# 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 Online

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

# Table of Contents

Vol. 13, no. 06 (April 2013)


1. A Cyber-Survivable Military
2. Redefining Information Operations
3. Command and Control Vulnerabilities to Communications Jamming
4. China's Internet: A Giant Cage
5. Cat and Mouse: How China Makes Sure Its Internet Abides By the Rules
6. Assessing The Effects - A Curse Disguised As A Blessing?
7. Shutting Down the Internet - Thou Shalt Not Kill
8. Internet Controls in Other Countries
9. Masters of the Cyber-Universe
10. The Great Firewall: The Art of Concealment
11. Electronic Warfare: The Ethereal Future of Battle
12. Why China Is Reading Your Email
13. Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling
14. Six U.S. Air Force Cyber Tools Designated As 'Weapons'
15. Mexican Social Network Manager Quits Post amid Threats from Drug Traffickers
16. U.S. Military Working to Integrate Cyber Weapons into Commanders' Arsenals
17. The Explosive Effects of Rumors in Syria and Insurgencies around the World
18. North Korea's Threats, Campy Videos Drawing Internet Attention
19. Socialism and the Global Information War
20. Training the CAPOC Soldier
21. Combat on the Online Battlefield
22. New Cyber Rules Put Combat Decisions in Soldiers' Hands
23. Cyber Warriors Association Points to Evolving Battlefield
24. Is Cyber War the New Cold War?
25. Air Force and Army Disclose Budget for Hacking Operations
26. Military Photographers Ready to Deploy Around the Globe
27. Air Force Academy Wins NSA Cyber Defense Title
28. How People in the Middle East Actually Use Social Media
29. New Electronic Warfare Tool Offers Innovative Approach
30. Jihadi Twitter activism – Introduction
31. SPAWAR Leadership on Information Warfare and the Growing Cyber Threat
32. Pentagon Paying China — Yes, China — To Carry Data

# A Cyber-Survivable Military

By Vincent Manzo, the National Interest, April 3, 2013

A recent report by the Defense Science Board (DSB) proposes a comprehensive approach to improving the U.S. military's resiliency to cyber threats. Many of its recommendations would address the cyber espionage plaguing the Department of Defense every day. But the study also considered how technologically-savvy, well-resourced states, such as China or Russia, might use cyber weapons against the United States in a war.

Within this surreal context, the DSB's prescriptions are sensible: the United States should ensure that its nuclear forces and a portion of its conventional-strike forces would function after a sophisticated cyber attack on U.S. military networks. For example, China might disrupt the networks linking U.S. forces, weapon, and satellites, or it might corrupt the programs operating these complex systems. If effective, these attacks would make the U.S. military much less capable by undermining communication, intelligence, surveillance and reconnaissance operations, navigation and precision strikes. Of course, China and any other state capable of executing such an attack would only do so during or on the cusp of a full-scale military confrontation, probably to achieve a strategic advantage in the physical world. Whereas otherwise the risks of conventional war with the United States would be too high, the potential for high-payoff cyber attacks may give adversary leaders confidence they can prevail in a short conflict or perhaps even deter U.S. officials from intervening altogether.

Denying them the ability to incapacitate U.S. forces via cyber attacks would, theoretically at least, thwart their strategy of fighting a significantly weakened U.S. military. Forces capable of functioning after a cyber attack would thus contribute to the broader goal of deterring major powers from risking war with the United States.

With that in mind, ensuring that other states are incapable of disrupting or manipulating the U.S. nuclear arsenal (especially its command, control, and communication system, through the insertion of malicious code) is a prudent policy goal. We should not let the DSB's more controversial argument—the threat of a nuclear retaliation may deter a catastrophic cyber attack on the United States—overshadow it. The members of the study appear to have anticipated that possibility, explaining that cyber-survivability is an essential characteristic of the U.S. nuclear posture, regardless of whether the United States would or should explicitly threaten or launch a nuclear strike after a cyber attack.

The DSB's suggestion that the United States invest in making a portion of its conventional-strike forces cyber-resilient presents a more difficult choice. It advocates implementing expensive and time-consuming defensive measures on a handful of bombers, cruise-missile-carrying submarines, long-range conventional missiles (if they are ever deployed), and command-and-control assets. This "protected conventional" force would enjoy less connectivity to the sensors and networks that make the U.S. military more lethal than its competitors and therefore less vulnerable to cyber attacks. The DSB is not proposing that the United States deploy a separate conventional arsenal for retaliating against all cyber attacks. Nor is it suggesting that a military response would be appropriate for the type of hostile operations witnessed thus far, such as taking down websites or erasing data on hard drive, despite how some may interpret the concept. Instead, the United States would only employ this reserve force in conflicts where a series of cyber attacks has left the rest of the military inoperative.

If an attack of this magnitude is possible, the DSB recommendation makes sense. It couches this approach in the language of escalation ladders. But put more simply, in a war where an adversary has done something as drastic as launching a large-scale cyber attack against the U.S. military, the United States would need conventional-strike options to defend itself and its allies.

Yet creating a reserve force means fewer conventional weapons for more frequent conflicts against adversaries that do not possess top-rate cyber weapons. This is no small tradeoff as the military grapples with global defense commitments and fewer resources.

Whether the threat warrants this tradeoff is unclear. The DSB's analysis raises questions about whether a disarming cyber strike, synchronized with other combat operations just as a war erupts, is feasible. An adversary would need to infiltrate and study secure U.S. military networks as well as the communication, intelligence, and weapons systems they connect and operate. Then the attacker must customize code to manipulate them, and for air-gapped targets, covertly gain physical access.

Even if adversaries succeed in planting cyber weapons throughout U.S. systems, their goal would be to affect the targets only when a war is imminent, so they would not have the luxury of attacking immediately. Weeks, months or years could pass before a conflict, during which time U.S. officials might detect and remove the virus, upgrade to more effective security software, or reconfigure their network architectures. Ensuring that deployed cyber weapons are poised for wars that will start at an unspecified time in the future would require consistent surveillance.

The DSB concluded that committed states could overcome these hurdles, and perhaps its recommendation is a prudent hedge. Nobody knows how cyber weapons will evolve. At the least, a cyber-secure conventional force could alleviate pressure to make rushed decisions in crises for fear of losing the ability to fight (for example, a use-them or lose-them scenario).

That rationale should sound familiar; it is the traditional concept of first-strike stability [4] applied to cyber attacks and network-dependent conventional weapons. Concepts from the Cold War are inappropriate for analyzing many cyber issues. But for now, they help us understand how new weapons and vulnerabilities could lead to miscalculation and inadvertent escalation.

Table of Contents

## Redefining Information Operations

By Col Carmine Cicalese, Joint Forces Quarterly (issue 69, 2nd quarter 2013), April 2013

Whether it is strategic communication, information operations, or cyberspace operations, the Department of Defense (DOD) recognizes the importance of conducting operations within the information environment. Over the past decade, several information-related capabilities have grown or matured revealing that the military recognizes the value of conducting operations in the information environment.

Computer network operations have expanded to cyberspace operations, and the Services have established cyberspace component commands to complement U.S. Cyber Command.[1] Military information support operations forces have also matured as the U.S. Army Special Operations Command has established the Military Information Support Command and added another group-level command.[2] The Air Force continues to increase the number of behavioral influence analysts, integrating them into joint commands.[3] In August 2012, the Joint Forces Staff College hosted the Office of the Secretary of Defense–sponsored Information Environment Advanced Analyst Course to further develop the military's ability to analyze and operate in the information environment.

To truly capture the power of information, DOD must recognize the value in understanding the information environment and articulating the integrating processes required within information operations. Despite continued misunderstanding and rewording, information operations is an important integrating function for achieving the commander's objectives through the information environment—a complex and dynamic environment depicted by human interaction with other humans, machines, and subsequent cognitive determinations or decisions. This information environment further comprises three interlocking dimensions, physical, information, and cognitive which are interwoven within a decision-making cycle (Figure 1.) This article uses historical vignettes to offer greater clarity in understanding the difference between strategic communication and information operations and adding depth in recognizing how military information-related capabilities affect the decisionmaking process.

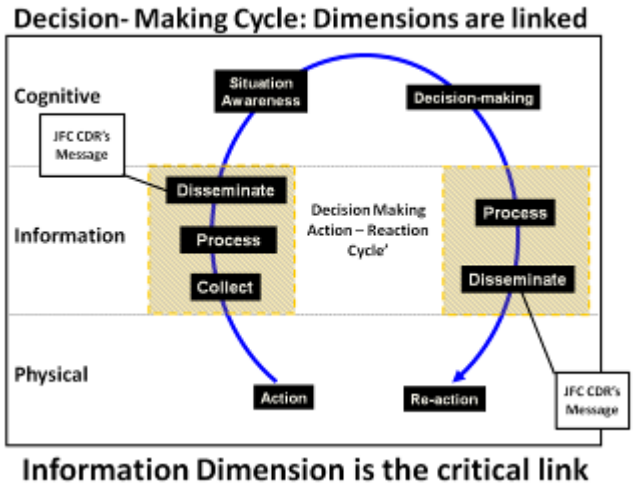



**Figure 1 Decisionmaking Cycle: Dimensions Are Linked**

### The New War of Words

The Secretary of Defense memorandum signed January 25, 2011, stresses the importance of strategic communication (SC) and information operations (IO) in countering violent extremist organizations, while also redefining IO for DOD and subsequently the joint force. As Dennis Murphy noted on mastering information, "The U.S. military will achieve such mastery by getting the doctrine right."[4] The Secretary's memorandum was a step in the right direction leading to recent doctrinal changes. *Joint IO* is now defined as the "integrated

[1] "Army establishes Army Cyber Command," available at <www.army.mil/article/46012/army-establishes-army-cyber-command/>.

[2] Curtis Boyd, "The Future of MISO," *Special Warfare* 1 (January–February 2011), 22–29.

[3] Air Force Instruction 10-702, *Operations* (Washington, DC: Headquarters Department of the Air Force, June 7, 2011).

[4] Dennis M. Murphy, "The Future of Influence in Warfare," *Joint Force Quarterly* 64 (1st Quarter 2012), 47–51.

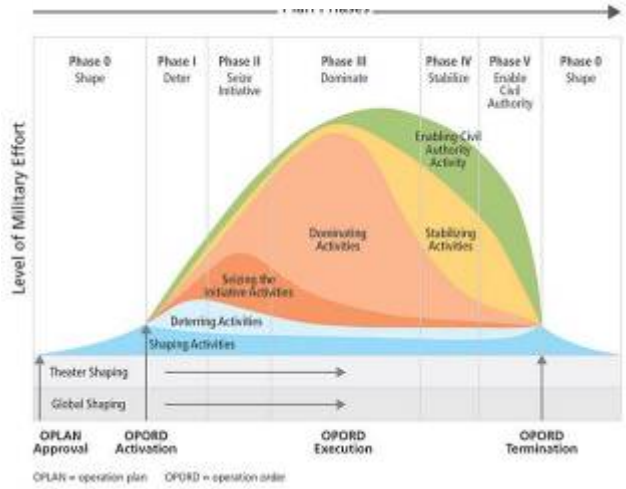
employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[5]

This new definition detaches itself from a reliance on the previously included core capabilities of computer network operations, operations security, and military information support operations—previously known as psychological operations, electronic warfare, and military deception. This change should benefit the force. First, it allows the commander and staff to consider more options for affecting decisionmaking than simply relying upon the previously stated capabilities. Simultaneously, it allows capabilities to grow and change unencumbered by a doctrinal or fiduciary connection to IO. Lastly, the new IO definition recognizes the ability of the commander to affect adversary and potential adversary decisionmaking. All the while, IO remains an integration function, not a capability owner, and one that is directed at foreign rather than domestic audiences.

This new IO definition is a long overdue improvement. Though, one might make the improper interpretation that IO is only about coordinating the themes and messages part of the SC "say-do" rubric as it is included within the same overarching DOD memorandum on Strategic Communication. The Joint Force Commander (JFC) should synchronize communication and operation efforts to support the national level SC process and overall narrative. By conducting IO coordinated with Public Affairs, the JFC can effectively communicate to the variety of intended audiences and affect adversary decision making to maximize effects in the information environment.

Since 9/11 and the start of the war on terror, the author has frequently heard fellow military officers calling for a supporting global IO campaign. These continuous calls are problematic because, doctrinally, IO in itself is not a campaign. The applicability of a global IO campaign can be challenged as the military cannot apply many IO or information-related capabilities, such as military deception or military information support operations, toward a U.S. domestic audience.

**Figure 2. Notional Operation Plan Phases**




Synchronizing communications and actions may not yet be a doctrinal campaign, but it is vital to support a combatant commander's coherent Theater Campaign Plan. For those who insist on some sort of an information campaign, a synchronized communication plan could supplant the heretofore unending calls for an IO campaign. Because of these reasons and the previous IO core capabilities having improved capacity, one might infer that IO is no longer relevant as the strategy's narrative or message would be paramount to all information. However, the narrative without IO is not enough to affect decisionmaking.

At the 2011 World Wide IO Conference, much of the first day's discussion supported the notion that strategic communication and IO are the same. The discussion centered on coordinating geographic combatant command Phase 0 (Figure 2 depicts the notional Phases) messages and the programs that support these activities to shape the operational environment. It was not until the afternoon panel session when Colonel James Gferrer, then commanding officer of the Marine Corps IO Center, commented, "IO is more than just messaging"[6] that the conference discussion duly adjusted. IO is much more than coordinating themes and messages or being the military's version of a chattering class.

While several military information-related capabilities deliver a message that can support communication strategy and IO, IO is still about affecting information content and flow as it relates to adversaries' and potential adversaries' decisionmaking cycles. Synchronized communication itself, while a contributing factor, is not enough to affect adversary and potential adversary decisionmaking because it solely focuses on the broadcast or dissemination of the commander's message.

Even though listening, understanding, and assessing are all part of the communication process, the primary communication goal is to send a message. While important, the commander's message is but one of several

[5] Joint Publication 3-13, *Information Operations* (Washington, DC: The Joint Staff, December 2012

[6] Colonel James Gferrer approved the author using this quotation from an otherwise nonattribution conference discussion.

messages competing for the audience's attention. This only affects the commander's information content output to adversaries and potential adversaries. It does not affect the adversary's information content or flow, neither is it the sole means of protecting the commander's decisionmaking capability. Figure 1 depicts a comprehensive decision–making cycle and annotates how the commander's message is part of the dissemination step within the decision–making cycle. To affect adversial decisionmaking and protect his own, the commander must demand his IO cell look beyond best practices and templated planning. He must insist upon an agile plan capable of affecting the information environment in more ways than coordinated themes and messages.

**More Than Themes and Messages**

Just as J2 has the intelligence and counterintelligence mission and J3 has the fires and counterfires mission, the Information Operations Working Group, on behalf of the commander, should also consider the countermessage mission. Limiting oneself to coordinating and delivering messages as a countermessage mission, however, is insufficient when engaged in a contest as it is both limited and inherently reactive.

Phase 0-Shape is the predominant phase across the combatant commands, and the commander's communication plan should include all information-related capabilities. Still, the IO professional needs to think beyond just messaging. He needs to maintain a holistic perspective of affecting the adversary's decisionmaking cycle to include part of the countermessage mission. In practice, the IO cell needs to consider a counterinformation or even counterdecision cycle approach.

As the Secretary Robert Gates noted to Congress, "adversaries leverage multiple communications platforms, to proselytize, recruit, fund, exercise [command and control], share tradecraft and perpetuate their ideology. Understanding the increasing complexity of the information environment and the compelling need to leverage information effectively as an element of national power is critical to achieving the Department's military objectives."[7]

Other nation-states have acknowledged a similar approach when they removed media access to their countries' populations:

- On February 12, 2010, U.S., British, and German broadcasts accused Iran of deliberately jamming their outputs to deny Iranian citizens access to an opinion that counters the Islamic Revolution.[8]
- On March 12, 2010, Yemeni authorities seized the transmission gear of al Jazeera and al Arabiya channels over their coverage of deadly unrest in the south of the country. Yemeni officials stated such equipment "should not serve to provoke trouble and amplify events in such a way as to harm public order."[9]

Iran and Yemen are not engaged in a legally declared war with one of the offended parties, but they still chose to limit a platform that was disseminating nonsupportive messages. The author does not advocate this tactic as a form of censorship, but instead recognizes the action as part of the IO integrating function. Iran, a US potential adversary, recognizes the value of affecting the information flow of its potential adversaries. IO professionals should understand how to affect the cycle depending on the overall situation more than the designated operational phase. Thus, a geographic combatant commander could ably adjust from Phase 0-Shape to Phase 1-Deter and future phases depicted in Figure 2.

**The Wartime Information Cycle**

Al Qaeda in Iraq (AQI) demonstrated an understanding of using a range of options to affect information during the period of the organization's apex from February 2006 to July 2007. AQI destroyed antiterrorist radio stations in Baghdad, deliberately assassinated Iraqi reporters in Mosul, and lethally targeted U.S. psychological operations teams in an effort to limit the messaging capabilities of AQI adversaries.

Meanwhile, the coalition inclination to counter AQI information was mostly limited to delivering broadcasted messages via handbill, radio, television, or any standard means of communicating across the tactical, operational, and strategic levels. The proclivity toward using paper resulted in an insufficient "death by a thousand paper cuts" approach.

The tactical coalition commanders saw a threat in AQI's Internet presence. This may have warranted a coalition response to deny AQI freedom of access on the Internet. The Internet presence, however, is just the transmission point within the communication process. An Internet video of an improvised explosive device

---

[7] "Request for Support of Funding Authorities to Combat Information Operations," Office of the Secretary of Defense, Washingtono, DC, 2010.

[8] "International Broadcasters Condemn Iran Over 'Jamming,'" BBC, available at <http://news.bbc.co.uk/2/hi/8511921.stm>.

[9] "Yemen Seizes Arab Satellite TV Gear Over Southern Unrest," Agence-France Press, available at <www.google.com/hostednews/afp/article/ALeqM5gkrWanPN6xBGeMX_ax8TdFNrC9Ow>.

destroying a coalition convoy vehicle is the culminating point of the process. A videographer must first record an event and move the video to a point where it can be uploaded to the Internet. Today's videographers often have the means to complete the entire information cycle, thus taking a tactical kinetic attack and transforming it into a strategic information attack.

During this period, a tactical Army division did not have the cyberspace-related means to affect an Internet transmission point and would have had to rely on an operational-level or higher response. If, however, the tactical commander had concerns over an operational- or strategic-level Internet posting, he might have corresponding tactical concern over the videographer's status. The tactical commander could affect the information cycle without relying on a higher element response.

Presuming the videographer broke host nation law by inciting violence toward legal authorities, the tactical commander could realistically interdict the information cycle by arresting the videographer. The terrorist message is never transmitted—or at least it is delayed—and the ability to keep transmitting is affected without having to fight through diplomatic or cyberspace authorities to stop a possible Internet transmission. This is how an IO professional must view the situation.

**Beyond the Information Cycle**

The IO perspective is not limited to counterterrorism or counterinsurgency. It is also applicable in stability or peacekeeping operations (PKO) where adversaries may not be shooting at the U.S. military but are nonetheless in opposition to the combatant commander's objectives and mission. For example, three ethnic groups are vying for position. Two are willing to disarm, but the third and most powerful is reluctant. United Nations (UN) and coalition-led town meetings are popular operations during PKO as a means to bring the belligerent parties closer toward mutual governance. The typical pattern for a town hall meeting is for representatives from the parties to socialize, discuss matters for an hour, come to tentative agreements, and then take a break. During the break, the representatives contact their superiors via mobile devices for further guidance on any tentative agreement. It is not uncommon for one of the parties to return to the meeting with a renewed reluctance to agree with what was otherwise tentatively achieved, such as an agreement to disarm. At this point, the IO professional should consider actions and outcomes to the following possibilities:

- What happens if the town hall representatives are unable to communicate with their superiors during the break and thus unable to renegotiate a new position?
- What happens if a public demonstration calling for immediate disarmament occurs inside or outside the town hall?
- What happens if the host nation media suddenly confront the supreme leader of the most powerful ethic group over his plans to support a tentative disarmament?

The answers to these questions lie in the IO professional's ability to understand the culture, emotion, and status within the adversary's decision cycle and a way to integrate a variety of activities as a means to inform, influence, or even persuade the adversary into taking action favorable to the commander's mission. While the events may occur around the spoken events of the town hall, the message is but a facilitator to something larger.

To accomplish some of these hypothetical tasks, especially disrupting potential commercial communication means, the IO cell should consult with the electronic warfare and staff judge advocate staff to understand the commander's authorities. According to the UN Charter, electronic warfare jamming may violate national sovereignty and be legally construed as an act of war.[10] Likewise, it may violate the UN General Assembly determination that freedom of information is a human right.[11] Still, these determinations may not apply to the situation. To overcome any limitations, the IO staff must make an argument for what the current situation requires as opposed to what the past allowed. Authorities underpin the mission at all levels, and much of the responsibility for acquiring the authorities for the commander rests on the joint IO staff.

**The Authorities Barrier**

In spring 2002, the Coalition Forces Land Component Command (CFLCC) in Kuwait developed the ground invasion plan that became known as Running Start. IO planners embedded within the command's strategic plans and civil military operations teams for planning Phase 2 through Phase 4 operations.

The CFLCC commander was keenly interested in the IO plan to support the invasion and wanted a separate brief on it so he could get more details. The attached plans team developed a thorough plan to use the available IO capabilities to support the land component commander mission to destroy Saddam's ground

[10] United Nations, Charter of the United Nations, 7/51, October 24, 1945, available at <www.un.org/en/documents/charter/chapter7.shtml>.

[11] GA Res 424 (V), UN GAOR, 5th Sess., Supp. No. 20, UN Doc. A/1775 (1950). (Freedom of information is a human right.)

forces by focusing IO efforts to disrupt the decisionmaking of the Iraqi ground forces center of gravity, the Republican Guard. As a supporting effort, IO would influence the Iraqi people not to interfere with coalition operations. The commander optimized the force and plan to swiftly and violently destroy a nation-state military more than stopping to deliver a message to the Iraqis.

