opposition have some of the advantages of the underdog in the information war. It has more impact when hackers jam the airwaves in

central Damascus, as they did a few months ago, and broadcast a famous song demanding that Bashar leave, than it does when pro-government activists hack opposition sites.

Abdul Hak says the two sides occasionally meet in cyberspace. —It happens a lot via Facebook pages," he explains. —It's like: 'Hey, we are going to bring down your pages', and you have an answer like: "Bring it on'."

[Table of Contents](#)

## Iran – Death for Blogging

By The [Washington Times](#), February 20, 2012 [editorial]

Iran has an easy way of dealing with people who do things online that displease the mullahs. Kill them.

For four years, computer programmer and Canadian resident Saeed Malekpour has languished in an Iranian jail cell. He was arrested in 2008 while in the country to visit his ailing father. The regime charged him with "spreading corruption," a catchall crime that can apply to many supposed affronts to the Islamic theocracy, but in this case referred to allegedly spreading pornography. A third party had used software Mr. Malekpour developed to upload graphic images without his knowledge.

At his trial, Mr. Malekpour confessed to abetting the act, but he later contended the confession was coerced. "A large portion of my confession was extracted under pressure, physical and psychological torture," he wrote in a letter smuggled from prison, "threats to myself and my family, and false promises of immediate release upon giving a false confession to whatever the interrogators dictated." He was found guilty and sentenced to death. Iran's Supreme Court later ordered a review, and last October, the death sentence was reaffirmed, with 7 1/2 years in prison added for good measure.

Last week, it was learned that Mr. Malekpour's case file had been transferred to the Circuit Court for Execution of Sentences and his execution could take place at any time. Mr. Malekpour's family sent a letter regarding the case to United Nations human rights commissioner Navi Pillay. The U.S. State Department formally protested the sentence against Mr. Malekpour and called on Iran to allow unfettered access for U.N. Special Rapporteur Ahmed Shaheed to investigate widespread allegations of human rights violations in the Islamic republic.

Mr. Malekpour is one of several people who have been imprisoned on charges of "polluting the minds" of Iran's youth. Vahid Asghari is an Iranian blogger who faces death for anti-government agitation and insulting Islam, also allegedly for uploading pornography. In January, the regime arrested at least six journalists, bloggers and other "netizens" as part of a crackdown ahead of the March parliamentary elections. Two of them, Parastoo Dokouhaki and Marzieh Rasouli, are female journalists who have been active in promoting the rights of Iranian women. Another arrestee, Mohammad Solimaninya, ran a social-networking website called u24 and designed and hosted websites for Iranian intellectuals and civil-society organizations. The charges against him haven't been made public, but anyone who facilitates communication among thoughtful people in Iran is a threat to the mullahs.

Independent Iranian journalists are a courageous lot to begin with. According to the latest press-freedom index from Reporters Without Borders, Iran ranks 175th out of 179 countries, edging out only Syria, Turkmenistan, North Korea and Eritrea on the scale of oppression. Death sentences for Mr. Malekpour and Mr. Asghari are intended to send a message to others that building informal information networks on the Internet won't be tolerated. While the world is focused on Iran's nuclear weapons program, its military support for the Assad regime in Syria and its attempts to use its international terror network to bomb Israeli diplomats, it should not forget the Iranians languishing in cells whose offense to the regime was the desire to tell their country's increasingly tragic story.

[Table of Contents](#)

## A Fatal Tweet

The [Washington Times](#), February 17, 2012 [Editorial]

In America, sending the wrong tweet can mean embarrassment, ostracism or losing your seat in Congress. In Saudi Arabia, it can cost you your head.

Hamza Kashgari is a 23-year-old journalist who wrote for the daily al-Bilad in Jeddah, Saudi Arabia. On Feb. 4, the observance of Muhammad's birthday, Mr. Kashgari sent out three tweets expressing what he would say if he met Islam's founder. "On your birthday, I will say that I have loved the rebel in you, that you've always been a source of inspiration to me, and that I do not like the halos of divinity around you. I shall not pray for you," the first read. "On your birthday, I find you wherever I turn. I will say that I have loved aspects of you,

hated others, and could not understand many more," went the second. The third tweet said, "On your birthday, I shall not bow to you. I shall not kiss your hand. Rather, I shall shake it as equals do, and smile at you as you smile at me. I shall speak to you as a friend, no more."

The messages immediately caused controversy. Some welcomed and retweeted them, but thousands more angry Saudis called for Mr. Kashgari's head for supposedly insulting Muhammad. He deleted the offending messages but soon lost his job. Last week, he attempted to flee to safety in New Zealand but was intercepted as he tried to pass through the Muslim country of Malaysia and whisked back to Saudi Arabia in a private jet. He is being held incommunicado in Jeddah while a prosecutor collects evidence to bring a case against him for "disrespecting God" and "insulting the prophet." A conviction on either charge could bring the death penalty. Freedom of thought is a capital crime in the Saudi kingdom. On Monday, Sheikh Saleh bin Fowzan Al Fowzan of the supreme committee of scholars in Saudi Arabia said, "We should first verify that this man did insult ... Muhammad in his article on Twitter ... if verified, then he must be killed." There are reports that those who expressed public support for Mr. Kashgari's message also could face the same charges; even a retweet could lead to the chopping block.

This is not merely a Saudi internal affair. When an Islamic theocracy may execute someone for a tweet, it's an affront to humanity. "I view my actions as part of a process toward freedom," Mr. Kashgari said shortly before his arrest. "I was demanding my right to practice the most basic human rights - the freedom of expression and thought - so nothing was done in vain." These words may be his epitaph.