The IO planner was cognizant of a variety of capabilities that could achieve palpable effects to support the CFLCC mission. However, the planner knew of problems in attaining authorities for some of these capabilities. For the prebriefing to J3 leadership, the planner inserted a slide titled "Issues" with five bulleted items to acknowledge up front what the IO plan did not cover. As soon as the J3 saw the slide, he directed the IO planner to remove it from the briefing.

The IO planner was too inexperienced to understand the need never to discuss issues with the commander until the staff tried to resolve them first. While the planner was unable to convince the J3 that the issues were germane to the plan, the intermediate leader was too inexperienced with IO to understand why the issues were significant and assist the staff in resolving them.

When the IO team briefed the CFLCC commander, the commander was dissatisfied with the IO plan. He believed that it did not go far enough and push the envelope. The commander thought IO could win the war without firing a shot. Within the first 5 minutes of the briefing, he inquired about three of the five items listed on the excluded "Issues" slide. The IO planner was on the right track, but he did not know how to resolve the authority issues.

Later, open source media reports indicated the coalition tried to influence a coup of Saddam from within his inner circle using emails and other means.[12] While no U.S. or coalition government official or agency has ever confirmed this, the notion of instigating a coup that targeted regime member decisionmaking might have satisfied the CFLCC commander's thirst for a more comprehensive IO plan. The planner's lesson learned was to develop a bold yet feasible plan and then seek the authorities to execute the plan instead of accepting the past authorities as an impediment to future plans.

The IO planner later added a second lesson learned. After further analysis, such an attempt to avoid conflict is an example of deterrence. Shape and deter phases matter. Even though Congress is cutting the DOD budget on such information programs,[13] today's joint force continues to invest more time and effort in planning and executing IO throughout the range of military operations.

**Conclusion**

Joint IO is evolving. The strategic communication process is improving as commander's inform all audiences. IO is much more than coordinating themes and messages. The IO integrator certainly needs to understand the coordinated message but needs to understand the information environment as it relates to the information and decisionmaking cycles of foreign audiences, adversaries, and potential adversaries even more. Communication synchronization is vital, but when the bullets are flying even the best messages are insufficient in affecting decisionmaking.

Future military operations will require IO professionals with an understanding of past authority limitations to explore the realm of the possible and justify new operations originating in the information environment. IO, as these vignettes revealed, is never a "cookie-cutter" or "best practices" solution. Planning and executing IO in accordance with its doctrinal definition requires thought and adaptation facilitated by operational analysis.

Meanwhile, many information-related capabilities are growing in capacity. All of this is for the better as the Defense Department's ability to operate within and affect the information environment remains a growth industry. To make the most of these processes and capabilities, the joint force commander needs a limber staff capable of maximizing the commander's options and minimizing staff frictions in order to achieve the commander's effects and complete the mission. *JFQ*

Table of Contents

## Command and Control Vulnerabilities to Communications Jamming

By Ronald C. Wilgenbusch and Alan Heisig, Joint Forces Quarterly (issue 69, 2nd quarter 2013), April 2013

If the United States ever has to face a peer adversary in a no-holds-barred fight, we will encounter a serious operational obstacle. The way we command and control our forces is highly vulnerable to disastrous

[12] Peter Ford, "Is it too late for a popular uprising inside Iraq? Refugees report signs of unrest in Baghdad," *Christian Science Monitor*, January 27, 2003, 14.

[13] Walter Pincus, "Lawmakers Slash Budget for Defense Department's Information Ops," *The Washington Post*, June 22, 2011, available at <www.washingtonpost.com/blogs/checkpoint-washington/post/lawmakers-slash-budget-for-militarys-information-ops/2011/06/22/AGVC3cfH_blog.html>.

disruption. Modern operations have become dependent on high-capacity communications, and this vulnerability could cause our forces to sustain a serious mauling or, perhaps, not to prevail.

Why is this? The ability to provide the information required for successful high-impact/low-committed asset warfare has developed an overwhelming reliance on unprotected communications satellites. There is an increasing public awareness of these vulnerabilities and the relative ease by which jamming can foil our methods of highly effective warfare. In this article, *jamming* is defined as electronically rendering a circuit or network unusable by disrupting it so it cannot be effectively used as a means of communication for purposes of command and control. Such an attack could be directed against any portion of the communications system and be of extended duration or else just long enough to lose crypto synchronization. Jamming is at the discretion of the enemy. It does not have to be constant or dependent on large fixed sites. It is often difficult to immediately distinguish jamming from other information flow disruptions caused by systemic disturbances such as cryptographic resets, system management changes, and natural phenomena.

**U.S. Air Force maintenance technicians conduct pre-flight checks on RQ-4 Global Hawk unmanned aerial vehicle**
DOD (Andy M. Kim)

While we have placed an appropriate emphasis on cyber warfare, we have neglected the less sophisticated threat of jamming. At some point prior to or during combat, an adversary might decide spoofing, intrusion, and exploitation of our networks are insufficient. The adversary could try to shut our networks down.

Then what? If our networks are jammed, commanders in the field, at sea, and in the air would not be able to employ their forces adequately. Our warfighters are dependent on these links to coordinate joint information, make reports, request supplies, coordinate land, sea, and air operations, and evacuate wounded. Clever application of jamming might go undiagnosed for a long period. Most likely, initial attribution would be to equipment malfunction, crypto problems, or operator error. This dependency is a significant vulnerability—one that can only get worse unless action is taken soon to direct our communication paths toward more protected communications systems.

In 2010, Loren Thompson of the Lexington Institute published an article pointing out this gap in future warfighting capability.[1] He stated that 80 to 90 percent of all military transmission travels on vulnerable commercial satellite communications channels and that only 1 percent of defense communications is protected against even modest jamming. He asserts that the "only satellite constellation the military is currently building that can provide protection against the full array of potential communications threats is the Advanced Extremely High Frequency (AEHF) system. . . . The feasible, affordable answer is not to begin a new program, but to start incrementally evolving AEHF towards a more robust capability." His assessment recognizes the persistent historic demand for greater capacity through satellite communications links.

In January 2012, the Department of Defense (DOD) released its Strategic Defense Guidance entitled *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*. The guidance states, "we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance [ISR]; counterterrorism; countering weapons of mass destruction; operating in anti-access [and area-denial (A2/AD)[2]] environments; and prevailing in all domains, including cyber."[3] We have taken great strides along these lines, but are we fully prepared?

The space-enabled communications systems used by the U.S. military are the most omnipresent information infrastructure to deployed forces. The military depends largely on commercial broadcast satellite systems architectures. In some cases, it leases capacity from the same operators of satellite systems that commercial organizations use. These systems are virtually unprotected against jamming, which is probably the cheapest, most readily available, and most likely form of denying or degrading the reliability of information flow.

Communications networks are decisive in all aspects of U.S. global military responsibilities. Commander of U.S. Pacific Command, Admiral Samuel Locklear, highlighted this issue: "we still have to be able to operate the networks that allow us to produce combat power . . . so one of my priority jobs is to ensure those [command] networks will survive when they have to survive."[4]

**Why So Critical?**

Since the 1980s, the U.S. military's approach to conventional operations has become more dependent on access to space-based systems—particularly long-haul satellite communications and the precision navigation and timing information provided by the Global Positioning System (GPS) constellation. For this reason, the military has invested heavily in developing battle networks to detect, identify, and track targets with sufficient timely precision to enable them to be struck. Intelligence, surveillance, and reconnaissance systems reflect how dependent U.S. forces have become on access to the orbital and cyber dimensions of the global commons.[5]

In concert with the move toward precision munitions, U.S. warfighting doctrine has become inseparably joint at all levels of the Services. Joint coordination between widely dispersed forces is only possible by assured information flows. Moreover, all Services have an increasing realization of their dependencies on protected communications. The protection of information and ability to maintain freedom of maneuver in space is essential to Army success;[6] the highly mobile Army of the future requires communications on the move with networked operations. It depends on the availability of high-bandwidth, reliable, protected satellite communications to achieve this goal.[7] The Air Force is hotly debating the methodologies to ensure space capabilities, including protected communications, at a balanced cost and risk.[8] The Navy has reorganized its entire information apparatus to focus on information dominance as a key element of its future. The Joint Staff has reestablished its J6 Command, Control, Communications, and Computers/Cyber Directorate due to the increased importance of and dependence on assured information technology and networks.

The dependence on information flows (communications) of all kinds has produced superior combat efficiencies and effectiveness. Today's Army uses significantly smaller and dispersed units to operationally control battlespace areas than in prior warfighting constructs. The shift to strategic small units is possible, in part, because of the significantly increased lethality of smaller units enabled by the use of ISR and precision weapons. This precision, however, depends largely on reliable communications. This overall change in operational concepts has become a fundamental shift in military thinking. The Army is starting to build around the platoon level and the Marine Corps around the squad. Special operations forces build around the team. This shift exponentially expands the need for high bandwidth information, particularly ISR.

The ability to provide the required voluminous information has so far developed a strong reliance on unprotected satellites including the ability to use unmanned aerial vehicles (UAVs) and beyond-line-of-sight capabilities for over-the-horizon control and real-time communication. This has led to an increasingly widespread public discussion of the vulnerabilities of using unprotected satellite communications.[9] The ubiquitous use of unprotected commercial wideband satellite communications leads to a false sense of comfort and assurance of availability, which is deceptively dangerous. Jamming is the enemy's side of asymmetric information warfare.

Potential adversaries have a variety of options to accomplish disruption including physical destruction of satellites and ground stations, cyber, and jamming. Jamming is an important element of any communications-denial plan. It is cheap to obtain and simple to operate. It can effectively be used surgically or in broadly based attacks. The absence of planning and programmatic actions to protect against a jamming threat is worrisome given the likelihood of its use.

**Jamming and Antiaccess/Area Denial**

A principal priority of the Strategic Defense Guidance is to project power despite A2/AD challenges.[10] The recent conflicts in Iraq and Afghanistan do not provide experience against an adversary employing significant communications-denial methods. Information access was assured in those conflicts. Potential adversaries in other areas of the world have studied U.S. force enablers for two decades. They realize how dependent we are on assured communications. They understand that the best way to confront U.S. military power is to prevent it from deploying. China, for example, has sent clear signals of its intent through a variety of activities including a naval buildup, submarine deployments, ballistic missiles capable of targeting aircraft carriers,

cyber activities, and an antisatellite demonstration. There can be no question that jamming capabilities would play a significant part in any A2/AD campaign.

**Air Force cadets defend their network during National Security Agency's Cyber Defense Exercise at U.S. Air Force Academy, Colorado Springs**

U.S. Air Force (Raymond McKoy)

The ability to counter area-denial activities depends in many ways on reliable satellite communications capabilities. Such capabilities exist today in China[11] and, by extension, any surrogate or client regimes with area-denial agendas. U.S. forces must be able to operate in this challenging environment. The obvious counter to jamming is to protect communications for operational forces. The necessity for protected communications is not limited to A2/AD scenarios. A striking example is the strong reliance by the Intelligence Community on UAVs for tactically relevant information supporting ground troops. These vehicles require wideband satellite communications systems for over-the-horizon control and real-time information dissemination. Future tactical forces will rely on robust and reliable information systems. They are at huge risk to jammers.

China and Russia have well-documented satellite jamming capabilities. Some versions of militarily effective jammers are even commercially available.[12] The proliferation of jamming technology has led to an increasing utilization of strategic and tactical jamming.[13] Satellite jamming, in particular, is proliferating. Military jamming equipment can be purchased on the Internet by anyone, including nonstate actors. The attraction of this economical, highly effective capability to disrupt vastly superior forces is an ominous reality. The omnipresent capability by widely divergent players almost guarantees that jamming source attribution will be a problem even after detection is accomplished.

In February 2012, the United Nations International Telecommunications Union hosted the World Radiocommunications Conference in Geneva. In recognition of the upswing of satellite jamming in 2011, the union issued a change to its regulations and a call to all nations to stop international interference with satellite telecommunications.[14] Moreover, recent incidents illustrating the need for action were the jamming of satellite operators EUTELSAT, NILESAT, and ARABSAT.[15] Jamming has occurred from a variety of locations recently across the globe. Interference with satellite television broadcasting has come from Indonesia,[16] Cuba,[17] Ethiopia,[18] Libya,[19] and Syria.[20] Additionally, in the case of Libya, the use of tactical jamming of satellite telephones was reported during the course of combat operations.[21]

The proliferation of jamming does not have to depend on land-based fixed or mobile facilities. China is not tied to castoff Soviet naval designs. The People's Liberation Army Navy (PLAN) has small, fast, and capable craft with good seakeeping capabilities such as the *Houbei* missile attack craft. Even a cursory look at the craft's superstructure shows that attention is paid to shipboard electronics. The superstructure could be equipped with powerful jammers and operated collaboratively far from U.S. forces. This could seriously complicate U.S. naval or air power projection. The PLAN continues to field these state-of-the-art, ocean-capable, wave-piercing aluminum hull SWATH craft. According to in-country open sources, by February of 2011, the PLAN had fielded over 80 type 22 *Houbei*-class fast attack craft, and the number is growing.[22] The question is no

longer who has jamming capabilities but, rather, have we prepared to operate effectively when it happens. At present, the answer is a resounding no.

**Causes and Actions**

Historically, protected communications were viewed as the realm of strategic existential threats to the Nation. The underlying principle of U.S. protected communications continued to have its raison d'être linked to nuclear communications survivability and essential, highest-level command and control. The approach was heavily focused on getting through a small number of human-to-human messages on which dispersed forces could execute preplanned objectives. This focused view kept protected communications capability development geared toward the "Armageddon" context and did not significantly influence tactical requirements.

During Operation *Desert Storm* in 1991, laser-guided bombs, Tomahawk land-attack missiles (TLAMs), and the GPS-aided conventional air-launched cruise missiles demonstrated that U.S. forces had the capability to hit almost any target whose location could be pinpointed. For this reason, the U.S. military has invested heavily in developing battle networks to detect, identify, and track targets with sufficient timely precision to enable target strikes. ISR systems such as the RQ-4 Global Hawk, GPS constellation, and photoreconnaissance satellites reflect how dependent U.S. forces have become on access to the orbital and cyber dimensions of the global commons.[23] The preplanned targeting initially envisioned for these types of precision weapons incrementally has given way to a need for real-time responsiveness.

*Desert Storm* also highlighted the inadequacy of the existing satellite communications architecture. The starkest reality was the inability to transmit large data files to tactical forces. The air tasking order (a daily compilation of all joint and coalition aircraft planning and execution) was unable to reach the significant airpower resident on Navy carriers. The reprogramming of TLAMs, laser-guided bombs, joint direct attack munition, and other precision munitions took exceedingly long times to transmit and overwhelmed the beyond-line-of-sight systems of the day.

The vulnerability of unprotected broadband communications went unchallenged in the last two decades. Recent conflicts have not been fought against major adversaries with comparable capabilities.[24] The U.S. military was able to accomplish its ends cheaply by taking advantage of a commercial overbuilding of satellite communications capacity in the late part of the last century and the early years of this one. That convenient resource is no longer available. Market developments have made commercial leasing a much more expensive alternative. Moreover, commercial communications satellites retain their inherent jamming vulnerabilities.

Realization and Acceptance of the Requirement

The paucity of protected communications below the highest levels of requirements of nuclear command and control is starting to wend its way into the thinking of military leadership. A 2010 Defense Intelligence Agency (DIA)–sponsored wargame, with over 60 Active-duty troops and civilian representatives from each of the Services, tried to grapple specifically with the loss of assured satellite communications. The players made several key comments as they became aware of the impact of threats to existing warfighting doctrine. The consensus among participants was that "significant risk" to mission success occurred when protected beyond-line-of-sight communications were limited to existing capabilities. In the presence of even modest jamming capability, participant reaction was to revert to Cold War–era doctrine and tactics.

**Arleigh Burke–class guided missile destroyer USS Hopper (DDG 70), equipped with Aegis integrated weapons system, launches RIM-161 Standard Missile**
DOD

Those reactions were immediately frustrated by a lack of available older systems; the infrastructure to accomplish those doctrines and tactics no longer exists. The combat functions of planning, command and control, movement and maneuver, intelligence, fires, force protection, logistics/personnel support, and special operations were all significantly or critically degraded. Additionally, there were issues with force structure, organization, training, and equipment. Essentially, the entire spectrum of warfighting capability beyond preplanned initial insertion and organic logistics was significantly adversely affected. These risks translated into longer engagement timelines, increased casualties, and the need for a larger force structure for each mission and reduced multimission capability.[25]

The wargame specifically focused on satellite jamming as the most mature and economically available means to deny satellite capability. The issue of physical destruction of orbital assets was not addressed as it had several military/political elements that were deemed too expensive or carried a significantly disproportionate geopolitical risk. The same denial effect is achieved by spot jamming without the protagonist having to develop physical methods of interfering with space-related infrastructure.

Pinpointing the source of jamming is not easy. Jammers can appear innocuous and can be quite mobile. They can be intermittent in operation. A jammer can physically appear as some sort of commercial system, such as a news uplink vehicle or normal receive antenna on a fixed site.

We have many lessons to draw on that point to a future where a large component of beyond-the-horizon communications must be protected. Given the huge advantages that space communications provide, it makes sense to protect the capability against the inexpensive and ubiquitous development of disruptive capability by potential adversaries. The risk of not protecting it is an exponential rise in force structure and cost coupled with the plummeting warfighting effectiveness of existing forces. Accordingly, DOD will continue to work with domestic partners and international allies and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space.[26] In the President's words, "Going forward, we will also remember the lessons of history and avoid repeating the mistakes of the past when our military was left ill-prepared for the future."

**Are There Options?**

Optimists would say that the picture is not so grim—that there *are* options. So what might these options be if or when we encounter an enemy who wishes to shut down our communications? How quickly can we turn options into operational capabilities? Are these really viable options that will keep our forces fighting as they have trained?

The most frequently discussed option is that we would "go old school." Participants in the previously mentioned DIA-sponsored wargame suggested that they could still accomplish their warfighting missions by using old-school techniques such as high-frequency (HF) radio links. But, on examination, they came to realize that this is not viable. The worldwide system of fixed HF transmitters and antennas that was once the

mainstay of our HF communications systems is gone. Even if it was still in place, the skilled HF operators needed aboard ships and ashore have been cashing retirement checks for years.

There is a more basic issue. Our satellite links have enabled completely different types of operational communications and tactics and procedures that cannot be supported on HF. This includes high bandwidth machine-to-machine data exchanges, video teleconference, Web sites, chat, email, and other mechanisms that in a large context allow decisionmaking to be viable at low levels in the chain of command. That is the fundamental capability that enables quick, adaptive, and effective warfighting that exponentially multiplies smaller force capabilities. Yet going old school, reverting to HF, was exactly the alternative a senior Navy officer suggested as the course of action in trying to overcome a potential jamming threat at the 2012 Navy Information Technology Day briefing.

**U.S. Soldiers set up tactical satellite communication system in Shekhabad Valley, Wardak Province, Afghanistan**
U.S. Army (Russell Gilchrest)

A second knee-jerk option is that we would "shoot the jammer." This is a nonstarter. Almost everyone has seen the massed army of television trucks/vans wherever and whenever some sensational news event occurs. Imagine downtown Baghdad or Kabul with the same number of trucks. Any one of them could be a jammer. Which one should be shot, and how long would it take to sort them out? Even if the jammer was working in the middle of an open desert in enemy-controlled territory, it would still be a tough target. The jammer could stand out in the open just long enough to disrupt the crypto set on the link/network. Then it could go silent, move to another location, or focus on another satellite link. As mentioned, operators frequently confuse jamming with equipment problems or a self-imposed mistake. At best, locating and shooting the jammer is a difficult targeting problem that would certainly tax the intelligence and strike assets assigned to other high-value targets.

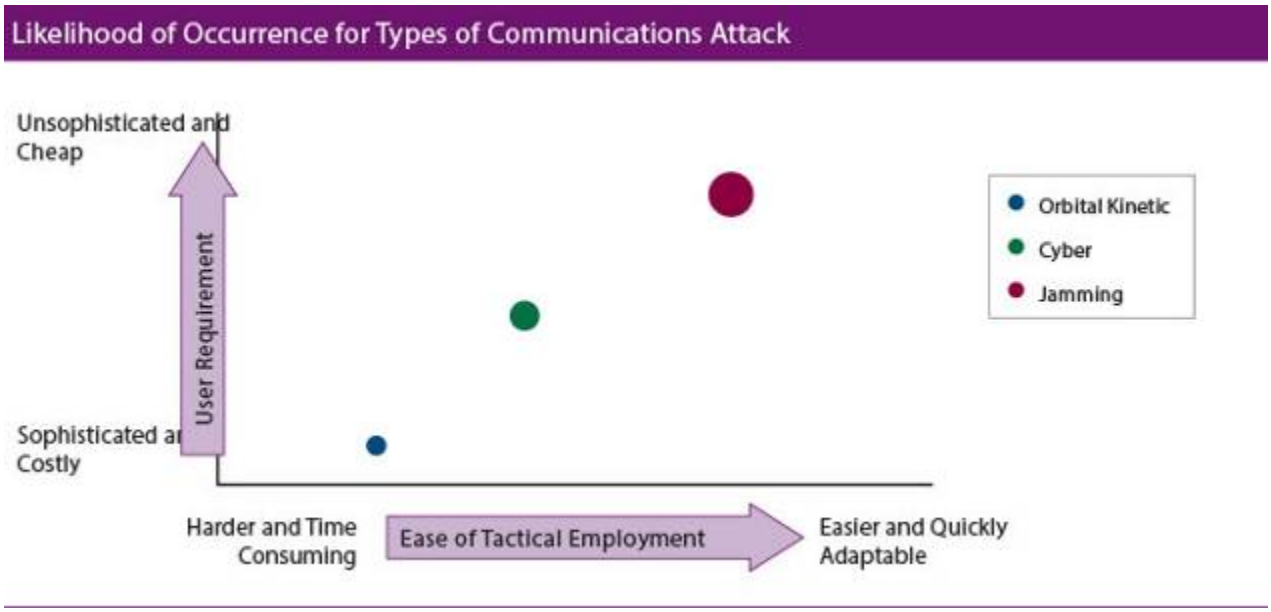
A third option is that we would attempt to reconstitute the satellite constellations by rapidly replacing capability on orbit. This usually implies a set of smaller satellites already in storage. It also means the availability of a nearly immediate launch period acceptable for military operations. However, replacing one disrupted satellite with another equally vulnerable to jamming hardly seems to solve the problem. Furthermore, none of the smaller satellites that have been proposed has the capability to replace the types of satellites used today. At present, there are simply not enough launch vehicles or launch sites available to support such an alternative.