[Table of Contents](#)

## **A Primer of Copyright Rules, Regulations, and Risks in Writing for Information Operations Publications**

By COL Nanette Gallant, USA DCS G-3/5/7 and Michael F. Litzelman (LTC, U.S. Army, Ret), January 2012 [\[full article embedded below\]](#)

The intent in writing this paper is to inform and remind interested personnel of Information Operations (IO) and related components, enablers, and activities of the rules, processes, hazards, and roadblocks normally encountered in writing and submitting publications for professional journals when using copyrighted material. An element of risk exists in using copyrighted material unless the writer knows the rules and is familiar with the limitations of copyright law. Understanding the processes and hazards of copyright should help ease the risks in putting together interesting and timely publications for the IO field. This paper reviews the common and traditional hazards associated with copyrighted material and how they relate to IO publications in order to inform potential writers about the main hazards of copyright so that they can better understand the rules for publication and the rights in owning, borrowing, copying, and disseminating copyrighted material. An additional purpose of this paper is to give the reader knowledge and awareness of some government sources and assets that are available in establishing, protecting, and using original work. Copyrighted material used in IO products could be an important tool for the IO community in informing and influencing foreign audiences. This paper will review these rules or hazards, which should help to educate—or at least remind—the operator in understanding their obligations and responsibilities in using protected works. In this paper, the IO community refers to its components, enablers, and activities as part of the U.S. government (USG).

Additionally, this paper aims to answer the following questions about the rules and regulations of copyright law as well as issues related to copyright protection.



COL Gallant and Dr  
Litzelman Final for Fel

[Table of Contents](#)

## **The 50 Ruble Army**

From [Strategy Page](#), 20 Feb 2012

February 20, 2012: Russia has apparently quietly adopted the Chinese tactics of paying Internet users a small fee to post pro-government responses on message boards where the government is being criticized or maligned. For some members of the original Chinese "50 Cent Party" it was a full time job, receiving up to 50 cents (two yuan) each for up to a hundred pro-government messages posted a day, using several dozen different accounts. But most of the posters are volunteers or just do it to earn a little extra money. If you can



Not only have the jihadi's taken to this idea more and more because of what is going on with AntiSec, but also it is finally fulfilling their desires to hit the infidels without having to strap on a bomb vest themselves. This is something I have written about in the past with regard to what Samir Khan and Al-Alawki were trying to foment with Inspire magazine and failing to reach the next gen of jihobbyists who are more self centered and unwilling to act for fear of the repercussions. Now, with the hacking model of AntiSec, they have seen that they can do damage AND not necessarily be caught (right away at least) as well as not have to blow themselves up in the process.

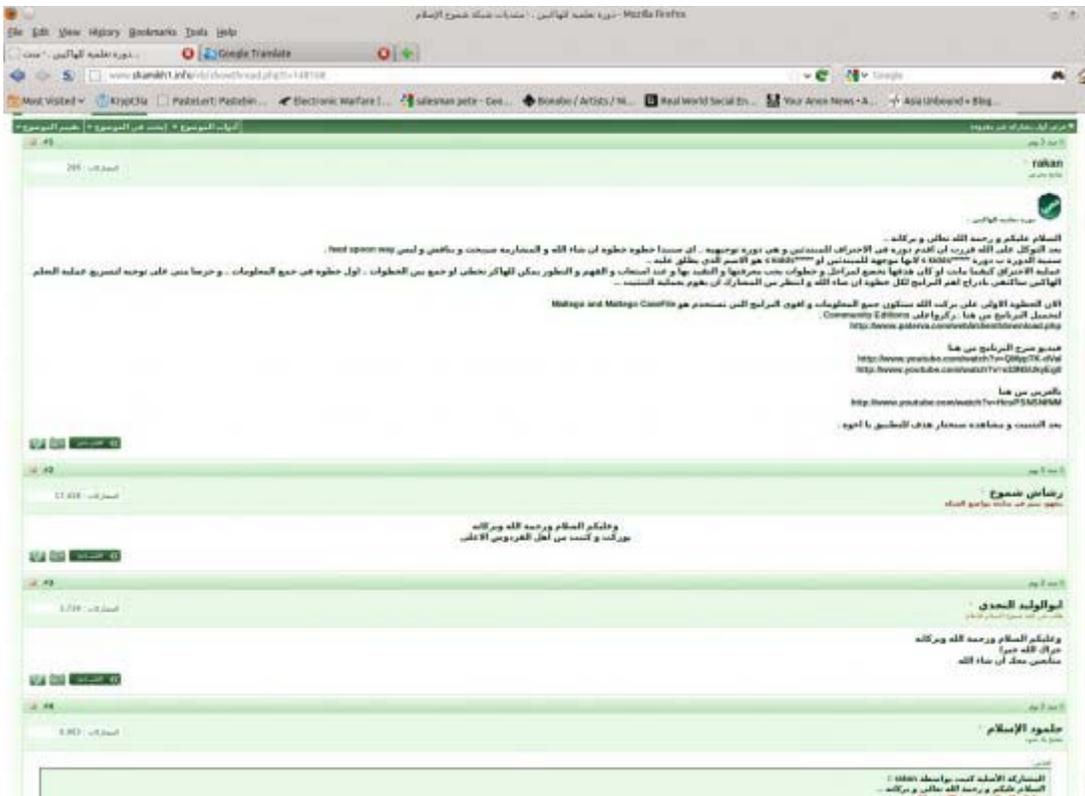
It's a win win for the jihobbyists and AQAP (the new AQ) and add to this the recent video by the old man Zawahiri (get off my lawn!) to the jihadi masses to start working on Syria as the next field of battle. A correlation of this is a post on Shamikh that shows TNT going on about helping with comm's in the area for AQ and the revolution there. The battle to destabilize the regime and perhaps have an AQ?Salafist win when the power vacuum occurs is high on their minds, and by facilitating things they see themselves helping the fight that will win the day for the global caliphate.