A fourth option might be to design an entirely new satellite system with new features. This is theoretically feasible. However, it is hard to envision what this solution additionally offers in the sense of timeliness, cost reduction, and operational improvement over expanding the constellation of existing protected communications satellites such as advanced extremely high frequency (AEHF) ones. The current and evolving technology is understood and carries known programmatic risk. We can certainly improve and expand the AEHF constellation much faster than engage in multiple new technology program starts.

A fifth option is centered on redundancy. In this alternative, even though most communications links are not protected, there are many of them. It is hard to imagine an adversary who could take the entire infrastructure down simultaneously. High-level DOD officials have suggested that an enemy might be able to mount a jamming attack that would leave operational forces with only about 60 percent of our present capability. But when was the last time we were using only 60 percent of our satellite communications capacity?

We must further assume that an intelligent enemy would have at least determined our most critical links to operations in progress. Those are likely to be the first to go. More concerning is the fact that a swept tone jammer could take out all our links, or certainly more than DOD officials estimate. The 60 percent figure appears unsupported by analysis.

In any event, forces experiencing jamming without prior training and a management plan would create operational chaos. Managing heavy jamming attacks in this environment becomes an effort to plan for gradual degradation of communications. Operational concepts must be modified on the fly as individual circuits are lost. Training must also be conducted both to recognize and counter jamming as it occurs. These actions should be pursued. It appears at present that little progress has been made in this direction. The reality is that many important circuits have no backup. For example, many UAVs have only one form of over-the-horizon communication available. It would not be difficult for an adversary to learn where to target his jamming efforts for the greatest effect against UAVs.




It has been suggested that the present military satellite communications system is composed of too many and too large satellites that are overly vulnerable, overly complex, and unnecessarily costly. The proposed solution is to develop and deploy disaggregated system architecture to replace present architectures.

There are two obvious problems with this suggestion. First, it presupposes that there is a disaggregated architecture that would offer the same capability at a reduced deployed cost. In order to make a disaggregated satellite constellation acceptable from a cost standpoint, it would have to be supported by math to show that it is less expensive than the evolving current highly effective and efficient systems. Second, it is suggested that disaggregation would reduce vulnerability, but in fact no amount of disaggregation could offer protection against effective jamming or ASAT attack. Furthermore, simple logic would tell us that, if it is known that an attack on our *strategic* antijam main asset, AEHF, is tantamount to an act of war, extending the use of that same asset to provide secure coverage for both tactical and strategic forces would make the tactical support more secure simply by being on the same strategic asset. On the other hand, disaggregating the two missions on different satellites would seem, from a logic standpoint, to make the disaggregated tactical asset more vulnerable to attack. After all, would jamming one of many tactical assets be considered an act of war? Additionally, a disaggregated architecture presents questions of technical risk and complexities not yet answered.

Of course, there are other alternatives, such as adding antijam capability to unprotected wideband systems. The properties of transmission physics dictate that an increase in antijam capability implies modifications to the waveform that would, of necessity, cause a reduction of the data rate. There are no halfway measures.

There is no point in adding just a "little antijam." We either defeat the jamming capability or we do not. So we have to be prepared to defeat the most likely jamming threats.

One alternative put forth that seems to offer potential is to supplement the existing satellite system through the development of the Aerial Layer Network (ALN). However, like an entirely new satellite system, it is not fully defined and has yet to be built. ALN is a solution that might be able to take existing satellite technology, scaled down in size but not in capability, and have it ready for rapid deployment to enable our forces to operate in some scenarios in the face of jamming. This involves engineering developments that carry all the risks of any new start. By its nature, it is best used in a permissive environment or one with airspace dominance. This concept seems ripe for use as a pseudosatellite augmentation to support a land area of operations or a battlegroup maneuvering at sea.

Dr. Thompson's thesis of incrementally expanding the capability of AEHF is not sufficient; it should be matched with a realization that the EHF spectrum also contains the capability to accommodate a wide variety of high bandwidth requirements. This could provide ground, maritime, and atmospheric forces with the protected wideband capabilities that complement the mobile, highly integrated forces the U.S. military fields today and will field tomorrow.

## Conclusion

Jamming is a highly effective technique that could cripple U.S. military operations, and our potential adversaries know it and have the capability to employ it. We should not underestimate what they might do. Realizing our current operational dependency on reliable high data rate communications, and considering the attractiveness and availability of jamming to potential adversaries, we have only two choices. The first is to reduce our dependency on communications—an unlikely alternative for obvious reasons. Doing so would reduce operational effectiveness and require a correspondingly larger and more expensive force structure. It should be obvious that the way we have learned to fight over recent years simply will not allow a reduction in the amount of communications capacity we will need.

The second choice is to ensure that our communications infrastructure is sufficiently resilient to withstand the type of attack discussed herein. As one unnamed senior officer put it, in our present situation and failing to add more protected communications, we could be "out of Schlitz by noon on the first day of battle." This is clearly not where we ought to be. Increasing the capacity of protected communications is an essential part of this latter alternative.

Failure to address the predictable jamming threat could (*will*) lead to mission degradation or failure. The time to act is now ***JFQ***

### Notes

1. Loren B. Thompson, "Lack of Protected Satellite Communications Could Mean Defeat for Joint Force in Future War," *Lexington Institute Early Warning Blog*, April 14, 2010, available at <www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war>.
2. *Antiaccess/area denial* is defined thusly: "anti-access capabilities [are] ones that slow deployment of friendly forces into a theater, prevent them from operating from certain locations within that theater or cause them to operate over longer distances than they would like. Area-denial efforts are those that reduce friendly forces' freedom of action in the more narrow confines of the area under the enemy's direct control." See Phillip Dupree and Jordan Thomas, "Air-Sea Battle: Clearing the Fog," *Armed Forces Journal* (June 2012), available at <www.armedforcesjournal.com/2012/05/10318204>.
3. *Sustaining U.S. Global Leadership: Priorities for 21*st *Century Defense* (Washington, DC: Department of Defense, January 2012).
4. Admiral Samuel J. Locklear, USN, U.S. Pacific Command change of command address, March 2012.
5. Barry D. Watts, *The Maturing Revolution in Military Affairs* (Washington, DC: Center for Strategic and Budgetary Assessments, 2011).
6. U.S. Army Training and Doctrine Command (USTRADOC), *The United States Army Operating Concept*, TRADOC Pamphlet 525-3-1 (Fort Monroe, VA: Headquarters Department of the Army, August 19, 2010), available at <www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf>.
7. Warfighter Information Network–Tactical Commanders Handbook, Version 1.6.
8. C. Robert Kehler, "Implementing the National Security Space Strategy," *Strategic Studies Quarterly* (Spring 2012), 18–26, available at <www.au.af.mil/au/ssq/2012/spring/kehler.pdf>.
9. "Protecting [unmanned aerial vehicle] satellite communications links also will be an important challenge in the future," stated Stuart Linsky, vice president of communications systems at Northrop Grumman. "Where it once took an advanced nation state to jam U.S. military communications, new ubiquitous technologies now expose unmanned systems to jamming and cyberattacks. 'The ease with which the bad guys can do bad things has gotten easier.'" See Henry Kenyon, "New satellite capabilities target UAV needs: Waveforms and spacecraft help support warfighter mission requirements," *DefenseSystems.com*, March 15, 2012, available at <http://defensesystems.com/articles/2012/03/15/satellite-2012-uav-satellite-needs.aspx>.
10. *Sustaining U.S. Global Leadership*.
11. Andrew Erickson, "China Testing Ballistic Missile 'Carrier-Killer,'" *Wired*, March 29, 2010, available at <www.wired.com/images_blogs/dangerroom/2010/03/asbm_graphic_admiralwillard-testimony_chinese-article.png>.
12. Available at <http://jammerfactory.en.made-in-china.com/product/DMcQoSIPCNWE/China-100W-Military-Communications-Jammers-Backpack-Blockers.html>.
13. Electronic and information warfare techniques including hacking into computer networks and electronic jamming of satellite communications links are negation capabilities that are becoming increasingly available to both state and nonstate actors. A number of incidents of electronically jammed media broadcasts have been reported in recent years, including interruptions to U.S. broadcasts to Iran, Kurdish news broadcasts, and Chinese television (allegedly by the Falun Gong). Iraq's acquisition of Global Positioning System (GPS)–jamming equipment for use against U.S. GPS-guided munitions during Operation *Iraqi Freedom* in 2003 suggests that jamming capabilities are proliferating; the equipment was reportedly acquired commercially from a Russian company. See *Space Security 2007* (Waterloo, ON: Project Ploughshares, August 2007), available at <www.spacesecurity.org/SSI2007.pdf>.
14. "International Broadcasters Call for End of Satellite Jamming," Broadcasting Board of Governors, January 24, 2012, available at <www.bbg.gov/press-release/international-broadcasters-call-for-end-of-satellite-jamming/>.

15. See David Klinger, "Satellite-jamming becoming a big problem in the Middle East and North Africa," March 28, 2012, *Arstechnica.com*, available at <http://arstechnica.com/science/news/2012/03/satellite-jamming-becoming-a-big-problem-in-the-middle-east.ars>.

16. Recent examples of satellite jamming include Indonesia jamming a transponder on a Chinese-owned satellite and Iran and Turkey jamming satellite television broadcasts of dissidents. See "Space, today and the future," available at <www.dod.mil/pubs/spacechapter2.pdf>.

17. Broadcasting Board of Governors, Washington, DC, July 15, 2003.

18. "Ethiopia Jamming Eritrean Television, Knock out own Satellite channel," available at <www.topix.com/forum/world/eritrea/TKPS5MNR2DH67LOFM>.

19. Peter B. de Selding, "Libya Accused of Jamming Satellite Signals," *Space.com*, March 1, 2011, available at <www.space.com/11000-libya-satellite-jamming-accusations.html>.

20. The Obama administration asserts that the Syrian government, with Iran's help, is actively jamming private communications and satellite Arabic television networks in an aggressive campaign to cut off antigovernment organizers from the outside. See "Officials: Obama ramps up aid to Syrian opposition," Associated Press, April 13, 2012, available at <www.usatoday.com/news/world/story/2012-04-13/syria-un-annan/54258456/1>.

21. "Thuraya Accuses Libya of Jamming Satellite Signals," *SpaceNews.com*, February 25, 2011, available at <www.spacenews.com/satellite_telecom/110225-thuraya-accuses-libya-jamming.html>.

22. David Lague, "Insight: From a ferry, a Chinese fast-attack boat," Reuters, May 31, 2012, available at <www.reuters.com/article/2012/05/31/us-china-military-technology-idUSBRE84U1HG20120531?goback=.gde_104677_member_120627756>.

23. Watts.

24. Ibid.

25. Verbal assessment comments from Protected Communications Wargame Outbrief, May 26–27, 2010.

26. *Sustaining U.S. Global Leadership.*

Table of Contents

# China's Internet: A Giant Cage

From the Economist, Apr 6th 2013

THIRTEEN YEARS AGO Bill Clinton, then America's president, said that trying to control the internet in China would be like trying to "nail Jell-O to the wall". At the time he seemed to be stating the obvious. By its nature the web was widely dispersed, using so many channels that it could not possibly be blocked. Rather, it seemed to have the capacity to open up the world to its users even in shut-in places. Just as earlier communications technologies may have helped topple dictatorships in the past (for example, the telegraph in Russia's Bolshevik revolutions in 1917 and short-wave radio in the break-up of the Soviet Union in 1991), the internet would surely erode China's authoritarian state. Vastly increased access to information and the ability to communicate easily with like-minded people round the globe would endow its users with asymmetric power, diluting the might of the state and acting as a force for democracy.

Those expectations have been confounded. Not only has Chinese authoritarian rule survived the internet, but the state has shown great skill in bending the technology to its own purposes, enabling it to exercise better control of its own society and setting an example for other repressive regimes. China's party-state has deployed an army of cyber-police, hardware engineers, software developers, web monitors and paid online propagandists to watch, filter, censor and guide Chinese internet users. Chinese private internet companies, many of them clones of Western ones, have been allowed to flourish so long as they do not deviate from the party line.

If this special report were about the internet in any Western country, it would have little to say about the role of the government; instead, it would focus on the companies thriving on the internet, speculate about which industries would be disrupted next and look at the way the web is changing individuals' lives. Such things are of interest in China too, but this report concentrates on the part played by the government because that is the most extraordinary thing about the internet there. The Chinese government has spent a huge amount of effort on making sure that its internet is different, not just that freedom of expression is limited but also that the industry that is built around it serves national goals as well as commercial ones.

### Walls have ears

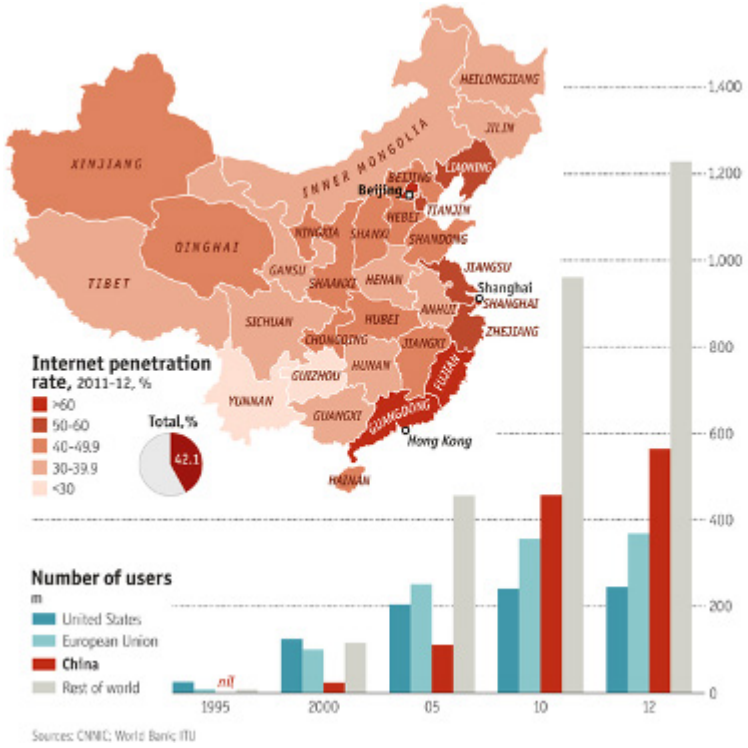
Ironically, the first e-mail from China, sent to an international academic network on September 14th 1987, proclaimed proudly: "Across the Great Wall we can reach every corner in the world." Yet within China's borders the Communist Party has systematically put in place projects such as the Great Firewall, which keeps out "undesirable" foreign websites such as Facebook, Twitter and YouTube, and Golden Shield, which monitors activities within China. It has also worked closely with trusted domestic internet companies such as Baidu (a search engine), Tencent (an internet-services portal), Renren (China's leading clone of Facebook) and Sina, an online media company that includes Weibo, a Twitter-like microblogging service.

Of all these newcomers, microblogging has had much the biggest impact on everyday life in China. It has allowed the spread of news and views in ways that were not previously possible, penetrating almost every internet-connected home in China. The authorities, having blocked Twitter and Facebook early on, allowed Chinese microblogs and social-media services to develop as trusted and controlled alternatives. They grew exponentially, far beyond anything that Twitter achieved in the Chinese market.

Google, the West's foremost search company, hesitantly tried to play by China's rules for a while, introducing a self-censored search engine there in 2006, but eventually withdrew that service in 2010, not so much because of the restrictions imposed on it but because it was being hacked by the Chinese. China's cyber-hackers continue routinely to break into the e-mails of dissidents as well as into the computer systems of foreign media that report sensitive stories on China's leaders. They have recently made headlines by stealing the technology of American defence firms and probing critical American infrastructure for vulnerabilities. Numerous hacking attacks abroad have purportedly provided Chinese firms with sensitive commercial information and given the People's Liberation Army valuable insights into other countries' defence apparatus.

The party has achieved something few had thought possible: the construction of a distinct national internet. The Chinese internet resembles a fenced-off playground with paternalistic guards. Like the internet that much of the rest of the world enjoys, it is messy and unruly, offering diversions such as games, shopping and much more. Allowing a distinctly Chinese internet to flourish has been an important part of building a better cage. But it is constantly watched over and manipulated.

Sometimes the authorities' efforts at controlling it are absurd, even ridiculous, but the joke is on the users. Government agencies across the country have invested heavily in software to track and analyse online behaviour, both to gauge public opinion and to contain threats before they spread, and the authorities deal ruthlessly with those who break the rules. In 2009 Liu Xiaobo, a Chinese writer, was sentenced to 11 years in prison for co-writing an online manifesto calling for an end to authoritarian rule and asking for signatures in support. At the time few in China had heard of Mr Liu, a much-jailed democracy activist, and not many saw the declaration. He became famous outside China when he was awarded the Nobel peace prize in 2010 but is still largely unknown within the country because of strict censorship (his name is among a huge and growing number of "sensitive keywords" which are blocked online).




Also in 2009, after riots in Xinjiang, a remote north-western region, the authorities shut off the area's internet from both the rest of China and from the world. By flipping an internet "kill switch", they isolated the area for almost a year. And in March 2012, when social media carried rumours of an attempted coup in Beijing, the government temporarily shut down some of the internet's microblogging services and detained six people.

**Wobbling Jell-O**

Will the Chinese state be able to go on controlling, manipulating and hacking the internet indefinitely? There are reasons to think it will not. When Mr Clinton made his famous remark about nailing Jell-O to the wall, only 20m people in China were online. Now the cage strains to hold in excess of 560m, almost as many as the online population of North America and Europe combined. The fastest growth in internet use is in China's poorer, more rural provinces, partly because of a surge in users connecting via mobile devices, which now outnumber those connecting from computers. The internet is no longer confined to an urban, educated and relatively well-off public. Most farmers are getting online to listen to music, play mobile games and check the weather, not blog dissent. But even casual users can be drawn into political debates online, and the internet is one place where people can speak their minds and criticise the government relatively freely.

In private they have always grumbled, and families at their dinner tables have scoffed at the propaganda served up on state-run television. But being able to express diverging views collectively online is new. Millions of users are low-grade subversives, chipping away at the imposing edifice of the party-state with humour, outrage and rueful cynicism. Only those deemed to be threatening the state—on a very broad definition that can include being critical of a leader, or airing some grievance—are singled out for punishment.

Sometimes online complaints do produce results, swiftly bringing offenders to book. When an army political commissar got abusive with a flight attendant, she posted photographs of the incident. Internet users soon ferreted out his name, job title and location and he was eased out of his job. When an official was photographed smiling at the scene of a gruesome accident, the online crowd noticed he was wearing a luxury watch and quickly came up with more photographs of the same official wearing other luxury watches. "Brother Watch", as he came to be known, was fired.

Small victories like this are becoming increasingly common, to the dismay of millions of Communist Party cadres. Many web users believe that the balance of power has shifted: in a survey conducted in 2010 by a magazine affiliated to the *People's Daily*, the party mouthpiece, more than 70% of respondents agreed that local Chinese officials suffered from "internet terror".

Yet for the party as a whole the internet holds much less terror than it does for local officials. The online mob can gorge itself on corrupt low-level officials because the party leaders allow it. It can make fun of censorship, ridicule party propaganda and mock the creator of the Great Firewall. It can lampoon a system that deletes accounts and allows them to pop up again under a new name, only for the new accounts to be deleted in turn. It can rattle the bars of its cage all it likes. As long as the dissent remains online and unorganised, the minders do not seem to care.

At the same time, though, the more sensitive tweets and blog posts, attacking senior party leaders by name or, most serious of all, calling for demonstrations in the real world, are quickly deleted, sometimes before they even make it onto the web. Activists who directly challenge the central party organisation or attempt to organise in numbers (like Mr Liu) are crushed long before they can pose a threat. (Pornography is also officially censored, though it proliferates nonetheless.) The rest of the chaotic internet that takes up people's time, energy and money carries on, mostly undisturbed. Dissident activity plays only a small but potent part in the overall mix.

**Adaptive authoritarianism**

For the party leaders the internet has created more subtle challenges. Collective expression on the web, led by civic-minded microbloggers with millions of followers, is focusing attention on recurring problems such as food safety and pollution, showing up the gap between expectations and performance. That means the authorities now have to try to come up with credible responses to crises such as the huge spike in air pollution in January and February. In short, the internet requires the party centre to be more efficient at being authoritarian.

This is the online blueprint for what scholars call "adaptive authoritarianism", and there is an international market for it. China sells its technological know-how abroad, including tools for monitoring and filtering the internet. Huawei and ZTE, two big Chinese companies, are leading suppliers of internet and telecoms hardware to a number of states in Central and South-East Asia, eastern Europe and Africa, including Kazakhstan, Vietnam, Belarus, Ethiopia and Zambia. Many of these would like to increase online access while retaining tight political and technological control. China has aligned itself with these countries and dozens of others, including Russia, in a global dispute with Western democracies over how the internet should be governed.