### Backtrack 5 and Jihadi's ... Now There's A Mix.

As an effort to get the global cyber jihad going, tutorials are popping up all over the net along with certain Islamic hacking sites offering not only how to's but also software and targets. One of the more interesting developments is how the jihadi's are now going mainstream hacking with the use of things like Maltego, and Backtrack 5 as well as using sandboxed USB drive operating systems. This is not your old jihobbyists online, its changing before your eyes. Now, this is not to say that all of these folks are becoming sophisticated hackers, but, one need not necessarily be one in order to sow chaos or hack a site nowadays right?

There have been tutorials on SQLi as well as how to use Metasploit online for a long time, but only recently have I seen them being translated into Arabi and placed on the technical forums. This means to me, that even the low end of the technically capable can now boot up their tools (courtesy of the security community) and viola, hack a site... Of course, what they plan on doing after that is not clear. So far these guys have not figured out the full Anonymous model's relevance to the global jihad.. Yet... I think though, that as Anonymous/Antisec moves along further, and the words of OBL reach their cognitive centers, they will understand that even this realm of warfare can be used to hit the infidels in the pocketbook, sow fear, and serve as the digital side of the kinetic attacks that the core of AQ would love to perpetrate for large effects.. Short answer.. Digital Warfare in support of actual kinetic attacks on infrastructure.



Maltego and Jihad.. Hmmm..



TNT\_ON and AQ Comm's Support for Syria



## The Take Away

I have been pointing this out for a while now and the jihadi's have been evolving. While the Arab Spring goes on and the changes are sweeping those countries in the Middle East, the jihad has begun to take notice of this area and asked its acolytes to learn. The E-jihad is budding in tandem with their thirst for power vacuums in places like Syria and Yemmen where they hope to take over by winning the popular sentiment. What they fail to see though is that they are not as loved as they think they are.

Meanwhile, in looking at Islamic/Muslim/Jihadi hacker sites, I am seeing the rise of a new player in the Anonymous space... Perhaps even they have become a part of that space and are working within. After all, Sabu keeps playing the Palestine Liberation card in his imagery and speech...

How long til the zeitgeist catches on with the kiddies.... The defacements ongoing and the dumps of credit cards are only the beginning I think...

Now we can add Jihadi's to the list of players in the great game of "Cyberwar" \*cough\* hate that term still...

[Table of Contents](#)

## DIA Director Reveals China's Villainous Capabilities In Space

[SatNews Daily](#), 24 Feb 2012

[SatNews] Keep your friends close, but your enemies closer... except when they're blowing things up.

Army Lt. Gen. Ronald L. Burgess, director of the Defense Intelligence Agency, disclosed new details of China's space weapons programs last week, including information regarding China's anti-satellite missiles and cyber warfare capabilities.

Burgess stated in little-noticed written testimony prepared for an appearance before the Senate Armed Services Committee that Beijing is developing missiles, electronic jammers, and lasers for use against satellites. Much of the space warfare activity is being carried out under the guise of China's supposedly non-military space program, he said.

"The space program, including ostensible civil projects, supports China's growing ability to deny or degrade the space assets of potential adversaries and enhances China's conventional military capabilities," Burgess said. "China operates satellites for communications, navigation, Earth resources, weather, and intelligence surveillance, and reconnaissance, in addition to manned space and space exploration missions," he said.

"China's successfully tested a direct ascent anti-satellite weapon (ASAT) missile and is developing jammers and directed-energy weapons for ASAT missions," he said. "A prerequisite for ASAT attacks, China's ability to

track and identify satellites is enhanced by technologies from China's manned and lunar programs as well as technologies and methods developed to detect and track space debris." China's January 2007 anti-satellite missile test involved a modified DF-21 missile that destroyed a Chinese weather satellite. The blast created a debris field in space of some 10,000 pieces of space junk that could damage both manned and unmanned spacecraft.

For the U.S. military, the successful 2007 ASAT test represented a new strategic capability for China. Analysts estimate that with as many as two-dozen ASAT missiles, China could severely disrupt U.S. military operations through attacks on satellites.

Burgess said China rarely admits that its space program has direct military uses and refers to nearly all satellite launches as scientific or civil.

Additionally, Burgess said Chinese state-run enterprises "continue to proliferate space and counter-space related capabilities," including some with direct military applications.

For example, China's Beidou global positioning system satellites will be available for regional users this year and globally by 2020, he said.

The satellites will provide foreign militaries with precision targeting capabilities through purchases of Chinese Beidou receivers and services.

The system will provide foreign militaries with "greater redundancy and independence in a conflict scenario that employs space assets," he said.

The Chinese, as well as the Russians, are also developing space capabilities that interfere with or disable U.S. space-based navigation, communications, and intelligence satellites.

Moreover, North Korea has demonstrated its ability to disrupt U.S. navigational capabilities through Soviet-made electronic jammers placed on vehicles near the North-South demarcation line that, when activated, were able to disrupt U.S. Global Positioning System signals up to 62 miles away. [Table of Contents](#)

[Table of Contents](#)

## **In Attack on Vatican Web Site, a Glimpse of Hackers' Tactics**

By Nicole Perloth and John Markoff, [New York Times](#), 26 Feb 2012

SAN FRANCISCO — The elusive hacker movement known as Anonymous has carried out Internet attacks on well-known organizations like Sony and PBS. In August, the group went after its most prominent target yet: the Vatican.

The campaign against the Vatican, which did not receive wide attention at the time, involved hundreds of people, some with hacking skills and some without. A core group of participants openly drummed up support for the attack using YouTube, Twitter and Facebook. Others searched for vulnerabilities on a Vatican Web site and, when that failed, enlisted amateur recruits to flood the site with traffic, hoping it would crash, according to a computer security firm's report to be released this week.

The attack, albeit an unsuccessful one, provides a rare glimpse into the recruiting, reconnaissance and warfare tactics used by the shadowy hacking collective.

Anonymous, which first gained widespread notice with an attack on the Church of Scientology in 2008, has since carried out hundreds of increasingly bold strikes, taking aim at perceived enemies including law enforcement agencies, Internet security companies and opponents of the whistle-blower site WikiLeaks.

The group's attack on the Vatican was confirmed by the hackers and is detailed in a report that Imperva, a computer security company based in Redwood City, Calif., plans to release ahead of a computer security conference here this week. It may be the first end-to-end record of a full Anonymous attack.

Though Imperva declined to identify the target of the attack and kept any mention of the Vatican out of its report, two people briefed on the investigation confirmed that it had been the target. Imperva had a unique window into the situation because it had been hired by the Vatican's security team as a subcontractor to block and record the assault.

"We have seen the tools and the techniques that were used in this attack used by other criminal groups on the Web," said Amichai Shulman, Imperva's chief technology officer. "What set this attack apart from others is it had a clear timeline and evolution, starting from an announcement and recruitment phase that was very public."

The Vatican declined to comment on the attack. In an e-mail intended for a colleague but accidentally sent to a reporter, a church official wrote: "I do not think it is convenient to respond to journalists on real or potential attacks," adding, "The more we are silent in this area the better."

The attack was called Operation Pharisee in a reference to the sect that Jesus called hypocrites. It was initially organized by hackers in South America and Mexico before spreading to other countries, and it was timed to coincide with Pope Benedict XVI's visit to Madrid in August 2011 for World Youth Day, an international event held every other year that regularly attracts more than a million Catholic youths.

Hackers initially tried to take down a Web site set up by the church to promote the event, handle registrations and sell merchandise. Their goal — according to YouTube messages delivered by an Anonymous figure in a Guy Fawkes mask — was to disrupt the event and draw attention to child sexual abuse by priests, among other issues.

The videos, which have been viewed more than 77,000 times, include a verbal attack on the pope and the young people who “have forgotten the abominations of the Catholic Church.” One calls on volunteers to “prepare your weapons, my dear brother, for this August 17th to Sunday August 21st, we will drop anger over the Vatican.”

Much as in a grass-roots lobbying campaign, the hackers spent weeks spreading their message through their own Web site and social sites like Twitter and Flickr. Their Facebook page called on volunteers to download free attack software and implored them to “stop child abuse” by joining the cause. It featured split-screen images of the pope seated on a gilded throne on one side and starving African children on the other. And it linked to articles about sexual abuse cases and blog posts itemizing the church's assets.

It took the hackers 18 days to recruit enough people, the report says. Then the reconnaissance began. A core group of roughly a dozen skilled hackers spent three days poking around the church's World Youth Day site looking for common security holes that could let them inside, the report says. Probing for such loopholes used to be tedious and slow, but the advent of automated tools made it possible for hackers to do this while they slept.

In this case, the scanning software failed to turn up any gaps. So the hackers turned to a brute-force approach — a so-called distributed denial-of-service, or DDoS, attack that involves clogging a site with data requests until it crashes. Even unskilled supporters could take part in this from their computers or smartphones.

“Anonymous is a handful of geniuses surrounded by a legion of idiots,” said Cole Stryker, an author who has researched the movement. “You have four or five guys who really know what they're doing and are able to pull off some of the more serious hacks, and then thousands of people spreading the word, or turning their computers over to participate in a DDoS attack.”

Over the course of the campaign's final two days, Anonymous enlisted as many as a thousand people to download attack software, or directed them to custom-built Web sites that let them participate using their cellphones. Visiting a particular Web address caused the phones to instantly start flooding the target Web site with hundreds of data requests each second, with no special software required, the report says.

On the first day, the denial-of-service attack resulted in 28 times the normal traffic to the church site, rising to 34 times the next day. Hackers involved in the attack, who did not identify themselves, said through a Twitter account associated with the campaign that the two-day effort succeeded in slowing the site's performance and making the page unavailable “in several countries.” Imperva disputed that the site's performance was affected and said its technologies had successfully siphoned the excess data away from the site.

Anonymous moved on to other targets, including an unofficial site about the pope, which the hackers were briefly able to deface.

Imperva executives say the Vatican's defenses held up because, unlike Sony and other hacker targets, it invested in the infrastructure needed to repel both break-ins and full-scale assaults.

Researchers who have followed Anonymous say that despite its lack of success in this and other campaigns, recent attacks show the movement is still evolving and, if anything, emboldened. Threatened attacks on the New York Stock Exchange and Facebook last autumn apparently fizzled. But the hackers appeared to regain momentum in January after federal authorities shut down Megaupload, a popular file-sharing site.

In retaliation, hackers affiliated with Anonymous briefly knocked dozens of Web sites offline, including those of the F.B.I., the White House and the Justice Department. At one point, they were able to eavesdrop on a conference call between the F.B.I. and Scotland Yard.

“Part of the reason ‘Op Megaupload’ was so successful is that they've learned from their past mistakes,” said Gabriella Coleman, an associate professor at McGill University who has studied Anonymous. Professor Coleman said the hackers had been using a new tool to better protect their anonymity. “Finally people felt safe using it,” she said. “That could explain why it was so big.”

In recent weeks, Anonymous has made increasingly bold threats, at one point promising to “shut the Internet down on March 31” by attacking servers that perform switchboard functions for the Internet.

Security experts now say that a sort of open season has begun. “Who is Anonymous?” asked Rob Rachwald, Imperva’s director of security. “Anyone can use the Anonymous umbrella to hack anyone at anytime.”

Indeed, in the last six months, hackers have attacked everything from pornography sites to the Web portals of Brazilian airlines. And some hackers have been accused of trying to extort money from corporations — all under the banner of Anonymous.