Dissidents in China say that freedom is knowing how big your cage is. It could be argued that with their internet the Chinese authorities have built one of the world's largest, best-appointed cages. It could equally be said that they have constructed an expensive, unwieldy monstrosity, a desperate grab for control to buy time for the party. Either way, a careful look at their edifice should throw light on the question whether the internet is an inherently democratising force. This special report will show how they built it and ask if it can last.

Table of Contents

## Cat and Mouse: How China Makes Sure Its Internet Abides By the Rules

From the Economist, Apr 6th 2013

The history of the internet in China is one of give and take, of punch and counterpunch, where the authorities are often surprised by the force and speed of online interactions but determined to keep them under control. The result has been a costly and diverse industrial complex of monitoring and censorship. Central-government ministries have invested in two pillars of control: the Great Firewall, a Western name for a system of blocking foreign websites, starting in the late 1990s, which some believe has cost as much as $160m (the details are state secrets); and Golden Shield for domestic surveillance and filtering, begun in 1998 by the Ministry of Public Security and estimated to have cost more than $1.6 billion so far.

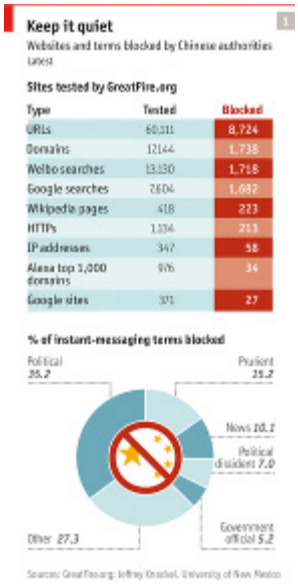
A number of other government departments have their own internet divisions. Many provincial and local governments, too, officially responsible for internet management in their area and keen not to be caught out by local unrest, have invested in their own tailored monitoring systems. More than 100 Chinese companies have made a total of at least 125 products for monitoring and filtering public opinion online, according to a Chinese government register. The most expensive of the publicly disclosed government purchases reviewed by *The Economist* was bought by Beijing's internet-propaganda office for $4.3m. (One foreign supplier, Hewlett-Packard's Autonomy unit, devised an online public-opinion monitoring system for the Chinese market in 2006 and has had some takers in government.)

One of the suppliers to government, Founder, created by Peking University, describes to potential customers how it helps overworked government staff by monitoring hundreds of domestic websites and overseas Chinese sites. "The early-warning [feature] monitors sensitive information which needs to be dealt with immediately…such as June 4th [the date of the Tiananmen Square crackdown in 1989 and] Charter 08 [Mr Liu's anti-authoritarian manifesto]." The authorities have learned to watch out for ingenious variants of June 4th, including May 35th, April 65th and March 96th. The Founder system also monitors material that may "prompt mass incidents in society and on campus".

In addition, a number of black-market internet companies sell services to individuals, including the deletion of negative articles from websites, using connections in government and at the big internet companies, sometimes at a cost of hundreds of thousands of dollars. Some 60% of the profits of one such company in Beijing, Yage Time Advertising, came from sales to local officials in smaller Chinese cities who wanted to delete negative reports about themselves, according to *Caixin*, a Chinese financial magazine. The software system for detection and filtering that Yage was offering these officials cost $64,000. Yage was busted by police in July last year, but the unofficial business of deleting posts—and of planting negative ones and of selling "zombie" followers and retweets of posts—continues to flourish.

**Manual labour**

Surprisingly, the machinery of control is far from monolithic, and rife with inconsistencies (especially from province to province: one study found that more than half the microblog posts in Tibet were deleted, compared with barely a tenth in other provinces). It is also much less automatic than might be expected. Academic studies of Chinese censorship show that for all the software and hardware involved in detecting and filtering content, much of the deleting is done manually, blog post by blog post, tweet by tweet. This system requires a substantial investment in people, perhaps as many as 100,000 of them. That includes internet police (20,000 or more), propaganda workers and in-house monitors at thousands of websites, from small discussion forums to behemoths like Tencent and Sina. A recent study reckoned that Sina Weibo, the country's main microblog, currently employs more than 4,000 censors.




This model seems to have a number of drawbacks. Humans make mistakes and can be overwhelmed, as they appeared to be after the crash in 2011 of a high-speed train near Wenzhou, when all of Sina's censors (then numbering only 600-plus) were called in to help, according to *Phoenix Weekly*, a magazine. Such a crisis can put intense strain on these individuals. Some disgruntled or liberal-minded employees clearly view the system as flawed and are providing information about its shortcomings to overseas sites. China Digital Times, a blog run by a dissident exile, Xiao Qiang, from the University of California, Berkeley, regularly publishes transcriptions of propaganda directives under the heading "Ministry of Truth".

For the most part, though, these workers accept the system, and not just because of Communist Party indoctrination and discipline. The party has cells inside most, if not all, of the big internet companies and makes sure that some key posts go to party members. Party leaders have also consistently worked on keeping the big web companies' CEOs loyal. Since 2003, when Hu Jintao became president, the web bosses have been invited on annual "red tours" of historic communist sites. Baidu's co-founder, Robin Li, and Sina's CEO, Charles Chao, have been on many such trips. (Mao Daolin, a Sina CEO before Mr Chao, demonstrated his loyalty by marrying Mr Hu's daughter in 2003.) Disciplinary sanctions also play a part. Internet companies that flout the rules, as some do in an effort to increase traffic, are suspended or shut down altogether. Companies that play by the rules can thrive, but have to budget for employing lots of censors.

For thousands of individual censors to do their jobs willingly and effectively, the system must have a fundamental logic. As it turns out, the party applies the same strict rules online as it has done on the ground

since the Tiananmen Square crackdown of 1989: do not jeopardise social stability, do not organise and do not threaten the party. In a study of deletions of Chinese blog posts in 2011 and 2012, researchers at Harvard found that posts which were merely critical of government policies were tolerated. The ones most likely to get deleted were those that might trigger collective action such as protests. This was true even for posts that appeared to be pro-government.

The authorities have been strikingly consistent in applying this rule. The earliest significant act of domestic internet censorship, in September 1996, was to shut down an online discussion forum at Peking University, "Untitled BBS", when nationalist students began agitating for demonstrations against Japan after a right-wing Japanese group had made a provocative display at the Senkaku, or Diaoyu, islands, Japan's claim to which China disputes. The internet had been commercially available in China only since January 1995, and at the time it had fewer than 80,000 users in the country, but the fear of a "virtual Tiananmen Square" was palpable, writes Xu Wu, an academic.

At about the same time the government started blocking foreign websites, including Voice of America. By July 1997, writes Daniel Lynch at the University of Southern California, Chinese police were looking for advanced filtering software at a conference in Hong Kong. In December 1998 China held its first known trial for a purely internet-based political crime, imprisoning Lin Hai, a software engineer, for sending 30,000 Chinese e-mail addresses to a pro-democracy magazine based in America. Since then China has often jailed activists either for posting pro-democracy messages online or for e-mailing sensitive material abroad, and continues to do so.

In 2005 it took to using "web commentators" and "public-opinion guidance" to supplement censorship and targeted repression. That spring anti-Japanese protests had erupted in cities across China, organised in part through Tencent's QQ chat groups and bulletin boards. In an internal party speech in 2005 Mr Hu gave warning of a "smokeless war" being waged by China's enemies, and of the need to defend the party ideologically. According to Wen Yunchao, a prominent blogger, "the authorities had felt the internet was out of control and they needed to address it immediately. At the end of 2005 they had a meeting in Qingdao to study how to control the internet."

They started to hire online commentators to steer conversations in the right direction, who became known as the "50-Cent Party" because they were paid 50 Chinese cents per post. In January 2007 Mr Hu gave a speech to the Politburo calling for it to "assert supremacy over online public opinion" and "study the art of online guidance". Controlling the internet was not enough; the party also needed to "use" the internet, said Mr Hu.

The arrival of Twitter-like microblogging services in China, and particularly of Sina Weibo in August 2009, forced the authorities and their web commentators to become more active than ever. Officials have tried but so far failed to compel all users to register for online accounts with their real names. Social media also made the government even more concerned about the threat of "hostile foreign forces" online, which it took on with a will. As a white paper on the internet in 2010 put it, "Foreign social-networking sites have become a tool for political subversion used by Western nations." The Chinese authorities reinforced the Great Firewall, their first line of defence against such sites.

**Control freaks**

These days, whenever something happens that the Communist Party sees as a threat to social stability, China's internet managers set in motion a rapid, massive and complex response. The system has evolved with each new technology for online interaction. The nerve centre is Beijing, where most of the big internet companies are based. The Beijing Internet Information Administrative Bureau gets in touch with its contacts at the city's internet portals and microblogs, telling them what is to be deleted from microblogs, blogs and news sites and what approved messages are to be promoted. If the story is very big, celebrity microbloggers (such as entertainers, billionaire entrepreneurs, media personalities and technology icons), each with many millions of followers, may be asked by minders at the internet companies to keep quiet, though most do not need to be told.

In cities around the country, local internet publicity offices will contact internet commentators to feed them the official guidance for their online bulletin boards and discussion forums. And at hundreds of local, provincial and national offices of the various ministries concerned, custom-tailored software helps authorities find "harmful" online postings and get internet service providers to take them down.

Compliance is expected within seconds. When censors at Sina Weibo noticed a flood of posts on a censored New Year's Day editorial at *Southern Weekly*, a newspaper, they waited a few minutes before deleting them. One censor wrote in an online rant against complaining users that they should have been grateful for the slight delay. The censor's rant itself was quickly deleted, but has been translated and re-posted by Global Voices Online, a free-speech pressure group based outside China. The tardy supervisors had to sit through a

pep talk by the authorities, which deliver such lectures whenever they perceive resistance to "running the internet in a civilised manner"—and then tighten up controls further.

The government constantly worries about losing control when an incident captures the public's attention. This happens quite a lot, despite all the precautions. Examples go back to 1999, when followers of Falun Gong, a spiritual movement banned by the Communist Party, organised protests in Beijing and, having been crushed, used overseas Chinese websites to spread anti-government propaganda.

In 2003 the authorities tried and failed to cover up the spread of the SARS virus. In 2005 anti-Japanese protests threatened to get out of hand. In 2007 opponents of a proposed chemical plant in Xiamen, in south-eastern China, organised protest "strolls". In 2008 riots broke out in Tibet and in 2009 in the north-western region of Xinjiang. In 2011 a number of people tried to organise protests inspired by the "Jasmine" revolutions in north Africa and the Middle East. Later that year a high-speed train crashed, killing at least 40 people. In 2012 rumours spread of a coup attempt in Beijing. And so on. Each of these incidents, and many more, prompted new efforts at control. But until the system changes, it will be a never-ending task.

Table of Contents

## Assessing The Effects - A Curse Disguised As A Blessing?

From the Economist, Apr 6th 2013

One of the world's most widely read bloggers, Han Han, who is based in Shanghai, once explained to your correspondent why he did not think much of the shorter forms of microblogs, which he uses only sparingly. It was not long after the high-speed train crash in July 2011 that had been a big moment for social media. Outrage at the accident and at the government's slow and bumbling response spread rapidly on Sina Weibo, overwhelming the censors. It seemed a rare case of the public shouting down the authorities. Urban intellectuals, including some hardened sceptics, saw this as a turning-point in the history of the internet, perhaps of China generally. But Mr Han was not impressed. "You feel everyone's really angry, you feel like you could go open the window and you would see protesters on the street," Mr Han said. "But once you open the window, you realise that there's nothing there at all." Microblogging, he said, encouraged people to tune into a big story briefly, almost as entertainment, until the next big story comes along. It did not bring about "any real change or progress".

And yet microblogging has already transformed Chinese society and the way it is ruled. It has fundamentally altered the relationship between the people and the state, allowing the public to demand more accountability from officials, even if it is often disappointed. In another era the authorities would surely have kept the details of that train crash secret, lied about its cause and understated the death toll. As it was, official orders kept it off the front pages the following day. Even so, microblogs quickly spread the news, along with lots of photographs, before officials could control them. When a spokesman failed to provide convincing answers, he was pummelled online and lost his job. Anger continued to rise at his employer, the powerful railway ministry, which is now being reorganised.

This special report has argued that by building a better cage, the Communist Party has reaped the economic benefits of the internet while absorbing and controlling its political impact, and that other countries have adapted China's blueprint to their needs. The high-speed crash posed a challenge to this state of affairs, a demonstration of the power of *weibo* to rattle the cage. So is that cage built to last or will it fall apart, shown up as an increasingly desperate and ultimately doomed effort to control the uncontrollable? Recently it has become fashionable to suggest that the cage is being rattled so much it will eventually break, heralding a Beijing spring. This special report, in contrast, has argued that if such a spring were to be on its way, the internet may well be delaying its arrival, not hastening it.

China's problems in the real world are mounting. Admittedly the economy remains one of the world's best-performing, with GDP expected to grow by 7.5% this year. Hundreds of millions of Chinese people have become middle-class or even rich, whereas the number of those in abject poverty continues to decline. But corruption, income inequality, pollution and food-safety scares are far worse now than they were before the internet arrived. Incidents of mass unrest have risen dramatically in the past two decades.

Even among some of the most prosperous Chinese, who have little reason to protest, a more subtle but palpable unease has taken hold. Some of them, including entrepreneurs and government officials, have hedged their bets by obtaining foreign passports and residence permits, buying properties overseas, sending their children to study abroad and sometimes getting their spouses to go with them (the term used for such officials is "naked", meaning there is nothing to hold them in China). Such moves have been spurred by concerns about things like smog, tainted milk and the quality of education, but also by a vaguer sense that

the current gilded age cannot last. For some people the train crash was a metaphor for years of unrestrained high-speed GDP growth propelling the country towards a social, environmental and political reckoning.

**Of mice and Chinamen**

So far the party's heavy investment in the internet has paid off, allowing the government to acknowledge the problems but keeping things under control. Outsiders often describe China's internet as an ever-evolving game of cat and mouse in which both parties keep getting cleverer. The metaphor is useful up to a point, but ultimately misleading. The Chinese government has a strong interest in catching and silencing the troublemakers among the mice, and this special report has shown how much effort and ingenuity it is putting into achieving this. But it has just as much interest in providing a roomier and more attractive cage for all the mice so that they might make less trouble. To this end it has allowed a distinctly Chinese internet to flourish, with more people getting online—and more of them shopping, watching videos, gaming and chatting with each other, all on trusted Chinese platforms—than in any other country. This customisation of the internet is an important part of building a better cage.

This special report has also shown that the internet is not just a forum where citizens can vent their concerns, it is also a place where the party can listen to them and take part in the discussion. The authorities have come up with serious responses to events such as the train crash and the recent air pollution. One reason that the train crash has had no further repercussions is that the authorities have heeded people's concerns about safety, reducing the number of trains and their maximum speed so that they are now running smoothly and on time.

If the internet makes the government more responsive to people's everyday concerns, does it matter if the party quickly crushes attempts to organise protests, as it did during the Arab spring? (China's top security official urged at the time that any such efforts be snuffed out "in the embryonic stage", and so they were.) Does it matter that the party continues to stamp on dissidents online, just as it does offline? Some will say that a few human-rights concerns hardly detract from the massive success story of the Chinese internet. But this misses the point.

Microblogging has already transformed Chinese society and the way it is ruled

The government has indeed provided a roomy and attractive cage, with helpful officials tending to it. But meanwhile the systemic issues that have contributed to the problems in the real world—such as corruption, unaccountability and a total lack of transparency—continue to fester, destabilising the foundations of authoritarianism.

It is not inconceivable that the entire authoritarian edifice may eventually founder, hastened perhaps by some huge domestic crisis. If the economy were to go into a deep slump, causing massive unemployment, or if some catastrophe were to befall the country that seriously undermined the party's legitimacy, the internet could play a dramatic and unpredictable role. Flipping the kill switch to turn it off could have equally unpredictable results. Until such a moment the authorities will try to fill in cracks in the edifice of power as the internet exposes them. By doing so they may be able to buy themselves more time, possibly a lot more.

The old way of doing things will not be viable indefinitely; but for now the party is still very much in charge, deciding on the new way of doing things. In that sense Mr Han was right to be sceptical about social media. When, many years from now, history books about this period come to be written, the internet may well turn out to have been an agent not of political upheaval in China but of authoritarian adaptation before the upheaval, building up expectations for better government while delaying the kind of political transformation needed to deliver it. That may seem paradoxical, but it makes sense for a party intent on staying in power for as long as it can.

Table of Contents

## Shutting Down the Internet - Thou Shalt Not Kill

Turning off the entire internet is a nuclear option best not exercised

From the Economist, Apr 6th 2013

In a crisis, might China flip the "kill switch" on its internet and disconnect its 564m users? It may sound unthinkable, but the idea is not altogether outlandish. The Communist Party has already given it a trial run in an entire province.

In July 2009, after ethnically charged riots left hundreds dead in Xinjiang, a remote north-western region with a sizeable Muslim Uighur minority, the authorities put the province on electronic lockdown. More than 6m internet users were cut off from the rest of China and from the world, and long-distance calls and text messages on mobile phones were disabled. Xinjiang residents could not use these telecoms services for many

months and were unable to use any of the outside internet, even most of the scrubbed Chinese version, until the following May, leaving a gap of more than ten months.

By the party's criteria it seemed to work. The combination of online repression and ruthless security on the ground enabled the authorities to quell the riots and prevent further disorder. This did not seem to cause any great harm to China's reputation abroad, but there was an economic price to pay. Xinjiang's exports in 2009 plummeted by 44%, compared with a less devastating drop of 16% in a difficult year for the global economy.

Technically, shutting down Xinjiang was relatively easy because it was already isolated both geographically and technologically. It required nothing more than blocking all internet-protocol addresses outside Xinjiang at the border so people were stuck in a Xinjiang "intranet", a rather dull place. Some users used long-distance calls to hook up to the internet by modem, though access numbers would get blocked. Others travelled long distances outside the province to get connected.

Cutting off the whole country would be a different matter. In December Renesys, a network-research firm, ranked more than 200 countries by how easy it would be to disconnect them from the internet. It reckoned that for 61 of them, with only one or two internet service providers at their borders (eg, Tunisia, Ethiopia and Yemen), it would be fairly simple, and for another 72 (including Rwanda, Kyrgyzstan and Iran) it would not be too difficult. China, with its well-developed internet backbone, was not on either of those lists. Renesys thought that given a "determined effort", its internet could be shut down over a period of time, "but it would be hard to implement and even harder to maintain."

The party has often proved itself capable of making a determined effort when it comes to security. The Great Firewall could easily block the foreign internet for most users in China; an unexplained glitch actually made this happen by accident one day last year for a couple of hours. Some large enterprises, banks and foreign companies have leased their own lines out of China, which might need to be shut down separately. As for the domestic internet, which would be of most concern to the party, shutting down the country's home-based internet service providers, and with them access to microblogs, video sites, bulletin boards and the rest, should be within its capabilities.

But would the party dare? In the Arab spring flipping the kill switch was no help to the dictators of Egypt, Libya and Syria. For China, even if its big cities were torn by riots, turning off the internet would seem to run counter to its operating logic: adjust the machinery, intensify filtering, round up far more than the usual suspects, but do not give the people added reason to go out into the streets. The kill switch may be necessary as a last resort, but using it would be an admission of system failure.

Table of Contents

## Internet Controls in Other Countries

China's model for controlling the internet is being adopted elsewhere

From the Economist, Apr 6th 2013

At a United Nations conference on telecommunications governance in Dubai last December representatives of most of the world's countries argued furiously over the way the internet should be managed. The debate established a clear divide over how much control a country should have over its own internet. On one side were America, the European Union and other developed countries that broadly back internet freedom; on the other were China, Russia, Saudi Arabia, Sudan and a number of other authoritarian states. A significant majority of these seem to favour China's approach to control (or a Russian variant), which involves allowing

more access to the internet and reaping the economic benefits, but at the same time monitoring, filtering, censoring and criminalising free speech online.

Many Asian and African countries are using Chinese technology both to deliver access to the internet and to control its use, and some Central Asian republics are believed to use Russian surveillance technology as well. A very few, such as Turkmenistan, prefer the North Korean model, in which hardly anybody is allowed to go online, and a few others, including Azerbaijan, do little to encourage use of the internet. Katy Pearce, of the University of Washington, explains that Azerbaijan has run an effective campaign against the evils of the web, linking it to mental illness, divorce, sex-trafficking and paedophilia. She says that only a quarter of Azerbaijan's population has ever been online, which puts it behind poorer neighbours; and only 7% are on Facebook.

But most authoritarian regimes have allowed the use of the web to grow rapidly, noting that China has found it perfectly possible to embrace the internet while keeping it under close control. In Kazakhstan, for instance, some 50% of the population is now online, compared with 3.3% in 2006, though access is tempered by some Big Brotherish constraints.

**What's your weapon?**

In Russia, Nigeria, Vietnam and elsewhere the government is paying people to blog and comment in support of government priorities, a tactic China started in 2005 with its "50-Cent Party" of web commentators for hire. Belarus, Ethiopia, Iran and many others are believed to use "deep packet inspection" to look into internet users' communications for subversive content, aided by hardware from, among others, China's Huawei and ZTE. Obligingly, internet users who know they are being watched are more likely to exercise self-censorship in the first place.

In addition some authoritarian states selectively block access to foreign websites that carry politically sensitive content, along with shutting down or harassing domestic opposition websites. In some countries opposition websites are subjected to massive denial-of-service attacks. Another technique, borrowed from Russia, is to accuse troublesome website operators of extremism or defamation, which in some countries are criminal offences. This method is employed by Kazakhstan, which also blocks some sites without acknowledgment, much less an explanation, in the same way as China does. Kazakhstan officials say they have a completely free, lively internet and block only extremist content. But that sounds doubtful in a country that also cracks down on its opposition press and where the president, Nursultan Nazarbayev, regularly claims more than 90% of the vote in elections.