“Anonymous is an idea, a global protest movement, by activists on the streets and by hackers in the network,” the hackers said through the Twitter account. “Anyone can be Anonymous, because we are an idea without leaders who defend freedom and promote free knowledge.”

[Table of Contents](#)

## Anonymous, It Could Become a Cyber Weapon

By paganinip, [Security Affairs](#) [blog], February 10th, 2012

The group of hacktivist known as Anonymous is considered as the uncontrollable variable in the cyber space capable of surprising us with striking operations worthy of the most skilled cyber army.

Precisely this is the point, are we sure that the group’s operations are so difficult to control or predict?

Are we able to mitigate the risks of exposure?

We consider that the group has as its cornerstone the recruitment of common people through social media to engage in protests.

Reflecting well we are facing with a powerful machine that moves, however, announcing his arrival and producing a loud noise. This undoubtedly provides two advantages:

1. Knowledge of group policies.

2. Ability to operate covert actions against strategic objectives by exploiting the group’s operations as a diversionary action.

Governments and law enforcement agencies understood the offensive potential of the group have accelerated the implementation of measures to control the main channels of communication adopted by hacktivist.

Monitoring systems increasingly powerful have been implemented and are being acquired, they are powerful tool able to correlate events and activities within main social media and search engines.

The battle is undoubtedly difficult, history suggests that ideologies are not fought with arrests and other highly restrictive measures, this leaves me to believe that we will hear a long talk about Anonymous, no longer tied to a group of people but to a new form of social expression.

My thought is shared in many environments, and many experts are convinced that the phenomenon Anonymus goes analyzed from another perspective in some ways innovative.

Is it possible to use the Group and its function as a cyber weapon?

How is it possible?

It is widely believed that it should be carried out intelligence operations aimed at infiltrating the system, become an integral part to affect its operations. Similar operations could benefit the needs of the group has to involve a critical mass of people for their attacks, unthinkable not to leave traces. In a hypothetical phase two does not makes sense to destroy it. It could be more profitable influence their actions against strategic objectives for cyber operations or planning military operations behind a coverage diversionary action conducted by groups like Anonymous.

Many consider this approach impractical, while feeling extremely efficient as cyber weapon the model of social protest through new media. At this point there may be fake cells that hacktivists recruiting ordinary people directing attacks against institutions and hostile governments.

The group has always been driven by purely political motives, and for this reason, imagining it for strategic planning of operations could destabilize an opponent government exaggerates the tone of the internal political debate. We found in more than one occasion how dangerous it can be a breath of wind of protest through the new social media. The Arab spring as the elections in Russia are proof of what can be destabilizing for a political context a protest designed a in cyber space. The involvement, of considerable masses could be according specific requirements.

What we really know regarding the genesis of these phenomena that we see just at the sensational climax?

Assumed the possibility of using groups like Anonymous, or rather its model of protest, as a cyber weapon who might be interested in its "recruitment" and what are related risks?

Obviously the idea is very appealing to all governments that tend to conceive cyber definitely aggressive strategies, but that need guarantee a low mediatic exposure. For this reason no doubt exclude government has always openly hostile as Iran, Syria living in the obsession of having to show the world their technical skills. Rule out also governments as Russian and Chinese for two reasons, first for the possibility of using satellite nations like Iran and North Korea for its cyber strategies, second the questionable management of internet, at the edge of censorship, practiced in these countries represents a serious obstacle to the growth and conditioning of movements such as that discussed.

It's obvious that the states in which these groups are more active as the U.S. and Europe might those more interested and motivated in groups hacktivist approach, an approach that would affect cyber operations without having to face the consent of the international community.

How to approach the dangerous groups and with what risks? Intelligence operations and study of the phenomenon are preparatory to the approach, but with regard to the possibility of infiltrating the group of course this could be achieved by conditioning, for example through financial compensation and other benefits, the medium and high level representatives of the groups, those people that define the strategies of protest.

The risks are related to the negotiation with unstable and mutable organizations that we know too little, but history teaches that such agreements are possible and have occurred in the past such as between states and criminal organizations.

[Table of Contents](#)

## **Report: Internet Radicalizes U.S. Muslims Quickly**

By Shaun Waterman, [Washington Times](#), February 27, 2012

Young American Muslims can become radicalized online very quickly and with few warning signs, becoming potential terrorists before federal agencies can identify them, a new congressional report warned Monday.

Zachary Chesser, a 22-year-old Virginia man now serving 25 years for terrorism crimes, took less than two years to transform "from an average American kid to a hardened supporter of terrorist organizations," according to a study of his case by staff from the Senate Homeland Security and Governmental Affairs Committee.

The bipartisan report analyzes his prolific online writing and correspondence with staff investigators after his guilty plea October 2010 to three terrorism-related felonies. The charges included attempting to provide material support to a foreign terrorist organization through his efforts to join al-Shabab, the al Qaeda affiliate in Somalia.

"Chesser represents a growing breed of young Americans who have such comfort and facility with social media that they can self-radicalize to violent Islamist extremism in an accelerated time period, compared to more traditional routes to radicalization," the report said.

Chesser, who converted to Islam after graduating high school in 2008, is "a harbinger, not an outlier," according to the report.

The report concluded that the federal government lacks a coordinated strategy to combat online radicalization, although it called a new State Department initiative aimed at countering terrorist chat on social media sites "encouraging but nascent."

"The United States currently has a haphazard approach to dealing with global Internet radicalization and propaganda," the report said.

[Table of Contents](#)

## **When Is A Cyberattack A Matter Of Defense?**

By Ellen Nakashima, [Washington Post](#), 27 Feb 2012

In the debate over how best to defend the nation against cyberattacks, one of the main points of tension relates to the extent to which the government should be able to deploy "active defenses."