A growing number of such countries have an internet that each of them can call their own, walled off as much or as little as suits them. They argue that Western governments also manage the internet, censoring it and shutting down objectionable websites, so they should let others do the same. This was the crux of the debate at the telecommunications conference in Dubai. Russia, China and 87 other states insisted that all countries should recognise each other's sovereign right to connect to the internet in their own way. That resolution failed, but China's internet model is clearly attracting plenty of followers.

Table of Contents

## Masters of the Cyber-Universe

China's state-sponsored hackers are ubiquitous—and totally unabashed

From the Economist, Apr 6th 2013

China's sophisticated hackers may be the terror of the Earth, but in fact most of their attacks are rather workaday. America and Russia have hackers at least as good as China's best, if not better. What distinguishes Chinese cyber-attacks, on anything from governments to *Fortune* 500 companies, defence contractors, newspapers, think-tanks, NGOs, Chinese human-rights groups and dissidents, is their frequency, ubiquity and sheer brazenness. This leads to an unnerving conclusion.

"They don't care if they get caught," says Dmitri Alperovitch, who used to work at McAfee, a computer-security firm, where he helped analyse several Chinese hacking operations in 2010 and 2011, and is a co-founder of CrowdStrike, another cyber-security firm. The indiscriminate tactics of China's 2010-11 campaign made it relatively easy to track. His team identified more than 70 victims (among many more unidentified ones), dating back to 2006, and found that the average time the hackers stayed inside a computer network was almost a year. "They'll go into an organisation and then stay there for five, six years, which of course increases the chances that they get caught."

Mr Alperovitch offers two reasons for the careless abandon of China's hackers. The first is that their attacks are on an industrial scale—"thousands of continuous operations"—so they could hardly be expected to go

unnoticed. The second is that "they don't see any downsides to being caught. They have so far not suffered economically or politically for being caught."

It is true that most victims are unwilling to remonstrate openly with the Chinese state. Except for Google, hacked companies have tended to keep quiet. Most governments have chosen not to confront China publicly, though American officials have recently started doing so. NGOs working in China have said nothing. Companies fear reprisals from customers and shareholders for failing to secure their networks. And perversely many victims do not want to antagonise their attackers. Even security companies, though obviously keen to capitalise on the threat, are wary of pointing the finger because they want to sell their antivirus products in China too.

This culture of secrecy and shame makes it harder to confront the problem. It also helps Chinese officials, who consistently and emphatically deny allegations of state-sponsored hacking. They rely on the hope that in such a murky field the evidence is always wanting. Yet in reality it is often fairly plain, and attitudes may at last be hardening. That could mean growing suspicion of the big Chinese technology companies, including Huawei, which is already politically unwelcome in America, and Tencent, which is trying to expand its social-media services abroad. But it is not clear what, in practice, America and other Western countries can do to restrain Chinese behaviour, other than becoming better at hacking themselves.

**Whodunnit?**

Security experts outside China have learned how to reverse-engineer methods of attack and trace attackers' internet-protocol addresses back to their physical origins. They have identified up to 20 "Advanced Persistent Threat" teams operating in China, including one that stole valuable commercial secrets from Google, Adobe and other Silicon Valley companies; another that for years targeted a number of global energy companies; and yet others that have hacked hundreds of companies, government agencies, think-tanks and NGOs the world over. The victims have included global steel companies; a firm that supplies remote-control systems for American oil and gas pipelines and power grids; a hotel computer system that provided access to data for important guests; a tech-security firm, RSA, that opened the way to hacking Lockheed Martin and defence subcontractors producing America's F-35 Joint Strike Fighter; and even NASA. Some of the attacks have been highly sophisticated, but many more have begun with a simple "phishing" e-mail fooling the recipients into clicking on a link.

The organisation and scale of these attacks, involving large teams of hackers and thousands of computers, strongly suggest that the Chinese party-state has played a guiding role. American experts point to the People's Liberation Army's 3rd Department, which according to the Project 2049 Institute, an American think-tank, is roughly equivalent to America's National Security Agency. Project 2049 describes an apparent fixation with North American targets at the Shanghai headquarters of Unit 61398, part of the 3rd Department. In February Mandiant, a security firm, identified Unit 61398 as the likely base for thousands of attacks on North American corporate and security targets.

The choice of targets also clearly points to China's government as the perpetrator. The Google hack, at a time when the company was facing increasing hostility in China, appeared to leave little room for doubt; one Chinese source actually told officials in America's State Department that two members of the elite Politburo Standing Committee ordered the attack, according to a State Department cable that was released by WikiLeaks. Other victims of hacking attacks included the International Olympic Committee and the World Anti-Doping Agency after the 2008 Beijing Olympics; Tibetan and Uighur activists and Chinese dissidents; think-tanks that analyse China (including its hacking capabilities); and NGOs operating in China. None of these seemed to have any commercial value.

For an individual caught up in such an attack the effect can be creepy. One day in early 2010 an American working for an environmental NGO in China noticed something odd happening on his BlackBerry: it was sending an e-mail from his account without his doing. He watched, dumbfounded, as the e-mail went out to a long list of US government recipients, none of which was in his address book. Seconds later he saw the e-mail disappear from his sent folder. Eventually he heard from the FBI that his e-mail account and those of several colleagues had been compromised by hackers from China. All the victims had attended a climate-change conference in Copenhagen in December 2009 where America and China had clashed.

Another obvious target was David Barboza, a journalist on the *New York Times*. In October 2012 he reported that relatives of Wen Jiabao, then China's prime minister, had amassed assets of $2.7 billion. After the story

was published, said the newspaper, Chinese hackers compromised its networks to get at Mr Barboza's work e-mail account. Following the newspaper's disclosure in January, other news organisations, including the *Wall Street Journal* and Reuters, noticed similar Chinese intrusions. But Bloomberg, which last year reported on the finances of relatives of Xi Jinping, China's new president, and has extensively investigated Chinese hacking, has denied suggestions that it was itself successfully hacked.

The Chinese authorities, which since the report on Mr Wen have blocked the *New York Times*'s English and Chinese-language websites, angrily denied the newspaper's hacking allegation. Wan Tao, one of China's first "patriotic hackers" (nationalists who in the early days of China's internet hacked into websites of foreign governments on their own initiative), offers a convenient alternative culprit: "underground hackers", or black-market operators who either sell their services or strike out on their own in hopes of finding a buyer. "Their business model is to sell," Mr Wan says, sitting in front of a ThinkPad in a coffee house in Beijing. The price of access to a target's e-mail box starts at less than $1,000, he says.

But Mr Wan's explanation is unconvincing. His own story offers evidence that what may have started as independent hacking has evolved into a state-supported enterprise. He is now a cloud-security consultant but was an "angry young man" in the 1990s, he says. In 1997 he joined China's first hacking group, "Green Army", leading attacks on foreign websites. His first (solo) patriotic hack, in 1997, was to crash the e-mail box of the Japanese prime minister's website; in 2001, after an American spy plane collided with another plane, he and fellow patriotic or "red" hackers conducted various attacks on American websites in what they quaintly called a "cyberwar".

**The quick and the dead**

The authorities gave Mr Wan and other hackers free rein. Police did not worry about hacking of targets outside the country, and still do not appear to. China has so far failed to sign an international cybercrime convention. Although hacking has been a criminal offence in China since 1997, the authorities have enforced the law only when the perpetrators were targeting things like state secrets and assets. The first publicised hacking trial in China, in 1998, was of two men who got into the website of a state-owned bank in Jiangsu province, stealing less than $100,000. One of them was executed.

In contrast, patriotic hackers like Mr Wan were sought out for their advice and expertise. In 1998 the cyber-police, then quite newly formed, approached Mr Wan at a security conference in Guangzhou. They wanted him to help them find out who had written anonymous subversive postings on bulletin boards. In response he designed a software system in 1999 that could analyse posts about sensitive subjects such as Falun Gong or democracy, compare them with other online content and find out who had written them. He believes it was the first of its kind in China. "I'm a security expert," he explains. "They had the need."

Later, after his hacks against America, says Mr Wan, he was asked for help by the People's Liberation Army (PLA). He did not want to work for them but agreed to introduce them to other hackers. Since then the PLA has openly recruited hackers, sponsoring contests at universities and posting job advertisements.

The Chinese army's doctrine of cyber-warfare (like that of a number of Western counterparts) is to knock out the enemy's information infrastructure, and its doctrine of cyber-security is to go on the offensive to defend itself against attacks. The Chinese authorities often point out, correctly, that they are the victims of frequent cyber-attacks from America. Thousands of such attacks are also carried out from Russia and Brazil every year. But more of them originate from China than from anywhere else in the world, and at least some of them are undeniably linked to the party-state. That Chinese model may well prove attractive to other countries.

Table of Contents

## The Great Firewall: The Art of Concealment

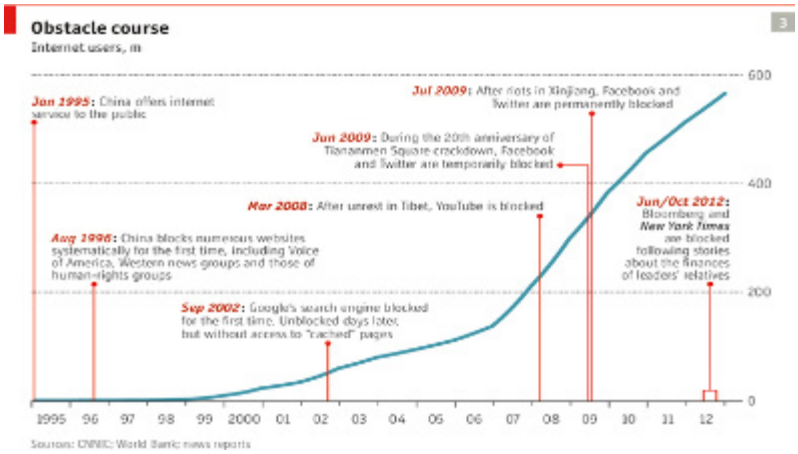
From the Economist, Apr 6th 2013 |From the print edition

On February 9th, Chinese New Year's Eve, Fang Binxing, known in China as the father of the Great Firewall, wished his followers on Sina Weibo a happy Year of the Snake. As always whenever Mr Fang tweets, thousands of fellow microbloggers sent messages along the lines of "get lost". They could not reply directly: Mr Fang gets so much abuse for his role in engineering China's censorship technology that the "comments" function on his microblog page had to be disabled long ago. Nor can users easily find the comments on the 35,000 retweets of his new-year post: Sina has blocked access to those as well.

Mr Fang is used to being, in the parlance of the system he helped create, a "sensitive keyword". He is one of the most important figures in the history of the Chinese internet, and perhaps its most reviled. In 2011 several students in Wuhan, in central China, said they threw eggs and a pair of shoes at Mr Fang when he visited their campus to give a speech. There was not a little irony in their spreading the news of their action

(and a photograph of one student's shoeless feet) on Twitter, which thanks to Mr Fang's work is accessible to China's internet users only with special circumvention tools.

Exactly how Mr Fang constructed his wall is a state secret and the subject of much speculation and academic research. Although China's entire system of internet controls is often described under the heading "the Great Firewall" (a term that first appeared in a *Wired* magazine article in 1997), in reality the Great Firewall is probably the simplest part of a complex effort involving many different agencies and companies. China's cyber-police have their own much larger and more expensive system of domestic filtering and surveillance, Golden Shield, and internet sites employ lots of people to censor their own content and implement government directives.




The Great Firewall that Mr Fang helped build stands separately, guarding a handful of gateways through which all foreign internet content and communications enter the country, sniffing through small packets of data to detect and block access to "harmful" foreign content. It is the world's most advanced national firewall, having evolved from crudely blocking entire web domains (though it still does some of this) to blocking just particular pages within websites.

Mr Fang's work on this system started in 1999, at the National Computer Network and Information System Security Administration Centre, under what is now the Ministry of Industry and Information Technology. It created the modern infrastructure for filtering foreign sites. In the early years China's efforts at blocking web domains had been straightforward. From August 1996 routers filtered out a list of foreign websites, including those of Voice of America, human-rights groups, Taiwan and Tibet independence advocates and some foreign newspapers. But the early blocks did not take account of the content of individual web pages, and savvy users could easily get round them.

Now the firewall is far more capable. If users try to get on Facebook, Twitter or thousands of other websites, or if they search for a banned keyword such as "Falun Gong" or the name of one of the many jailed Chinese dissidents, they are taken to a dead end with an error message (such as "web page not available"). The system can intercept messages containing banned terms sent across China's borders on chat software. It can also block access to many circumvention tools, and in December last year it began more intensive disruption of private commercial services, called VPNs, that are widely used to "tunnel" under the firewall. It also subtly and intermittently "throttles" websites such as Google's search engine to slow them down.

**Degoogled**

Google has been one of China's favourite targets over the years, making it a useful measuring stick for the way that filtering technologies have developed. In September 2002 the firewall blocked Google entirely, using a technique called "DNS poisoning" that intercepts requests for web pages. The blocking made global headlines. The service was restored after nine days, but Google's "cache" pages (snapshots of web pages stored and delivered by the company), which had been a convenient way for Chinese users to find banned content, remained blocked. The Great Firewall was getting smarter. Today searches for banned keywords on Google will take users to a dead end and leave them in a virtual sin bin, blocking access to the search engine for about 90 seconds, though other parts of the internet will remain readily available.

Google has been one of China's favourite targets over the years, making it a useful measuring stick for the way that filtering technologies have developed

The centrepiece of this sophisticated filtering effort had been the National Information Security Management System, named Project 005 after its starting date in May 2000. Mr Fang and other engineers worked on it until 2002. The project won a national prize for science and technology in 2003. It had cost $60m to build and is believed to be the most critical and most expensive component of the Great Firewall.

Mr Fang, who in 2007 became president of Beijing University of Post and Telecommunications, has sometimes played down his involvement in such efforts, but he has clearly had a big part in them. For example, he helped develop filtering technology used for domestic search engines, according to the summary of a study (itself not in the public domain) he co-wrote in 2005. The system "has yielded good results", the summary states, and will help in "purifying the domestic internet space".

Many Chinese internet users are less keen on these advances. In January Han Weili, a professor at Fudan University in Shanghai, was attacked for inviting doctoral students to conduct research on China's Great Firewall (GFW, as Chinese users abbreviate it). His notice on the university's online bulletin board read: "Anyone interested in improving the GFW. Their team is recruiting PhD students. If interested, get in touch with me."

Mr Han felt compelled to defend himself. "So in your opinion the scientists who studied nuclear bombs should be ashamed of themselves throughout history? The launch button for nuclear weapons is controlled by the politicians of a country," Mr Han wrote in a reply that was later deleted. "As for how to use [the GFW], it's not something scientists can handle. You can be the king of morality and refuse to do it, but you don't have to condemn those who try to improve it." Mr Han later wrote that he has not worked directly on the firewall. His last word on the matter was that authorities had asked to meet him: "Both sides hate me. Damn it." That comment too was deleted.

Mr Han has a point. It is generally senior bureaucrats, not engineers like Mr Fang, who decide what foreign sites are unfit for Chinese users, such as YouTube (blocked permanently in 2009), Facebook and Twitter (blocked since riots in Xinjiang in 2009) and Bloomberg and the *New York Times* (blocked in 2012, after publishing detailed reports on the finances of Chinese leaders' families).

The engineers' job is to fine-tune the instruments. Michael Robinson, an American network engineer who in 1996 worked on some of the early infrastructure of commercial internet access in China, says that "most of the development of the technical capabilities of the Great Firewall over the past 15 years has been toward an ability to minimise the impact of the government's content-control policies through more precise mechanisms." Such improvements often aim to minimise not the censorship itself but the sense of being censored. One technique is to leave tweets that have been removed from public circulation visible to those who posted them.

To most Chinese internet users, though, exactly who is responsible for what in the machinery of censorship matters much less than the idea of censorship itself. Mr Fang is a symbol, and the term GFW has become a hated archetype. It is shorthand for the restriction on their experience of the internet and for the increasing number of Chinese words that have become too sensitive to use, including many innocuous ones that happen to be homophones for sensitive ones. This prompted one user to write a science-fiction parody in which a new project, GFW Turbo, becomes self-aware and runs out of control, banning almost the entire Chinese language. The parody looks ahead to 2020 when a "National Anti-GFW Ministry" adds "2,000 more Chinese characters to meet the people's ever-increasing needs for means of production, only to find them censored within two seconds." Finally, in 2025, there is only one phrase left in the Chinese language: "sensitive word".

Table of Contents

## Electronic Warfare: The Ethereal Future of Battle

By Sharon Weinberger, BBC, 4 April 2013

The future of warfare is no longer about bullets and bombs, or dominating land, sea and air. Instead, tomorrow's victors will dominate the ether.

The voice of the foreign military commander is sinister and gloating.

"On the anniversary of our nation's most glorious sea victory, let us remember our heroes that helped bring the United States to its knees," he says, his face obscured by shadows. "We ground to dust the vaunted American navy like the impotent clay figurines that they had become."

The speech continues, providing hints of how the devastating attack of 2025 began—carried out initially not with bombs and bullets, but invisible electromagnetic energy and cyberattacks that dropped drones from the sky, left US cities in total blackness, and disabled entire aircraft carriers at sea.

This video may sound like the opening of an apocalyptic movie, but the brief clip was created as part of a US Navy game called MMOWGLI, an acronym for the unwieldy sounding Massive Multiplayer Online Wargame Leveraging the Internet. The crowdsourcing game, which was run by three elements of the US Navy – the Navy Warfare Development Command, the Office of Naval Research and the Naval Postgraduate School—invited players to help develop ideas for how the navy could prepare for this brave new world of electromagnetic warfare, where enemies use invisible, and often untraceable weapons, that can theoretically disable everything from satellites and computers to radar and aircraft.

Electromagnetic warfare covers any and all weapons that attack using electromagnetic radiation, which can jam or even permanently fry electronics. But the Navy now may be looking at such weapons as part of a broader approach to warfare. In a recent article, Admiral Jonathan Greenert, the chief of US Naval Operations,

argued that cyber weapons needed to be merged with electromagnetic attacks, or what he calls the "electromagnetic cyber realm."

"The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a warfighting domain on par with—or perhaps even more important than—land, sea, air, and space," he wrote. "Future wars will not be won simply by effectively using the EM spectrum and cyberspace; they will be won within the EM-cyber domain."

**Electronic warhead**

Much has been written about cyber-weapons, such as the Stuxnet virus that infiltrated Iran's nuclear facilities, or any number of attacks on government and military departments and contractors, but the electromagnetic realm rarely features.

These weapons trace their origins back to the cold-war idea of exploding an atom bomb high in the atmosphere above an enemy, which results in an electromagnetic pulse, or EMP, that fries the electricity grid and communication network.

While such nuclear-generated EMP weapons are still largely theoretical, the US has pursued electromagnetic weapons that use conventional sources, such as high-power microwave generators. Such weapons could, at least in theory, stop vehicles in their tracks and even take down enemy weapons.

Much of the work on such weapons is secret, but there are unclassified weapons as well. For example, the US military has funded a Radio-Frequency Vehicle Stopper - a satellite dish sized weapon that can be mounted on top of a jeep that can be used to disable enemy vehicles at a distance.

Many of these existing weapons are for relatively close-in use. "[Electromagnetic weapons] always had the problem of getting close enough to be really effective," says Dave Fulghum, a former senior editor of Aviation Week & Space Technology magazine.

But defense companies have also been working on new weapons that can strike at greater distances. In October of last year, Boeing released footage of its development weapon, the Counter-electronics High-powered Microwave Advanced Missile Project (Champ), a cruise missile with an electromagnetic warhead. Though Boeing has declined to discuss the project in any detail, a video produced by the firm shows the missile disabling a bank of desktop computers. US firm Raytheon has worked on missiles equipped with electromagnetic warheads, according to Fulghum.

This growing interest in electromagnetic weapons explains the military's interest in preparing defenses. "An aircraft carrier [is] a huge emitter, and anytime you have an antenna putting stuff out, those then become targets," says Fulghum. "Any emitter that can send stuff out, can have stuff put into it."

It also helps explain the US Navy's – perhaps unconventional - approach of using a crowdsourcing game to finding potential solutions to electromagnetic warfare.

**'Zombies in hyperspace'**

The idea of MMOWGLI was to attract a wide group of people to come up with ways to help the military prepare for electromagnetic and cyber warfare. Unlike previous crowd-sourcing games sponsored by the navy and open to the public, such as one focusing on counter-piracy, the electromagnetic warfare game was limited only to those with a military or government email account. The explanation, says Don Brutzman, a professor as the Naval Postgraduate School in Monterey, California, was because of the sensitive nature of the subject.

While the game itself was unclassified, Brutzman, who helped run the game, says keeping it "limited access" introduced a layer of security. "It's quite easy for players to go classified in a hurry," he says. "As soon as you talk about this radar, or that antenna—the numbers and vulnerabilities—that's classified."

While designed as a "game," MMOWGLI may fall far short of many people's idea of entertainment.

"It's not a shoot 'em up, let's go blast zombies in hyperspace," cautions Brutzman. "It's people typing ideas and interacting with each other."

In reality, players submitted an idea, such as a way to bolster US defenses, winning points based on the number of discussion and response that their submission generates.

So what exactly can crowdsourcing do for improving electromagnetic-cyber warfare? It's not completely clear: though the naval researchers involved in the project did post some examples of award winning concepts, at least some, such as a method for secure communication, cannot be discussed in an open forum.

While limiting it to government officials and members of the military may make the game sound less like an experiment in true crowdsourcing, Rebecca Law, a research associate at the MovesInstitute at the Naval Postgraduate School and a game administrator, points out that it still had over 200 active players. And the

anonymity granted to players online allowed them to propose ideas without regard to their status or rank. "I believe it makes the information accessible when it's done in a game-like fashion," she said.

But more importantly, using a game with points and winners encourages a creative mindset. "They want to have great ideas," she says. "They want to win."

Whether they will , time will tell.

Table of Contents

## Why China Is Reading Your Email

By David Feith, Wall Street Journal, 30 Mar 2013

Fort Leavenworth, Kan.--For several years, Washington has treated China as the Lord Voldemort of geopolitics—the foe who must not be named, lest all economic and diplomatic hell break loose. That policy seemed to be ending in recent weeks, and Timothy Thomas thinks it's about time.

The clearest sign of change came in a March 11 speech by Tom Donilon, President Obama's national security adviser, who condemned "cyber intrusions emanating from China on an unprecedented scale" and declared that "the international community cannot tolerate such activity from any country." Chinese cyber aggression poses risks "to international trade, to the reputation of Chinese industry and to our overall relations," Mr. Donilon said, and Beijing must stop it.

"Why did we wait so long?" wonders Mr. Thomas as we sit in the U.S. Army's Foreign Military Studies Office, where the 64-year-old retired lieutenant colonel has studied Chinese cyber strategy for two decades. More than enough evidence accumulated long ago, he says, for the U.S. to say to Beijing and its denials of responsibility, "Folks, you don't have a leg to stand on, sorry."

U.S. targets of suspected Chinese cyber attacks include news organizations (this newspaper, the New York Times, Bloomberg), tech firms (Google, Adobe, Yahoo), multinationals (Coca-Cola, Dow Chemical), defense contractors (Lockheed Martin, Northrop Grumman), federal departments (Homeland Security, State, Energy, Commerce), senior officials (Hillary Clinton, Adm. Mike Mullen), nuclear-weapons labs (Los Alamos, Oak Ridge) and just about every other node of American commerce, infrastructure or authority. Identities of confidential sources, hide-outs of human-rights dissidents, negotiation strategies of major corporations, classified avionics of the F-35 fighter jet, the ins and outs of America's power grid: Hackers probe for all this, extracting secrets and possibly laying groundwork for acts of sabotage.

China's aggression has so far persisted, Mr. Thomas says, because "it makes perfect sense to them." The U.S. has difficulty defending its cyber systems, the relatively new realm of cyber isn't subject to international norms, and years of intrusions have provoked little American response. "I think they're willing to take the risk right now because they believe that we can't do anything to them," he says. "You have to change the playing field for them, and if you don't, they're not going to change. They're going to continue to rip off every bit of information they can."

Hence the promise of Washington's apparent shift in policy. "There's something going on," Mr. Thomas says, and the Donilon speech was only one part. This month's more significant news, he argues, was the announcement that the U.S. military's Cyber Command (founded in 2009) would for the first time develop and field 13 offensive cyber-warfare teams. The Chinese "now know we are ready to go on the offense. There's something that's been put in place that I think is going to change their view."

Not that he expects Beijing to back down lightly. On the contrary, Mr. Thomas points to the literature of the People's Liberation Army to demonstrate that China's cyber strategy has deep—even ancient—roots.

The essence of China's thinking about cyber warfare is the concept of *shi*, he says, first introduced in Sun Tzu's "The Art of War" about 2,500 years ago. The concept's English translation is debated, but Mr. Thomas subscribes to the rendering of Chinese Gen. Tao Hanzhang, who defines *shi* as "the strategically advantageous posture before a battle."

"When I do reconnaissance activities of your [cyber] system," Mr. Thomas explains of China's thinking, "I'm looking for your vulnerabilities. I'm establishing a strategic advantage that enables me to 'win victory before the first battle' "—another classic concept, this one from the "36 Stratagems" of Chinese lore. "I've established the playing field. I have 'prepped the battlefield,' to put it in the U.S. lexicon."

Or, as Chinese Gen. Dai Qingmin wrote in his 2002 book, "Direct Information Warfare": "Computer network reconnaissance is the prerequisite for seizing victory in warfare. It helps to choose opportune moments, places and measures for attack." Says Mr. Thomas: "He's telling you right there—10 years ago—that if we're going to win, we have to do recon."

A 1999 book by two Chinese colonels put it more aggressively (albeit in a sentence as verbose as it is apocalyptic): "If the attacking side secretly musters large amounts of capital without the enemy nations being aware of this at all and launches a sneak attack against its financial markets," wrote Qiao Liang and Wang Xiangsui, "then, after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis." No kidding.

This vision from 1999 reads like an outline of the report published last month by Mandiant, a private-security firm, about "Unit 61398," a Shanghai-based Chinese military team that since 2006 has mounted cyber assaults to steal terabytes of codes and other information from U.S. assets. Among the targets of Unit 61398 was Telvent Canada, which provides remote-access software for more than 60% of the oil and gas pipelines in North America and Latin America.

Unit 61398 is said to engage in "spearphishing," whereby would-be cyber intruders send emails with links and attachments that, if clicked, install malware on target computers. Lesser hackers might spearphish while posing as Nigerian princes, but Unit 61398 developed sophisticated ways, including colloquial language, to mimic corporate and governmental interoffice emails.

Spearphishing, too, draws on traditional Chinese stratagems: "The Chinese strive to impel opponents to follow a line of reasoning that they (the Chinese) craft," Mr. Thomas wrote in 2007. With this kind of asymmetric approach, he says, "anybody can become an unsuspecting accomplice."

In this context Mr. Thomas mentions a cartoon published last year in Army magazine in which one Chinese general says to another: "To hell with 'The Art of War,' I say we hack into their infrastructure." Good for a chuckle, perhaps, but Mr. Thomas warns against taking the message seriously. China's hacking is in fact "a manifestation of 'The Art of War,' " he says, and if the U.S. military doesn't realize that, it "can make mistakes. . . . You have to stay with their line of thought if you're going to try to think like them."

"Boy," he later laments, "we need a lot more Chinese speakers in this country"—a point underscored by the fact that he isn't one himself. He reads Chinese military texts in translation, some published by the U.S. government's Open Source Center and some he has found himself. He stumbled upon Gen. Dai's "Direct Information Warfare" on a trip several years ago to Shanghai, when an associate led him (and an interpreter) to an unmarked military bookstore on the top floor of a building on the outskirts of town. "I could tell when I walked in that the people behind the cash register were stunned I was there," he recalls. In public bookstores, he says, material addressing Chinese national security is often marked "not for foreign sale" on the inside cover.

The Ohio native does speak Russian, having focused most of his military service (from West Point graduation in 1973 until 1993) on the Soviet Union. That language skill still comes in handy, and not just because Russia is suspected of having carried out cyber assaults against Estonia in 2007 and Georgia in 2008.

Look at the Mandiant report's map of Chinese cyber intrusions (at least those tied to Unit 61398): Russia is untouched. "That's a huge area. . . . I really would wonder why they're after South Africa, the U.A.E. and Singapore but not Russia. And Luxembourg. They went after Luxembourg but not Russia?" Together with Iran, he argues, China and Russia make up "not the axis of evil but the axis of cyber."

So what is to be done? Security firms are working to harden networks against hackers, and members of Congress are promoting legislation to let the government work more closely with Internet service providers without opening up the companies to lawsuits or infringing on civil liberties. Washington could challenge Chinese cyber espionage with targeted economic sanctions. Meanwhile, there is much talk about establishing international standards for cyber space, but it is unclear what that would mean—which probably explains why top officials in Washington and Beijing have both endorsed the idea.

None of this seems promising to Mr. Thomas, who stresses building deterrence through offensive capabilities, such as the 13 new teams at U.S. Cyber Command. The implication is that the best defense is a good offense.

And doesn't that suggest, in turn, that the U.S. and China are headed toward a dynamic of mutually assured cyber destruction? "It seems like it," he says.

It's heartening to hear, then, that Chinese military literature isn't uniformly aggressive toward America. This includes writings about the "China Dream," which posits that China will overtake the U.S. economically and militarily by midcentury—and which has been adopted as the signature cause of new President Xi Jinping.

"They give you both versions," says Mr. Thomas. "They give you a model that says, 'There will be no way we'll ever fight [the U.S.], we'll work on cooperation.' A chapter later, 'There could be a time where if pushed hard enough, we'll have to do something and there will be a battle.' "

But what about the argument that the U.S. is shedding crocodile tears? America (and Israel) were almost certainly behind the most successful known cyber attack to date: the Stuxnet virus that impeded Iran's uranium-enrichment program. There might be some comfort in knowing that the U.S. is doing unto China what China is doing unto the U.S., says Mr. Thomas, but "we don't seem as intrusive as the other side." That is illustrated especially, he says, by China's state-sponsored commercial espionage. He frequently hears complaints from U.S. firms dealing with Chinese counterparts who know their secrets, adding that "I don't think people really get the security briefing of just how invasive it is."

Then there's the argument that all this is overblown because no cyber attack has ever killed anyone. Mr. Thomas responds, somewhat impatiently: "If I had access to your bank account, would you worry? If I had access to your home security system, would you worry? If I have access to the pipes coming into your house? Not just your security system but your gas, your electric—and you're the Pentagon?"

He adds: "Maybe nobody's been killed yet, but I don't want you having the ability to hold me hostage. I don't want that. I don't want you to be able to blackmail me at any point in time that you want." He cites the Chinese colonels' vision, back in 1999, of "social panic" and "street riots." "I wonder what would happen if none of us could withdraw money out of our banks. I watched the Russians when the crash came and they stood in line and . . . they had nothing."

Table of Contents

## Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling

Authored by Dr. Colin S. Gray, Strategic Studies Institute (SSI), 4 April 2013

*EXECUTIVE SUMMARY*: Generically viewed, the challenge that cyber power poses to our understanding is a familiar one. After all, within living memory (just about) we have had to try and make sense of air power, and then, a generation later, of nuclear weapons and their possible delivery by ballistic missiles. What unites our experience with air power, nuclear weapons, and now cyber, is the authority of strategic explanation conveyed in the general theory of strategy—Carl von Clausewitz's rules, even though he was ignorant of hydrogen fusion weapons and of networked digital computers.

Our challenge is the need to be thoroughly respectful of the science and engineering that generates the technology for cyber, while at the same time declining to be so dazzled by the technical wonders that are ours to command that we are unable to look beyond technology and tactics. To date, the networked computer has fueled a large library on the technology and the tactics of the emerging digital age, but very little of lasting note on the strategic meaning of it all. Senior people in the ranks of strategic studies have by and large ignored the growing cyber challenge, while those who are technically highly cyber knowledgeable typically have scant background in strategy. On the one hand, those who are technically competent have not been sufficiently strategically educated to know how to think about cyber strategically. On the other, those who have some serious credentials as strategic thinkers have been deterred both by their uncertain technical grasp of cyber and—it needs to be said—by the more pressing demands of other strategic challenges. In the 2000s, cyber has been "coming," but it has not been urgent in its need for attention today, unlike the problems associated more directly with terrorism and insurgency. Regarded historically, the American extended defense community strives to cope seriatim with the biggest issue of "now." As counterterrorism (CT) and counterinsurgency (COIN) have more than somewhat faded from high official interest in very recent years, so, predictably, there has been opportunity for the next new big conceptual challenge to dominate conference and seminar agendas—cyber.

The revolution in military affairs (RMA) theory of the 1990s (and the transformation theory that succeeded it) was always strategyand politics-light. It is not exactly surprising that the next major intellectual challenge, that of cyber, similarly should attract analysis and assessment almost entirely naked of political and strategic meaning. Presumably, many people believed that "doing it" was more important than thinking about why one should be doing it. Anyone who seeks to think strategically is obliged to ask, "So what?" of his or her subject of current concern. But the cyber revolution did not arrive with three bangs, in a manner closely analogous to the atomic fact of the summer of 1945; instead it ambled, then galloped forward over a 25-year period, with most of us adapting to it in detail. When historians in the future seek to identify a classic book or two on cyber power written in the 1990s and 2000s, they will be hard pressed to locate even the shortest of short-listable items. There are three or four books that appear to have unusual merit, but they are not conceptually impressive. Certainly they are nowhere near deserving (oxymoronic) instant classic status. It is important that

cyber should be understood as just another RMA, because it is possible to make helpful sense of it in that context. Above all else, perhaps, RMA identification enables us to place cyber where it belongs, in the grand narrative of strategic history.

In addition to thinking about cyber in the context of strategy's general theory, also it is enlightening to consider cyber in the contexts of geography and of information. Much of the unhelpful undue technicism about cyber is suitably sidelined when the networked computer and its cyberspaces are framed both geographically and as only the latest stage in the eternal and ubiquitous story of information. To approach cyber thus is not to demote or demean it; rather, is it simply to locate cyber properly in our relevant universe.

Argument by historical analogy is commonplace and essential; indeed, it is unavoidable, because history is our sole source of evidence. We cannot help but argue from what we know to what we do not (and cannot) know. It is helpful to consider cyber with reference to its prospective utility in terms of net assessment, and to resort to analogical thinking strategically and tactically, being suitably respectful of the critical distinctions between them. In strategic analogy, cyber is entirely familiar. If we are able to think strategically about Landpower, sea power, air power, and Earth-orbital space power, ipso facto we can think strategically about cyber with its electrons. The EMS does not pose a challenge to the theory of strategy.

However, efforts to think tactically by analogy about cyber are certain to be seriously misleading and probably disastrously wrong. Cyber is as different from the military power of the other geographical domains as they are from each other. Indeed, because of the nonphysicality of cyber power (though not of the cyber infrastructure and its human operators), this fifth domain is uniquely different technically and tactically. The challenge to understanding is the necessity for us to be fully respectful of the distinctive "grammar" of cyber, without falsely assigning similarly unique meaning to its policy and strategy "logic. "

Four broad conclusions are compelling at this time. First, cyber power will prove most useful (or dangerous, as enemy cyber power) as an enabler of joint military operations. Horror scenarios of stand-alone (miscalled "strategic") cyber attacks are not persuasive. The United States should expect its cyber assets to be harmed in conflict, but, if disrupted as anticipated, the country will repair, recover, and fight on. A like judgment applies to our Landpower, sea power, air power, and space power.

Second, while it is probably true to claim that, for technical reasons, cyber offense usually is likely to achieve some success, more significantly, is it probably true that the harm we suffer is most unlikely to be close to lethally damaging. Thanks to the technology that makes cyberspace, our discretion in the re-creation of cyberspace should present our enemies with unsolvable problems. Cyber offense is swift, but it is not likely to be deadly, and it should not work twice. Cyber defense ought to prove good enough.

Third, it is sensible to try and remember that cyber power is only information. Moreover, cyber is only one among many ways in which we collect, store, and transmit information. As if that were not contextual caveat enough, it is important to recognize that there is a great deal more to conflict and actual warfare than information, no matter what the tools for gathering and transmitting data may be. From the beginning of time, armies have clashed in relative ignorance. This is not to demean the value of information, but it is to remind ourselves that information, even knowledge (or its absence), is not a wholly reliable key to strategic success or failure.

Fourth, overall, despite the acute shortage of careful strategic thought on the subject, and notwithstanding the "Cybergeddon" catastrophe scenarios that sell media products, it is clear enough today that the sky is not falling because of cyber peril. The fundamental reason we can be confident about this is because cyber power, ours and theirs, is ruled by the general theory of strategy. Once we shed our inappropriate awe of the scientific and technological novelty and wonder of it all, we ought to have little trouble realizing that as a strategic challenge we have met and succeeded against the like of networked computers and their electrons before. The whole record of strategic history says: Be respectful of, and adapt for, technical change, but do not panic.

*Download the complete study (435 kb) at the US Army War College SSI site.*

Table of Contents

## Six U.S. Air Force Cyber Tools Designated As 'Weapons'

By Rick Wilking, Reuters, 10 April 2013

COLORADO SPRINGS, Colo. (Reuters) - The U.S. Air Force has designated six cyber tools as weapons, which should help the programs compete for increasingly scarce dollars in the Pentagon budget, an Air Force official said on Monday.

Lieutenant General John Hyten, vice commander of Air Force Space Command, which oversees satellite and cyberspace operation, said the new designations would help normalize military cyber operations as the U.S. military works to keep up with rapidly changing threats in the newest theater of war.

"This means that the game-changing capability that cyber is is going to get more attention and the recognition that it deserves," Hyten told a cyber conference held in conjunction with the National Space Syposium in Colorado Springs.

Hyten's remarks came a month after U.S. intelligence officials warned that cyber attacks have supplanted terrorism as the top threat to the country. Spending on cyber security programs has gone up in recent years, but may face pressure given mandatory across-the-board cuts to the Pentagon's planned spending on military equipment, programs and staff.

Hyten said the recent decision by Air Force Chief of Staff General Mark Welsh to designate certain cyber tools as weapons would help ensure funding.

"It's very, very hard to compete for resources ... You have to be able to make that case," he said.

Hyten said the Air Force is also working to better integrate cyber capabilities with other weapons.

He gave no details on the new cyber weapons, but the Pentagon has become more open over the past year about its work to develop offensive cyber capabilities in the face of escalating cyber attacks by China, Russia, Iran and others.

The United States and Israel are widely believed to have developed the Stuxnet computer virus that was used to attack an Iranian uranium enrichment facility, the first publicly known example of a virus being used to attack industrial machinery.

Hyten said the Air Force planned to expand its cyber workforce of about 6,000 by 1,200 people, including 900 military personnel.

He said it took the Air Force decades to explain the central importance of space-based assets for warfare, but did not have time to wait with cybersecurity.

"We have to do this quickly. We cannot wait. If we just let decades go by, the threat will pass us screaming by," he said.

Hyten said the Air Force was trying to leverage investment in cybersecurity already being made by private industry, but still had work ahead to improve its interface with the companies that operate the largest computer servers, and any agreements would have to benefit both sides.

"We have to bring resources to the table," he said. "They don't stay in business by doing things for free."

Table of Contents

## Mexican Social Network Manager Quits Post amid Threats from Drug Traffickers

From Latin American Herald Tribune, April 10, 2013

MEXICO CITY – The manager of the Facebook and Twitter accounts for Valor por Tamaulipas, or VxT, an outlet that reports on drug-related violence in the northeastern Mexican state, said he was shutting down the sites nearly two months after a drug cartel put a price on his head.

"I cannot remain in this trench for different reasons, I believe it is not necessary to explain them. And I do not know if you will believe that I have not surrendered and will not surrender. But I believe I have given all I can give and it has started to become impossible to manage the Web site, the reports, the risks," the unidentified online journalist said in a Facebook post.

"The social networks are a battlefield on which the main users have some type of interest or role in this war," the message said.

Valor por Tamaulipas, whose name means "Courage for Tamaulipas," has 214,000 "likes" on Facebook.

The online media outlet has reported on drug-related violence in Tamaulipas, a state plagued by a turf war pitting the Gulf cartel against the Los Zetas and Sinaloa cartels.

Mexico's drug cartels are using social-networking sites to battle "intelligence personnel from the National Defense Secretariat and the Navy Secretariat," as well as other individuals who pass themselves off as "high-level representatives of 'citizen cooperation'" without openly revealing their interests in the conflict, the message said.

A drug cartel put a bounty of $47,200 in February on the head of the manager of Valor por Tamaulipas's Twitter and Facebook accounts.

The outlet's posts are widely followed in northern Mexico.

Table of Contents

## U.S. Military Working to Integrate Cyber Weapons into Commanders' Arsenals

By John Reed, Foreign Policy, April 9, 2013

U.S. military commanders around the world are discussing how to integrate cyber weapons with all the other tools in their arsenals, according to the chief of the Navy's cyber forces.

Doing this will give battlefield commanders the ability to choose which weapon they want to use to achieve a desired effect.

"Whether we do that through the spectrum [via electronic warfare], we do that through the network [via cyber] or we do that through something kinetic [bullets and bombs], what we want to be able to do is be able to tee up to the commander, multiple options," said Vice Admiral Michael Rogers during the Navy League's annual Sea Air Space conference just outside Washington today. Then, "the commander can make the decision about what's the best tool to use. . . . I don't get any pushback on that idea at all."

"If we think we're going to do cyber off in some closet somewhere we have totally missed the boat on this thing," Rogers noted.

At the same time, the lines between traditional electronic warfare -- radar jamming, electronic eaves dropping, etc. -- and cyber warfare are containing to blur, at least in the U.S. Navy.

"I see those lines blurring increasingly There is great convergence between the spectrum [EW] and the cyber world at the moment which I think just offers great opportunities, as a SIGINT [signals intelligence] kind of guy by background, I just lick my lips at the opportunities that I see out there in that arena," said Rogers.

While Rogers didn't elaborate on the type of combined cyber-electronic warfare missions he envisions, a fellow admiral noted that the Pentagon is looking at non-cyber ways of shutting down an enemy's ability to fight without firing a shot. (Remember, cyber-philes often point out that cyber weapons can cripple a nation without a single missile being launched.)

"Cyberspace can be an enabler but there's [other] non-kinetic ways to disadvantage the enemy in cyberspace that don't require a cyber activity; [electronic warfare] capability, and other things like that," said Rear Admiral Michael Hewitt, deputy director of the special programs cross functional team on the Joint Staff, during the Navy League's annual Sea Air Space conference just outside Washington today.

Table of Contents

## The Explosive Effects of Rumors in Syria and Insurgencies around the World

By Scott W. Ruston, Chris Lundry, Pauline Hope Cheong and Daniel Bernardi, Small Wars Journal, March 21, 2013

Abstract: Frequently dismissed as trivial or unimportant because untrue, rumors are a potent in the information war that characterizes contemporary conflicts, and they participate in significant ways in the struggle for the consent of the governed. As narrative forms, rumors are suitable to a wide range of political expression, from citizens, insurgents, and governments alike. The authors make a compelling argument for understanding rumors in these contexts as "narrative IEDs," low-cost, low-tech weapons that can successfully counter elaborate and expansive government initiatives of outreach campaigns or strategic communication efforts. While not exactly the same as the advanced technological systems or Improvised Explosive Devices to which they are metaphorically related, narrative IEDs nevertheless operate as weapons that can aid the extremist or insurgent cause. Building from a book length study, this article explores how rumors fit into and extend narrative systems and ideologies, particularly in the context of insurgency, civil unrest and terrorism/counter-terrorism; and the article provides four basic rules to help strategic communicators, diplomats, planners and development personnel deal with the deleterious effects of rumors.