The White House in January blocked draft legislation that would have enabled the National Security Agency or any government entity to monitor private sector networks for computer viruses and to operate "active defenses" to block them.

The monitoring, officials said, would have crossed an Obama administration red line — that there be no government monitoring of private networks. In particular, the phrase “active defense” set red lights flashing. In the end, White House officials prevailed upon an aide to Sen. Dianne Feinstein, the chairman of the Senate Intelligence Committee, to remove the language from draft legislation.

But officials at the NSA, a Defense Department spy agency with advanced capabilities to detect harmful software targeting military and classified networks, disapproved of the move, according to documents and interviews with administration officials.

“It caused some consternation” because NSA “frankly wanted to get that authority,” said an administration official, who spoke on condition of anonymity to discuss internal deliberations. “But that was very much contrary to the administration’s position.”

NSA Deputy Director John C. Inglis said in an interview that the agency “did not register displeasure” over the language being removed. And, he said, NSA has never proposed any government plan “where it would monitor private sector networks.”

But interviews and documents make clear that agency officials felt the scaling back of the authority to monitor for cyber threats and to push out countermeasures to industry was of great concern.

It’s unclear what kind countermeasures the NSA would have been authorized to take under the proposal. In fact, one problem with proposals over active defense is that the term itself can be open to interpretation.

The Defense Department has defined active defense as a “synchronized, real time capability to discover, detect, analyze and mitigate threats and capabilities.”

But, said the administration official, that definition still wasn’t precise. “It wasn’t clear what active defense meant, and where the effects would be authorized to occur,” he said.

The administration felt that the measures could entail some form of government monitoring of private networks. NSA officials said they distinguish between monitoring, which connotes reviewing content, and scanning, which they say is an automated process to look for software that could damage computer systems.

Proposals advanced internally by NSA officials have called for Internet carriers to do the scanning of network traffic on systems operated by critical industries such as electrical grids. Private sector companies would then turn over to the NSA any e-mail or other communications that contain viruses so the agency could analyze them and devise more effective countermeasures, administration officials said.

Richard Schaeffer Jr., former information assurance director at NSA, says the debate over active defense suffers from a lack of linguistic clarity. “Let’s talk very precisely about what specific actions we want to take, under what conditions, so there’s no misinterpretation,” he said.

Active defense has been used to mean everything from “hunting in your network” for viruses, to quarantining malware, to shutting down an attacking server outside the military’s networks — including at its source. The latter can be seen as a form of cyber offense.

The issue has long been a subject of debate inside the Pentagon. As long as the military is acting inside its own networks, it is on solid legal ground. But legal and policy questions surround the extent to which the military can take actions outside its network without having to get presidential approval.

In the thick of the debate is Gen. Keith Alexander, NSA director and head of U.S. Cyber Command, the military’s offensive cyber arm. In 2010, when Alexander and the fledgling Cyber Command pushed for standing authority to take action inside the United States to protect critical systems against crippling attacks, the notion did not survive interagency debate. It even encountered resistance within the Pentagon.

“They were asking for way too much authority and they were contravening the Constitution with what they were asking for — to take unilateral action outside of their area of responsibility,” recalled Gen. James Cartwright, who retired in September as vice chairman of the Joint Chiefs of Staff.

Last November at a conference in Omaha, Alexander recalled taking a boxing class as a youth. The instructor, he said, divided the class into two teams. One could only hit. The other could only defend. “Which team do you want to be on?” he asked.

“We have to have more authorities to protect ourselves in cyberspace,” Alexander said. “We can’t just defend.”

One military official, who was not authorized to speak for the record, said “to have true active defense, you’ve got to be able to meet the threat wherever it occurs.”

When Alexander talks about active defense, "he's talking about a set of pre-approved responses to counter specific threats," said the military official. "The problem is he's never come up with a scheme that specifies what threat may be met with what response that the interagency is comfortable with."

[Table of Contents](#)

## **S Korea develops technology to jam electronic signals**

วันอาทิตย์ ที่ 26 ก.พ. 2555

SEOUL, Feb 26 (Yonhap) -- South Korea has developed a technology to disrupt electronic signals in electronic warfare, a military source said Sunday.

"The Agency for Defense Development (ADD) has recently developed electromagnetic pulse (EMP) technology to paralyze electronic devices," the source said. "The ADD began working on this technology in 1999."

According to the source, the ADD will further build on this primary technology and develop capabilities to repeatedly send EMP signals at high frequencies. The ADD will then look to develop EMP bombs with advanced capabilities, the source added.

"The EMP technology we have now would be rated 'soft kill,' meaning it would paralyze electronic devices or systems within a 100-meter radius," the source explained. "If we can improve on this, we will then reach the 'hard kill' level, whereby the technology will actually destroy intended targets."

EMP bombs are considered critical assets in new types of warfare for their ability to neutralize or damage radars, airplanes, naval fleets and aerial defense systems. Experts believe such bombs may disrupt North Korean electronic systems at its nuclear or long-range missile bases. EMP is also produced from nuclear explosions.

North Korea is also known to be developing EMP bombs. South Korea has been trying to protect key military facilities, including the defense ministry headquarters, from potential electronic attacks. In its report submitted to the parliament for an annual audit last September, the ADD said South Korea doesn't have sufficient technology to fend off EMP attacks, and it can only defend against less-damaging electromagnetic interference (EMI).

[Table of Contents](#)

## **Quran Burning a PSYOP Failure in Afghanistan**

By Kerry Patton, [Big Peace](#) [blog], Feb 22nd 2012

Afghanistan has imploded once again. Riots swarm epicenters, people have been injured, and now reports of deaths unfold. Islam's most holy book, the Quran, has been desecrated, and US forces have been deemed the culprits.

The real culprits in today's complex situation in Afghanistan are not the US-led coalition—rather, a few select prisoners who successfully brought masses of locals together. This tactic was achieved from inside prison cells. Amazingly, without any assistance from the outside world, a bunch of prisoner's activities fueled battle against the United States.

Prisoners desecrated the Quran by utilizing the holy book for coded messaging. This act is a very old and historic tactic utilized in many past conflicts among prisoners. While the Quran may or may not have been used in the past, religious books, which are mandated by law to be available to prisoners, have been utilized for communication purposes.

US forces intercepted these covert communications and rapidly disrupted them. The holy texts were confiscated and destroyed. Unfortunately, the initial defacing of the texts caused by prisoners was never revealed to the local indigenous population through a proper psychological operations (PSYOP) campaign.

Had a proper PSYOP campaign occurred, the current effects of riots and protests would likely have never evolved. For years, astute military advisors pushed the idea of incorporating Islamic principles in PSYOP campaigns. Some military leaders understood the need however many did not. For those who refused to listen to their advisers, only one reason comes to mind—political correctness.

The majority of Afghans believe the US-led coalition are comprised of "people of the book." This means that they understand we are not followers of Islam. They also realize how intelligent we are in doing everything in our power to study their culture, values, and religion.

One mistake can cause chaos, and we often must walk on our tippy toes when interacting with the local populace. One wrong move and all hell could break loose, as observed currently. Of course, we have made

many wrong moves in the past ten-plus years in Afghanistan, but we have done much more good than bad ,and most Afghans know this.

General Allen did his best to ease the situation, but that was not good enough. The State Department also did their best, yet that, too, wasn't enough. Reactionary actions are never enough. We must be proactive when dealing with the Afghan people. A proper proactive tactic would have been to launch nationwide messages showing how un-Islamic many prisoners are. We cannot do this, however, because as a whole, American political correctness has socially conditioned us to never discuss religion with those who believe differently.

Richard Brodie states in his book *Virus of the Mind*, "The meme is the secret code of human behavior, a Rosetta stone finally giving us the key to understanding religion, politics, psychology, and cultural evolution. That key, though, also unlocks Pandora's box, opening up such sophisticated new techniques for mass manipulation..."

Psychological operations are truly meant to serve as meme warfare. With sound PSYOPs, an entire nation-state's population can catch a mental virus. That virus spreads rapidly, causing people to behave in ways we desire. Our enemy in Afghanistan has perfected the meme warfare tactic while we have failed time and again.

There is a reason why the war in Afghanistan has prolonged itself. That reason doesn't necessarily entail poor rules of engagement, a stronger enemy force, or lack of numbers. One of the main reasons Afghanistan has been a blunder is because the United States and our partners have been manipulated and we simply do not know how to counter Afghan manipulation practices.

The Afghan enemy loves to manipulate anyone they can, and we have become perfect targets. We listen, do what is asked, and pay the price. This is not the first time an incident involving the Quran unfolded, and it will likely not be the last. Until we learn how to properly mitigate future uproar due to similar incidents through sound PSYOP campaigns, local reactions will be the same.

[Table of Contents](#)

## Psychological Warfare Must Precede Strike on Iran

By William A. Levinson, [American Thinker](#), February 25, 2012

Sun Tzu wrote 2,500 years ago that war is of vital interest to the state, and a matter of life and death. Colonel Paul Linebarger's *Psychological Warfare* says the same of his science: "Yet success, though incalculable, can be overwhelming; and failure, though undetectable, can be mortal." Most of the West does not understand this science, and Israel is particularly deficient in its study.

Any attack on Iran's nuclear program will, in the absence of preparatory psychological warfare, unite the Iranian people against the attacker. Germans who had no use for Hitler and Nazism nonetheless fought harder when Allied troops entered Germany itself, and Russians who feared or despised Stalin took up arms against German invaders. Iran's government is obviously relying on its people to react similarly to any Western effort to derail Iran's nuclear program, and may in fact want to provoke an attack to divert the minds of Iranians from their government's numerous shortcomings. This is why a PsyWar campaign must precede an attack on Iran, and it may in fact make such an attack unnecessary.

The campaign must educate the Iranian people that the West has no quarrel with them, but only with their rulers, who plan to attack other countries with nuclear weapons. Mahmoud Ahmadinejad's "World Without Zionism" poster shows a glass ball with the Israeli flag falling through an hourglass, along with a broken one with an American flag at the bottom. Iranians must realize that their leaders are effectively brandishing weapons of mass destruction, which both invites and justifies a pre-emptive response.

The first step of such a campaign is to identify the Propaganda Man, or hypothetical audience we seek to persuade. Most countries have more than one Propaganda Man. In Iran, for example, we have the soldiers who control the means of violence, as well as civilians who live in fear of the government and religious police. Both audiences are likely to dread the inevitable nuclear retaliation should their rulers put their threats into effect.

The propaganda campaign should therefore state, "The West has no quarrel with Iran unless Iran starts it, in which case the target of Iran's aggression would have no choice but to retaliate in kind and with overwhelming force. Tens of millions of Iranians would die, and the great cities and proud heritage that date back to your Persian ancestors would lie in ruins. This [insert pictures of victims from Hiroshima and Nagasaki] is not what you seek for your great nation, but it is where your self-serving rulers are leading you."

The phrase "self-serving" is important because a leader who does not serve his followers loses what China calls the Mandate of Heaven: the right to lead as derived from effective service to stakeholders. This argument can be phrased with the ancient Indo-European word *dher*, for the duty of a leader or ruler to care

for the welfare of his subjects. It appears, for example, in the name of Darius (a king of Persia), Jemadar (lieutenant, holder in trust of a body of men), and Dharma (the Right Way). The Iranian words for duty and stewardship should therefore be used as often as possible.