**Introduction**

Strategic communicators often dismiss rumors as untrue or as gossip and thus trivial. Yet research shows that rumors can have serious social, economic and political consequences. Rumors about President Obama's birthplace, despite their falsity, have armed his political foes and distracted attention from his governance.

Rumors that Jews or the Bush Administration were behind the 9/11 attacks on the World Trade Center extend and reinforce troubling stereotypes and conspiracy theories. And in Iraq and Afghanistan, rumors magnify the use of violence and ideology that shapes the allegiance of the contested population—those caught between supporting the host government and coalition forces on the one hand and the insurgency or Taliban on the other. Recognizing the importance of rumors, especially their function in periods of civic unrest, and understanding their nature and spread as a particular kind of story phenomena are the subjects of our recent book *Narrative Landmines: Rumors, Islamist Extremism and the Struggle for Strategic Influence* (Rutgers University Press, 2012).

Rumors form a particular threat during emerging and ongoing insurgencies, and we are seeing this played out in Syria today, where rumors are rocking the embattled regime of Bashar Al-Assad. Al-Assad's brother's legs were blown off by a recent rebel attack and military deputy chief of staff Asef Shawkat was poisoned strike at the heart of Assad family security. Al-Assad's wife fled to Russia and Vice President Farouk al-Sharaa defected to Jordan both suggest a crumbling regime amidst a socio-political crisis. At the same time, rumors abound about the insurgency. The rebels are funded and supported by al-Qaeda and Chechens are fighting side-by-side with the rebels feed into regional and global fears of terrorism, and also position the rebels as antagonists in the broad foreign policy narratives of both the United States and Russia.

As with all rumors, these rumors feed on small bits of information and events, fill in gaps of information and integrate with the larger narrative landscape—the complex array of stories prevalent within a specific social, economic, political and mediated environment. For example, the successful rebel attack on July 19, 2012 that killed two Syrian defense ministers and other top officials created plausibility for rumors of Maher Al-Assad's injuries, and the lack of public sightings of Shawkat and al-Sharaa created a gap in information that the rumors filled. (Reports have confirmed Shawkat died in the July blast, not in May by poison as the rumors claimed.) Rumors of foreign fighters, whether al-Qaeda or Chechen, integrate with the global narrative system of stories of fighters pouring into Iraq and Afghanistan, as well as al-Qaeda fighters honing their skills supporting the Chechen insurgency, thereby leveraging regional narratives stretching from Iran to Lebanon to Israel.

In the context of an insurgency, rumors are narrative IEDs. Like their kinetic cousins, they are the preferred communication weapon of the insurgent because they can be constructed of locally available stories and hidden in the landscape until detonation. This is because they are ad hoc and difficult to detect by the diplomat, analyst, or combatant until they explode, disrupting outreach, communication and influence campaigns. Of course, many governments also plant narrative IEDs in the form of whisper campaigns, and these also leverage bits and pieces of prevailing stories. Yet regardless of the source of a rumor, once let loose these narrative IEDs can become volatile and unpredictable. Understanding the following four basic rules governing the nature and function rumors can help strategic communicators deal with this lethal threat.

**Rule 1: Truth and Falsity Do Not Matter**

When it comes to the relationship between rumors and insurgencies, the first rule is that facts do not matter—just ask President Obama. People caught in an information vacuum often digest rumors as news. These "news" stories spread in multiple directions and in various media and draw upon prevailing stories. During the build-up to the Iraq war, the story heard around the world was that Saddam Hussein had stockpiled weapons of mass destruction. To support this story, U.S. government officials and journalists cited an array of "facts." Other government officials and journalists contested the story with their own battery of "facts." As we now know, the naysayers were correct. Yet in the post 9/11 environment, coupled with Hussein's previous use of chemical weapons against the Kurds in Northern Iraq, the rumor that Iraq has stockpiles of WMD that could lead to a mushroom cloud appearing over the U.S. prevailed. What is fascinating about this whisper campaign is that Saddam Hussein also spread it in an effort to intimidate Iran. Even today, long after the fruitless search for WMD during the occupation of Iraq, the story that Hussein shipped his WMD to Syria remains credible among a large number of Americans, according to a 2012 poll.[1]

**Rule 2: Story Matters**

Why do stories matter? Storytelling is one of the foremost methods of organizing information and making sense of the world around us. While the psychological elements (fear, anxiety, dread, wish, etc.) are important, it is the narrative elements—how rumors operate as stories and within broader systems of stories—that illuminate their potency, significance and potential consequence far more. Stories take characters, events, actions and settings and make sense of them through cause and effect. For example, the July 19 attack (event) in Syria (setting), subsequent public absence of Maher Al-Assad and al-Sharaa (characters), coalesced into explanatory tales of death and defection. Al-Sharaa's defection made sense as the effect of a crumbling regime and collapse of support for Basher Al-Assad. Participating in a broader system of stories centered on the Syrian conflict, they become predictive or wish-fulfilling (for the rebels) or dread-inducing (for

regime supporters), which are common functions of rumors. Furthermore, seeing rumors through a narrative lens also points towards methods of countering them by organizations negatively impacted by rumors. In fact, the recent rumor that Al-Assad released Al-Qaeda strategist Abu Musab Al-Suri dilutes the narrative clarity of rumors that the rebels are working with Al-Qaeda.[2]

**Rule 3: Rumor Mosaics Signal an Emerging Threat**

While some of the anti-Assad rumors have been tempered by public sightings of their subjects, they nevertheless constitute a rumor mosaic. A rumor mosaic is a cluster of otherwise distinct rumors that collaboratively reinforce a particular narrative. The mosaic of Assad regime collapse and defection presents a picture of a vulnerable government struggling to maintain internal unity and personal security. This narrative fits the desired worldview of the rebels and these "micro-stories" work together within a broader narrative system. In this case, the narrative system includes other stories (of rebel victories for example) and charts a narrative trajectory of the demise of the Syrian regime: rebel attacks wound and kill key personnel; family members flee; other leaders defect. This particular narrative resolves with Assad's defeat. Regardless of whether these rumors are actually true (and some have been proven false), it is not the facts that matter, but rather the believability of the cluster of interconnected rumors forged by their integration with the narrative landscape.

**Rule 4: Rapid Transmediation Signals an Imminent Threat**

The spread of rumors, whether in the U.S., Iraq, Syria or most anywhere else, is facilitated by transmediation, a process involving the appropriation, reconfiguration and retransmission of messages across different media platforms—frequently but not exclusively online. Each change of medium involves both alteration of form and, sometimes subtly, meaning. In particular, one rumor meme that exhibits this phenomenon of transmediation is the rumor of Asma Al-Assad's departure for the safer haven of Russia. Reports of her evacuation first circulated on Twitter, and then in mainstream newspapers. Jumping from text to image, political cartoons of the posh Asma running from a smoking Damascus and using Syrian flag draped coffins as stepping-stones joined the rumor of her exit with previous stories of extravagant shopping during times of crisis. This exit rumor is thus believable as it exhibits narrative fidelity—it rings true—in the context of the rumor environment and narrative landscape concerning the Assad regime. Yet despite the subtle changes in form and meaning, the underlying story remains intact as the rumors cluster into a mosaic that extends the narrative that the Assad family cares little for the Syrian people and the regime is at risk.

**Conclusion**

Media environments in places such as pre-conflict Syria tend to foster skepticism since their citizens are seldom exposed to news critical of the government. This skepticism facilitates an information vacuum in which rumors fester and spread through underground channels. Rumors then explode in chaotic environments like war-torn Syria, becoming important sources of news for the population, and can cause civilians to support or reject an existing regime, an insurgency, or even an outside actor. Indeed, despite the fact that rumors are often (though not always) comprised of lies and half-truths, if the stories seem credible or "ring true" they can seriously impact political, economic and governmental action. An example from Iraq illustrates this principle succinctly.

In 2005, U.S.-led coalition forces in Iraq began an outreach campaign inoculating cattle, trying to prevent significant losses in the face of drought and disease. What began as an economic stability program quickly became a problem when rumors spread that the U.S. Army veterinarians were poisoning the cattle in order to starve the Iraqi people. The conspiratorial punch and narrative elements of this rumor appealed to imagination and fear, especially during a time of crisis when official news sources were silent or untrustworthy. The rumor both exhibited consistency with a long history of stories of foreign invaders pillaging Iraqi resources (Crusaders, Mongols, et al.) and provided an explanation for the increase of dying cattle. The rumor's power came from its congruence with established stories of exploitation, and the rumor effectively disrupted the outreach campaign.

Rumors are the reality of the citizens who believe them. In conflicts from Iraq to Indonesia to Singapore – as well as in Syria or other flashpoints—those who ignore rumors and their potential effects do so at the peril of their strategic communication interests. To be sure, detrimental rumors, as narrative IEDs, are not insurmountable. Just as new technology allows for defense against their explosive cousins, understanding a culture's narrative and media landscape, where rumors form and cluster, allows for defenses against these weapons of the weak and the strong. Strategic communicators need to pay attention to them, track their flow and understand their narratological charge in order assess their impact and develop appropriate countermeasures. And while that is certainly easier said than done, it is certainly possible.

**Notes:**

[1] In a 2012 poll, 63 percent of Republicans, 27 percent of independents, and 15 percent of Democrats believe that Iraq had WMDs when the US invaded in 2003. http://www.huffingtonpost.com/2012/06/21/iraq-wmd-poll-clueless-vast-majority-republicans_n_1616012.html.

[2] http://www.dailystar.com.lb/News/Politics/2012/Feb-01/161761-rumors-swir...

Table of Contents

## North Korea's Threats, Campy Videos Drawing Internet Attention

By Chico Harlan, Washington Post, April 11, 2013

SEOUL — North Korea — the reclusive, impoverished state that denies Internet access to all but a handful of its citizens — has, improbably, become an online sensation.

With its chubby dictator, campy propaganda videos and near-daily threats of attack against its neighbors and the United States, the secretive police state has never been more searched for, tweeted or discussed. Some semi-chagrined analysts say the North, for the first time, has gone viral.

Although Pyongyang tries every few years to drive up regional tensions and win political concessions, this latest saber-rattling has more forcefully captured global attention, in part because the mysterious and potentially dangerous North so perfectly feeds the appetites of the Internet and social media.

In recent days, Google search interest in North Korea has spiked: Seven times more people searched for information about North Korea in March than at the previous high point of interest, October 2006, when the state successfully completed a nuclear test. Within the United States, North Korea was Twitter's No. 3 trending topic for the week ending April 4, behind Easter and Good Friday.

Analysts say the surging interest plays into North Korea's hands, amplifying the sense of crisis on the Korean peninsula. The North caters to the Web by using social media and updating its state-run news agency Web site several times a day — fresh rhetoric for every news cycle, in what South Korea's national security chief called a "headline campaign."

"In tension-building, North Korea is succeeding beyond expectations," said Andrei Lankov, a North Korea expert at Seoul's Kookmin University. "This is the most publicity North Korea has gotten in 30 years, and perhaps since the Korean War."

In recent weeks, the North's rhetoric and belligerent activity has been particularly intense. North Korea nullified the armistice that ended the Korean War, threatened a preemptive nuclear strike against Washington, announced the restart of a reactor that generates weapons-grade plutonium, and shuttered an industrial complex that it had operated jointly with South Korea. Thursday, it claimed "powerful striking means" were on standby ahead of an expected midrange missile test.

With Secretary of State John F. Kerry due to arrive in South Korea on Friday for previously scheduled meetings, Seoul deployed three naval destroyers, an early-warning surveillance aircraft and a land-based radar system to help it detect the potential launch, a Defense Ministry official told the Associated Press.

Some 36 percent of Americans say they are tracking North Korea-related news, making it the most closely followed foreign news story of the year, according to a survey conducted by the Pew Research Center.

The Web popularity is notable, in part, because the North's leaders — fearful of any tool that could spread dissent — have tried to seal off their nation from the Internet, limiting access to only a few hundred people. Those elites, largely members of the North's propaganda department, use the Web strictly for state-sanctioned purposes, crafting messages that portray the North as an imperiled but determined fighter, under threat from U.S. imperialists, united under its peerless leader.

Table of Contents

## Socialism and the Global Information War

By Heiko Khoo, China.org.cn, April 14, 2013

The battle of ideas is central to the struggle for world socialism. Leaflets, newspapers, books, theatre troupes, radio, film and television have all played an important role in ideological warfare over the last 100 years. Recently the Internet has facilitated the rapid mobilization of rebellions in North Africa and the Middle East, which shattered apparently stable regimes.

However, what Marx wrote in 1845 remains true:

"The ideas of the ruling class are in every epoch the ruling ideas, i.e., the class which is the ruling material force of society, is at the same time its ruling intellectual force."

The world hegemony of capitalism remains a fact. It is backed by powerful instruments of propaganda, which constantly seek to anchor the outlook of the ruling class within wider society. This continues despite a profound transformation in the balance of power that has accompanied the world economic crisis.

Analysts working for the People's Liberation Army have long understood the need to study and develop methods of "people's warfare in the information age." As early as 1996, the Liberation Army Daily carried an excellent article by Wei Jincheng, where he explained that: "A people's war in the context of information warfare is carried out by hundreds of millions of people using open-type modern information systems." The era that he prophesied is now reality. But the tools available are inadequately used to transform global consciousness. Today's world of network-centric information war, where public perceptions and attitudes are shaped by interaction with the Internet and the global mass media, necessitates a constant struggle to explain reality, and to win hearts and minds to the socialist cause.

Capitalist governments are waging war against their own people in the name of everyone "tightening their belts" meanwhile the super-rich have stashed away US$32tn in offshore tax havens. The justification for the system of wealth distribution is undermined by ruthless cuts targeting the working classes and poor. Nevertheless a barrage of absurd and persistent propaganda seeks to blame the poor for being poor. It accuses public sector workers of being selfish and lazy and promotes the concept of national-patriotic unity to confuse people during times of crisis.

Democratic elections do not change the fact that these governments represent the business and banking elite, who pull the strings behind the democratic facade. They buy political and ideological power and manipulate the minds of the people to believe that they live in freedom. In Europe, where welfare capitalism provided decades of relative stability, tens of millions are waking up to the real character of the crisis and are gradually forming views antithetical to capitalism itself.

Nobel Laureate Joseph Stiglitz, the influential former chief economist and senior vice president of the World Bank, wrote a damning condemnation of the system in his book, "The Price of Inequality: How Today's Divided Society Endangers Our Future". He shatters the myth that making a tiny minority rich helps society and shows that increasing inequality hinders economic and social progress. Beijing University Professor Justin Yifu Lin recently held the same World Bank post as Joseph Stiglitz had. He believes that China's economy must upgrade its infrastructure and organize its productive activity to exploit its comparative advantages in the world economy. However, his ideas avoid any consideration of the comparative advantages of socialist economics and philosophy. In the world battle to win hearts and minds, what social and economic policies can offer an alternative to ever increasing inequality? Surely it is because of the advantages of publicly owned banks and industries that China avoided the worst of the global crisis.

The need to impact world opinion of the majority is rooted in the internationalist vision of Marxism. Before 2008 Western business advisors lectured China about the need to adopt the capitalist model. It continues to be the case that business lobbies get more attention in China than links to the workers of the world. But if Europe's workers knew that China is building 36 million low-cost apartments for the workers; that wages are rising rapidly; and that welfare provision is expanding, this could play a big role in shifting consciousness about the so-called necessity of austerity in their own countries. If they knew the colossal scale of China's public sector investment in railways, transport and green technology, European workers would more easily be able to envisage and demand alternative economic plans.

Inside China, real and dramatic progress, when poorly expressed in the form of propaganda, often evokes scorn, skepticism and mockery. This is multiplied in the Internet age at a speed and scale that no one can contain. So there is an urgent need to focus attention on defending core public sector advances and improving all aspects of democratic control over public property. Improvements for the masses should find expression from the people themselves and the media should act to facilitate this.

Yu Jianrong, the director of the Social Issues Research Center at the Chinese Academy of Social Sciences Rural Development Institute, hit the nail on the head in a recent article where he explained that the present system of rigid and static stability – aimed at the preservation of order – should give way to a dynamic, resilient and creative stability. In this way, the dialectics of social unrest can become a source of energy and vitality. This can help to sweep away corruption and the abuse of power, defend public property and invigorate the communist cause. Social unrest can become a productive force that helps to reduce inequality and foster a more participatory and harmonious society.

Table of Contents

# Training the CAPOC Soldier

By Sgt. 1st Class Andy Yoshimura, DVIDS Hub, 16 April 2013

JOINT BASE MCGUIRE-DIX-LAKEHURST, N.J. - A group of Army Reserve soldiers comprised of military occupation specialties such as ammunition specialists, infantry and finance all have one thing in common. They are all here in New Jersey attending one of two courses: the civil affairs or the psychological operations reclassification course.

More than 90 percent of CA and Psyop enlisted soldiers of the U.S. Army Civil Affairs & Psychological Operations Command (Airborne) have attended the reclassification course taught by soldiers of the 80th Training Command. Both 29-day courses are comprised of classroom activities, a tactical situational training exercise and end with a week-long field training exercise which combines soldier tasks along with MOS tasks.

The FTX has also allowed the opportunity for CA and Psyop teams to work together in various simulated scenarios.

"Combining CA and Psyop allows both groups to get a better understanding of each other's MOS," said Sgt. 1st Class Vaid Sadiku, 37F Psyop course manager, 80th Training Command. "They can learn how to integrate and work with each other for future exercises and deployments. A lot of CA and Psyop soldiers who are deployed don't know the capability of each other."

For Sadiku, training at this level is crucial before they return to their unit.

"The standard needs to be increased and we want to create a higher caliber soldier then what has been produced in the past. We have the personnel in place to ensure that standards are adhered to," added Sadiku.

Students such as Sgt. 1st Class Sonya Lundy of the 448th Civil Affairs Battalion had the opportunity to experience the school on both sides. Lundy, a Psyop soldier, is attending the CA course and is having to learn the critical task training of all ranks. Lundy is joining her husband as the new CA soldier in the family.

"I am learning a lot. It’s a very interesting perspective to see the difference between Psyop and CA," said Lundy. "I see that the Psyop and CA are encouraged to work together which is something you see in a community and I really like that part."

As Initial Entry Training soldiers attend the U.S. Army John F. Kennedy Special Warfare Center and School of Fort Bragg, the seasoned experienced soldiers have attended schools taught by the 80th Training Command in three locations: Joint Base McGuire-Dix-Lakehurst, Fort Knox and Fort Hunter Liggett. The training that the soldiers are receiving follows the guidelines that of SWCS. Integrating and adapting to a new MOS have challenged the seasoned veterans.

"It is a challenging course," said Sgt. 1st Class Aaron Stubenvoll, 38B CA course manager, 80th Training Command. "Having the students to think outside of their prior experiences and tying it into civil affairs scenarios can bring difficulty."

"Because most of the senior noncommissioned officers have already gone to the advanced and senior leader course for their prior MOS, it is harder for them to understand the more advanced portion of the CA and Psyop skill sets." added Stubenvoll.

For Lundy the transition was easy. "I know what those guys are doing. A lot of things that they do is what we do as civil affairs," said Lundy. "It’s easier when you understand what the people you are supposed to be closely working with are also up to."

The FTX at the end of the course has helped students who are not accustomed to the verbal and nonverbal ways of communication. Spc. Ian Macleith, a former ammunitions specialist and now with the 315th Psyop Company, came from a controlled non-personal environment and has enjoyed the integration of the interpersonal communication portion of the course

"Coming out to the FTX is good and it allows us to put all of the things we learned in class into play," said Macleith. "This gives us the chance to exercise what we learned and the FTX portion of the course is perfect because it is the culmination of all of the events of classroom and all of the exercises that we have done."

Upon completion of the FTX, CA and Psyop students look for two things: qualification and a certificate in completing the course. These soldiers will now go back to their unit understanding their new roles and at the same time strengthen unit's capability in completing their mission.

"I really want to go back to my unit and use the skills that I have learned here," added Macleith.

Table of Contents

## Combat on the Online Battlefield

By Steve Arel, U.S. Army Cadet Command, April 16, 2013

LEXINGTON, Va. -- The once-definitive frontlines of the battlefield have become blurred. A Soldier never knows when or where the enemy might surface.

So when military leaders and strategists discuss the combat environment, they describe it as a 360-degree arena.

Cyber warfare offers even more disguise, taking those blurred battlefield lines and completely wiping them away.

"Eventually, we'll be talking about battles online," said Joshua Smith, a Cadet with the University of Wisconsin-Stout. "It's as important as any battlefront we'll fight on."

Cyber warfare has become an increasingly relevant topic among the mix of roundtables offered to soon-to-be lieutenants attending the annual George C. Marshall Awards and Leadership Seminar. Electronic dangers pose such a threat to national security these days that all branches of the military created specialty fields to employ Soldiers who can understand the vulnerabilities and devise ways to combat them.

The Marshall roundtable session titled "Ethics of Cyber Warfare" demanded considerable contemplation from Cadets, getting them to use critical thinking skills and outcomes-based methodologies to weigh what might provoke forceful action and how best to respond. Unfortunately, Navy Capt. Michael Boock admitted a few times, the definition of an act of war in the cyberworld isn't clear-cut.

Besides, there aren't established norms and rules of engagement covering technological warfare as there are in traditional combat. And that's what can make judging something as a use of force that warrants armed conflict so difficult.

So when would a cyber-related situation cross the line from peace to war, Boock asked the Cadets.

He posed a scenario where a foreign country enacts a cyber attack against the United States that ends up shutting down Wall Street for a day. No transactions get made, no stocks get traded, no purchases or sales go through. Losses from the inactivity could be immense.

Beyond that, the shutdown could trigger panic, affecting people's psyche as they wonder how long the shutdown will last and how badly their investments will suffer, said Morgan Mushlitz of Seattle University.

"That's a visible action against the United States," an adamant Mushlitz said.