The first step is therefore to persuade Iranians that the Ahmadinejad government, unlike a true Persian leader, rules for its own benefit and not for that of its people. The next step is to tell Iranians, and especially those who control weapons, what they can do about it.

Another great nation, the people of Germany, had a heritage of learning and culture that, while not as old as Iran's, was the envy of Europe. Then they made the mistake of electing a self-serving demagogue named Adolf Hitler. Hitler said he would lead Germany to greatness, but by 1944, it was clear that he was leading Germany nowhere but to utter ruin. Millions of Germans already lay dead, and the nations that Germany had attacked the way your government threatens to attack the West were closing in on it from both sides.

Then a group of patriotic German officers realized that loyalty to Hitler was not compatible with loyalty to their Fatherland. These German patriots conspired to kill Hitler, overthrow his government, and make peace with the nations whom Hitler had attacked. Had they succeeded, it is quite likely that the Allies would have made peace without occupying and humiliating Germany as they did in 1945. The elimination of the Nazi government and Germany's withdrawal from all occupied countries would have left the Allies with no real reason to continue to fight.

Does your duty to your countrymen and to Iran's ancient heritage call upon you to help start a senseless war in which your friends and families are likely to die wholesale, or to remove the self-serving rulers who call for this war in the name of an ideology every bit as deranged as that of the Nazis?

The appeal can add that the Italian people took matters into their own hands with regard to Benito Mussolini, and the famous or infamous pictures of Mussolini hanging upside-down could be included as a suggestion as to what ordinary Iranians can do with their government -- especially religious judges and secret police who have made Iranian dissidents disappear, or have sentenced women to be stoned to death for mostly imaginary offenses.

This propaganda offers the added effect of fomenting paranoia in the Iranian government, and Sir Thomas More's Utopia actually recommended this approach. It was the practice of More's fictional Utopians to offer a reward for the murder of the enemy leaders, with amnesty for any enemy leader who turned on his associates. The resulting breakdown of trust, at least in a despotic government, is quite likely to result in preemptive executions and/or assassinations.

Commentators on Sun Tzu's Art of War added a case study in which a country sent a "secret" message to a high-ranking official on the other side, with the intention that it be intercepted to make it look like the official was disloyal. The valuable official was put to death; Germany used the same technique to cause the execution of a Russian general during the Second World War.

Colonel Linebarger contended quite accurately that psychological warfare is the most humane of all weapons. If you can persuade an enemy to lay down his arms, desert, malingering, or otherwise not do his master's bidding, he won't kill you, and you don't have to kill him. The persuasion of the Iranian people to overthrow their dictators will save lives on all sides while offering Iranians a prosperous future free of religious oppression, violence, and the dreaded knock on the door in the middle of the night.

[Table of Contents](#)

## **U.S. Should Not Follow China's Example in Merging Cyber and Electronic Warfare Efforts**

Loren B. Thompson, Ph.D., [Defense Pro](#), February 27, 2012

On November 14, Defense News ran an interesting story by Asia correspondent Wendell Minnick about how the General Staff of China's People's Liberation Army (PLA) manages cyber warfare activities. Minnick quoted Australian security expert Desmond Ball as speculating that the General Staff may have merged its offensive cyber and electronic warfare activities into an "integrated network electronic warfare" directorate within the General Staff's Fourth Department. If this sounds too arcane to matter, guess again: the way major military powers organize their network defense, exploitation and attack efforts could decide the outcome of the next big global conflict.

Let's assume for the sake of argument that Desmond Ball is right. By merging cyber warfare with electronic warfare in a single military department, the General Staff would be breaking down the bureaucratic barriers between two specialties that both are useful in degrading the command and communications networks of adversaries. Both approaches are "non-kinetic," meaning they achieve their effects through techniques other

than dropping bombs or blowing things up. In the case of electronic warfare, signals are generated that jam or confuse electronic systems operating on similar frequencies. In the case of cyber warfare, attackers use malicious computer code to penetrate information systems and manipulate or disrupt their operations.

These sound like similar kinds of operations, but they really aren't. Electronic-warfare specialists may use advanced algorithms to attack enemy networks, but they remain outside those networks, modulating power levels and signal transmissions to achieve desired effects. Cyber warfare specialists actually get inside the enemy's network and use its own software to hijack or deceive it. If cyber warriors are really good at conducting network exploitation or attack missions, adversaries may have no idea their systems have been compromised for years. That sort of delay in enemy situational awareness seldom occurs in electronic warfare, where the effects of an attack are usually obvious to operators within minutes.

It makes sense to understand both aspects of network attack when organizing an integrated war plan, because different wartime scenarios will demand divergent responses, and using both approaches in combination will sometimes produce the best effects. However, we are talking about two separate communities of specialists, one of which (electronic warfare) is relatively mature and the other of which (cyber warfare) is still in its infancy. If combining the two in an integrated organization resulted in the more mature specialty dominating development of the more fledgling specialty, that could be disastrous over the long run. Strategic bombardment probably could have ended World War Two much sooner if U.S. Army leaders had applied it without bias rather than bending it to the needs of ground forces (air power proponents wanted to attack refineries and electric grids rather than enemy forces).

Thus, what looks like an enlightened organizational move by the Chinese General Staff to combine all the methods of network attack in the same directorate actually could backfire by slowing development and application of new methods. We've seen some evidence in the U.S. that more traditional military communities would like to subsume emerging capabilities within existing institutional frameworks rather than letting them evolve in an open environment. Over the long run, that could undermine America's ability to stay ahead of countries like China. The notion that institutional barriers and "stovepipes" are always a bad thing therefore needs to be reexamined. If the barriers protect an emergent skill-set from bureaucratic empire-builders who would retard or pervert its progress, then maybe they serve a useful purpose. We don't need guys who operate jammers telling cyber warriors how to pursue their craft.

[Table of Contents](#)