But when Boock suggested bombing the responsible party because of its perceived use of force, Mushlitz balked. Boock said a resolution could come through diplomatic means or by not responding at all.

In cyber warfare, targets usually don't know they've been affected -- or by whom -- until it's too late. One Cadet asked about time limitations on retaliation.

That depends, Boock said. One would have to know the source of the attack and who or what initiated it. Then, political leaders would have to be convinced and approve a response. And if they choose to do so, they'd have to determine the most appropriate means.

"It's a lot easier if you've got guys with AK47s coming across the border," Boock said. "It's not so easy with a group of guys on a computer."

Smith will graduate this spring with a bachelor's degree in information technology. He knows the importance of digital technology, the power of the Internet and the havoc wrong-doers can wreak by hacking and manipulating computer systems.

The world has become so reliant on computers and connectivity that even the slightest interruption can have far-reaching effects, Smith said. Technology is so key, he believes more damage can be done with a computer than with a rifle.

"There will always be a need for land and air warfare," Smith said. "This is going to be the way wars are fought."

Cyber issues have been discussed in government circles since the 1990s, but they've moved to the forefront in recent years. As the cyber field continues to evolve and new threats emerge, Boock predicted that someone participating in his roundtable would spend time during their career working in the field.

"It's going to be a growth industry," he said. "Even with budget cuts, they're not cutting cyber. Everybody's in."

Table of Contents

# New Cyber Rules Put Combat Decisions in Soldiers' Hands

From The Army Times, 16 Apr 2013

The Defense Department is close to completing a version of the rules of engagement that will clarify how troops operating in cyberspace may respond to threats, cyber espionage and attacks, according to military and cybersecurity experts.

The rules would allow troops to identify threats and ensure senior leaders share information quickly and take action, if necessary, Gen. Keith Alexander, the top officer at Cyber Command, has said.

Pentagon officials have been more public about U.S. Cyber Command's efforts in recent months. The military is creating a series of cyber teams, 13 focused on offense — when directed by the White House — and an additional 27 to support the military's war-fighting commands and domestic security organizations, according to Alexander.

The standing rules, which are being updated for the first time since 2005, cover the physical war-fighting domains as well as cyberspace, according to Pentagon spokesman Lt. Col. Damien Pickart. Once released, they will not be made public.

The rules would establish a framework of legally permissible responses for U.S. troops operating in cyberspace, a new war-fighting domain defined by rapidly changing technology, adversaries whose identities are often unclear and knotty legal questions.

"The technology always outpaces the policy and the [tactics, techniques and procedures]," said Jeff Moulton, a researcher with the Georgia Tech Research Institute. "It's clear as mud in the cyber world because there are so many variables that you don't know."

The cyber teams operating under those rules will be assigned to the joint geographic and nongeographic combatant commands, such as U.S. Strategic Command and U.S. Transportation Command, according to an Army official. Soldiers in newly created military occupational specialties related to cyber will be part of these teams.

The rules would reduce the need for an operational unit to consult an attorney before taking action, the official said. Troops will be able to react to threats quickly without asking for permission at every step.

"You want rules of engagement so you don't have to go back and say, 'Mother may I,'" the Army official said.

The rules would allow troops to conduct reconnaissance and counterreconnaissance, and offer more flexibility to identify threats and mitigate attacks, the official said.

Without rules of engagement, commanders have no idea what they are permitted to do, and with them, they have some autonomy, said Paul Rosenzweig, founder of Red Branch Consulting, who advises The Chertoff Group, a security and risk-management firm. Rosenzweig is a former deputy assistant secretary for policy in the Department of Homeland Security and former acting assistant secretary for international affairs.

"You have two modes, button-down with pre-programmed responses, and the ones where you need authority to begin the action — where you need to push the button to go," Rosenzweig said.

It is not as though the military is paralyzed against cyber attacks today. The Defense Department is responsible for defending the nation's critical infrastructure from an attack, supporting its combatant commands in their operations in planning, and defending its networks and other networks, "as authorized," according to Alexander's congressional testimony in March.

Cyber Command's operating concept calls for it to recognize when an adversary is attacking, block malicious traffic that threatens its networks and data, and then maneuver in cyberspace to block and deter new threats. Alexander was asked how Cyber Command would respond to an attack on critical infrastructure.

"Right now, those decisions would rest with the president, the secretary [of defense]," Alexander responded. "And they would tell us to execute. I think as we go down the road, we're going to have to look at what are the things that you would automatically do. Think of this as the missile defense, but missiles in real time."

**New 'space race'**

Though a draft of the rules is said to be nearly done, it is unclear when it will be issued. In Alexander's testimony this month, he said the Defense Department, the White House and interagency partners would finish setting up the rules within months. In congressional testimony a year earlier, he said roughly the same thing.

Time is of the essence. The last update to the Defense Department's standing rules of engagement came in 2005, and in about seven years, computing power has advanced by a factor of 16, Rosenzweig said.

"We're rushing to militarize the space," he said. "We're kind of like where we were with the space race with the Russians and Sputnik."

In this case, the main adversary appears to be China. A Chinese People's Liberation Army-run hacking group out of Shanghai is said to have unleashed countless attacks on U.S. companies and government agencies over the past few years. A recent report by Mandiant, a cybersecurity firm, exposed the group, although Chinese officials have denied government-sponsored attacks.

"To a large extent the war we are in with the Chinese is not a war, it's an espionage game, and that's OK because we know how to deal with that," Rosenzweig said. "If we keep ourselves there, we'll get to a stable solution."

There is cloudiness over this issue that raises questions of national security law. As the Defense Department creates its rules of engagement, it must grapple with the separate legal authorities for the country's armed forces and its intelligence operations.

"In the conventional world, these are defined, but [in] the virtual battle space, there's serious blurring," said Moulton. "The laws on the books are not necessarily congruent with the things we want to do or need to do to protect the nation, protect our critical infrastructure and conduct conflict."

The Pentagon is grappling with how much autonomy to give local combatant commanders and how much needs to be controlled by higher-level commanders in the United States.

If a commander in Maryland pulls an "electronic trigger" at the wrong time, it might leave soldiers on the battlefield vulnerable, but a commander without broader visibility might trigger second- and third-order effects outside his area of responsibility, Moulton said.

"What if we did something in the Pacific, we didn't understand the network topology and we knocked granny off a dialysis machine in the Netherlands?" Moulton said.

A Government Accountability Office report in 2011 found that under the DoD standing rules of engagement, authorities needed to be better coordinated, particularly in geographic combatant commands. In at least one incident, overlapping authorities led to "uncoordinated, conflicting and unsynchronized guidance," the GAO says in its report.

When the Defense Department launched a malware eradication effort in 2008, Strategic Command "identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both U.S. Strategic Command, military services, and a geographic combatant command."

**What response?**

When fighting back, what response is the right response? A NATO think tank recently released a new manual for cyberwarfare that, for example, differentiates between a cyber operation that has kinetic effects and cyber espionage, which does not qualify as an attack — an issue Alexander indicated is still unresolved.

"The issue that we're weighing is, when does a nuisance become a real problem?" Alexander has said. "And when are you prepared to step in for that? And that's the work that, I think, the administration is going through right now in highlighting that."

The manual suggests "proportionate countermeasures" against state-sponsored cyber attacks are allowed, but countries should refrain from the use of force. If for example, one country incapacitates a hydroelectric dam in a dispute over water resources, the other country is within its rights to target the offending country's irrigation control system.

Cyber weapons, or system exploits, are usually single-use, Moulton said, because an adversary will act quickly to patch his system after it's been disrupted. How should those cyber weapons be managed?

"It's a disposable commodity, so using one in the Pacific combatant command may take an arrow out of the quiver of the European combatant commander," Moulton said. "They're a perishable asset, and they need a centralized management system."

But who is attacking? The manual also highlights the thorny issue of attribution. It states that the fact that a cyber operation was launched from a government's infrastructure is not proof that the state's government launched the attack.

"Right now, there is an ambiguity in the attribution," Rosenzweig said, "and our response is difficult."

Table of Contents

## Cyber Warriors Association Points to Evolving Battlefield

By Kenneth Stewart, DOD Live, April 17, 2013

A Naval Postgraduate School student, U.S. Army Capt. Joseph Billingsley of Stamford, Conn., is building the military's first cyber warfare professionals association.

The Military Cyber Professionals Association, soon to be launched from Monterey, Calif., where Billingsley is currently studying for his master and doctoral degrees, will provide a professional home for the burgeoning cyber operations community. The association's Monterey chapter will be both a prototype and the association's flagship as it branches out to build a national organization.

"Monterey is a natural home for the association due to its proximity to NPS, DLI [Defense Language Institute], Silicon Valley, other defense personnel, and the interest in cyber initiatives," said Billingsley.

In a recent visit to NPS, U.S. Cyber Command deputy commander, Marine Corps Lt. Gen. Jon M. Davis, also recognized the area's commitment to cyber operations research and for its contribution to the creation of a community of cyber professionals.

"We are going to need 6,000 people in the next three years to build a cyber force … I know that those people live here [at NPS]," said Davis.

"The cyber domain matters because the prosperity and security of our nation depends on it," said Billingsley. "It's hard to imagine a single American business or military unit that does not rely on connectivity to accomplish at least some of its core functions. That trend is not expected to change any time soon."

Billingsley, an Army strategist with a background in signal intelligence, was selected by the U.S. Army's Cyber Command to pursue graduate cyber operations studies at NPS. He is currently pursuing a master's degree in cyber systems and operations, and a Ph.D. in information sciences.

"The Army cyber command gave me the opportunity to earn a cyber master's degree here at NPS that met our needs," said Billingsley. "Most cyber programs are more technical and seek to produce operators, but NPS' cyber systems and operations degree is perfect for me because it is a balance between strategy and technical scholarship."

Billingsley's graduate work revealed the need for a cyber association to bring together myriad professionals pioneering work in the cyber operations field. Professional military associations, like the one envisioned by Billingsley, provide a venue for military professionals to share lessons-learned and recognize each other's achievements. They also serve a social role, offering camaraderie and fellowship to highly-specialized groups that share jargon and experiences often foreign to those outside their communities.

Groups like the Association of Old Crows, which is mostly composed of electronic warfare professionals, or the ubiquitously named Air Defense Artillery Association, support closely-knit communities of professional military interest. Because these associations are often tied to specific defense disciplines, they reflect the way modern warfare has evolved over time.

"The cyber 'battlefield' has evolved tremendously in recent years," said Billingsley. "We have seen nation-states taking the cyber threat seriously by investing in their own cyber forces. With nations now explicitly fusing their military and cyber capabilities, we should expect to see an increasing level of lethality and destruction associated with the cyber domain … The benefits of our pervasive penetration of connectivity now leaves us rife with vulnerabilities to be exploited. This is a risk to be managed.

"More than influencing a target via information operations, we should expect to see entire networks and services rendered unusable, and even physical destruction by cyber means," continued Billingsley. "America has a shortage of people who really understand cyberspace, how it works, and how it may be integrated into operations large and small."

NPS' cyber ops students are researching a host of cyber security and warfare related subjects designed to protect cyber infrastructure, counter cyber attacks, and to build anti-hacking measures. Billingsley seeks to unite students like these with professionals from across the defense community and academia.

"As a strategist with an interest in cyber, I wanted to support strategic priorities like the development of the cyber workforce and operationalization of cyberspace. I intend to encourage folks from different world views like warfighters, academics, network techs, and intelligence personnel to come together and collaborate," said Billingsley. "I came up as a signal officer overseas and I saw the need for more cross talk and understanding in the cyber domain. I also saw the important role our military associations play and decided that the time was right for a cyber association that was joint and interdisciplinary."

MCPA hopes to recruit members from diverse cyber related backgrounds. As the cyber community continues to evolve, its connection with disciplines not traditionally linked to the cyber domain continues to increase.

"I did not want to get caught up with debates about hard boundaries of who is or who is not a cyber warrior because we are all still trying to determine what a cyber warrior looks like and where they fit in military operations," said Billingsley. "Theories about cyber warfare are not well developed yet. An association that includes a journal and various venues for dialogue may help inform discussions at every echelon."

Billingsley envisions an association that will encourage professional and social activity amongst its members, grant awards, support youth science and volunteering efforts, and encourage educational initiatives. Despite its infancy, association members have already begun outreach activities on the Monterey Peninsula that they hope will encourage future interest in cyberspace.

"The association has already begun a science, technology, engineering and mathematics (STEM) outreach program encouraging members to get involved by leveraging existing local initiatives like the Coder Dojo, supported by the Steinbeck Innovation Cluster, and the Cyber Adventures Program supported by NPS' Cebrowski Institute," said institute director and NPS Department of Computer Science Chair, Dr. Peter Denning.

"The MCPA outreach program provides access to enthusiastic and skilled technologists in order to better prepare youths for an increasingly interconnected world," added MCPA STEM Outreach Coordinator David Steinberg. "We offer curricula, trainings, and facilitate partnerships with entities that share our priorities. Our members span many disciplines and are determined to help raise the next generation of cyber professionals."

Table of Contents

## Is Cyber War the New Cold War?

By Trefor Moss, the Diplomat, April 19, 2013

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.

But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare's new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?

For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations – repeated attacks followed by often flimsy denials – almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.

The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China – Google and The New York Times being just two of the most high-profile victims – and which President Obama has now insisted are at least partly state-sponsored.

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM's operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military's regional commands; and a third to conduct national offensive operations.

As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another's virtual sovereignty much as they do one another's physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21st century reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

**Warfare's Wild West?**

Cyberspace is anarchic, and incidents there span a hazy spectrum from acts of protest and criminality all the way to invasions of state sovereignty and deliberate acts of destruction. Cyber attacks that might be

considered acts of war have so far been rare. It is certainly hard to characterise the rivalry between China and the U.S. as it stands as cyber warfare, argues Adam Segal, a senior fellow at the Council on Foreign Relations. "I tend to stay away from the term 'cyber war' since we have seen no physical destruction and no deaths," he explains. Segal accepts that there is a conflict of sorts between China and the U.S. in cyberspace, though he says it is "likely to remain below a threshold that would provoke military conflict.".=

While there is no internationally accepted categorization of different kinds of cyber activity (individual states have varying definitions), it is self-evident that some episodes are more serious than others. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) – a unit based, not by accident, in Estonia, which experienced a massive cyber-attack from Russia in 2007 – distinguishes between "cyber crime,""cyber espionage," and "cyber warfare."

China's cyber operations, for all their notoriety, have essentially been acts of theft – either criminals attempting to extract privileged data, or incidents of state-sponsored espionage (some of which, admittedly, had national security implications, such as the extraction of blueprints for the F-35 Joint Strike Fighter). But these operations did not seek to cause any physical destruction, and so would be hard to interpret as acts of war. This may explain why the U.S. government has been quite tolerant of Chinese hacking until now, seeing it as an irritant rather than as anything more provocative.

However, other states – notably the U.S. with its use of the Stuxnet virus against Iran – have arguably engaged in acts of cyber aggression. "Stuxnet might be considered an act of war, or at least a use of force," suggests Segal, though he adds that assigning labels to such incidents is never straightforward, even in the physical realm.

States certainly appear to be testing the boundaries in cyberspace, safe in the knowledge that those boundaries are undefined. There is almost a sense of lawlessness given the lack of consensus on how to treat cyber warfare from a legal standpoint. The U.S., for example, takes the view that existing international law can be applied to cyberspace. Others, notably China and Russia, have advocated a new code of conduct to address the unique problems that cyber operations create.

**Virtual Progress**

Recently , the CCDCOE made an important attempt to inform this debate when it published the Tallinn Manual, a detailed examination of the way in which existing international law might be applied to cyber warfare. "What makes the situation fairly unique is that there is not much cyber-specific international law regulating actions between states, and therefore states have to assess and analyze how the already existing, but not cyber-specific norms, apply to cyber activities," explains Liis Vihul, a scientist with the CCDCOE's Legal and Policy Branch. "It is at least the view of most western states that the international law dealing with the right of self-defense and also the conduct of armed conflict apply to cyber operations; the devil lies in the details – in other words, in some matters the states really have to think hard to figure out how exactly these norms play out in the context of cyber."

The Tallinn Manual is meant to guide governments through some of this hard thinking. Under international law, states are legally entitled to respond to an "armed attack" or a "use of force" in a proportionate way. Vihul says that "cyber activities carried out by states that injure or kill people or damage or destroy objects are most likely to be considered as uses of force." If a state suffers such an attack, it could be legally entitled to retaliate with cyber or conventional forces, even if the attack was purely cyber in nature, and even if the attack was perpetrated by civilian, rather than military, agencies.

However, cyber complicates the application of the existing law in two ways. The victim of a cyber attack might hide the fact that the attack ever took place so as not to reveal its vulnerability to other potential aggressors. Even more importantly, it is hard to attribute a cyber attack to another state in a way that would satisfy international law, given the attacking state's likely use of proxies.

The first challenge that states face is therefore proving the origin of an attack.

Secondly, states have to decide how to respond legally and effectively to cyber crime and cyber espionage. So far the governments have seemed inclined either to accept such attacks as a fact of interconnected life, or to try to retaliate with cyber operations of their own. The former approach only encourages further aggression, while the latter probably breaches international law if the original hack was not an example of the use of force. In future, the victims of virtual theft might instead focus on gathering evidence and then seek reparations at the World Trade Organisation or the International Court of Justice, much as they would do in cases of IP theft or breaches of sovereignty.

Thirdly, the international community must continue the debate where the Tallinn Manual has left it, and work to develop universally accepted rules and norms for operating in cyberspace. "I think the risks of

miscalculation or inadvertent escalation are very high if two sides do not share a common vision of what are legitimate targets or thresholds for acts of war," says Segal.

China and the U.S. have both said that they would like to see a rules-based cyberspace, but they do not see eye to eye on how those rules should be established. A costly and potentially dangerous Cyber Cold War awaits if they cannot do better, and agree on some rules of engagement for their rapidly expanding online forces.

Table of Contents

## Air Force and Army Disclose Budget for Hacking Operations

By Aliya Sternstein, NextGov, 19 April 2013

The Pentagon has for the first time detailed $30 million in spending on Air Force cyberattack operations and significant new Army funding and staff needs for exploiting opponent computers.

Since 2011, top military brass have acknowledged the United States has the capability to hack back if threatened by adversaries in cyberspace. Now, the Defense Department is providing lawmakers and taxpayers with evidence of network assault programs to sustain funding, budget analysts say.

The Air Force in fiscal 2014 expects to spend $19.7 million on "offensive cyber operations," including research and development, operations, and training, according to budget documents circulated this week.

The service estimates needing $9.8 million for new tools to run those offensive cyber operations, including memory storage, local and long-haul communications, and "unique intelligence and analysis equipment," a spending justification stated.

The Air Force money also would cover products for certain defense operations, described as "counter information" capabilities that protect systems and content against deliberate or inadvertent intrusions, corruption and destruction.

In addition, the account would fund infrastructure for training, exercises and rehearsals "to support real-world contingency missions."

Air Force officials told Nextgov they chose to divulge this information because cyber offense will be a standard line item from now on and the public needs to understand what it is paying for.

"We know the Air Force's capabilities in cyber are going to continue to be touchstones for the whole joint team, the whole of government and for the private sector," Air Force spokesman Maj. Eric Badger said. Cyber Command, for instance, is on track to install by fall a full mission force to deflect incoming assaults on networks powering energy, banking and other critical U.S. businesses.

The Air Force must explain why this additional money is necessary, at a time when the Pentagon is cutting back on other personnel and weapons.

"We are committed to maintaining the right balance of integrated cyber capabilities and forces that are organized, equipped and trained to successfully conduct operations in cyberspace. We're equally as committed to doing so in a way that's respectful of the taxpayers' dollar," Badger said.

Elsewhere in the Pentagon budget, the Army proposes hiring 65 new employees and spending more money -- $4.9 million more -- for "computer network exploitation" and "computer network attack" capabilities.

Some military spending analysts wonder whether the services are wasting money by duplicating hacking investments.

"Do we really want each service going off and developing their own capabilities for these threats?" questioned Todd Harrison, senior fellow for defense budget studies at the Center for Strategic and Budgetary Assessments. "How much redundancy are we building across the services in the areas of cyber? What is unique to the Army?"

It could be more economical for a single component to manage all cyberattack spending, he added.

"Maybe it's time to give Cyber Command more budget authority," Harrison said.

Other military experts said the services might be giving away these details to ward off potential foes on the Internet.

"For some time now, U.S. Cyber Command has advertised it is prepared to conduct full spectrum cyber operations," which include attacking adversary networks, said retired Air Force Maj. Gen. Charles Dunlap, a former deputy judge advocate general.

Dunlap, now executive director of Duke University's Center on Law, Ethics and National Security, added, "It is pretty clear that the U.S. intends to convey the message that it is prepared to fight in cyberspace with cyber weapons."

As for signaling the Air Force's cyber might with money, Badger said, "Operating with assurance in the cyber domain is a national security imperative," but "rest assured, the cyber activities of the Department of Defense are always undertaken in accordance with existing policy and law and executed under specific authority."

Harrison quipped, "It's probably more of a signaling to Congress."

Table of Contents

## Military Photographers Ready to Deploy Around the Globe

From FAS.org, 24 April 2013

Just as law enforcement relied upon surveillance cameras and personal photography to enable the prompt identification of the perpetrators of the Boston Marathon bombing, U.S. armed forces increasingly look to the collection of still and motion imagery to support military operations.

Combat camera (COMCAM) capabilities support "operational planning, public affairs, information operations, mission assessment, forensic, legal, intelligence and other requirements during crises, contingencies, and exercises around the globe," according to newly updated military doctrine.

COMCAM personnel are "highly trained visual information professionals prepared to deploy to the most austere operational environments at a moment's notice."

COMCAM units "are adaptive and provide fully qualified and equipped personnel to support sustained day or night operations" in-flight, on the ground or undersea, as needed.

"Effectively employed COMCAM assets at the tactical level can potentially achieve national, theater strategic, and operational level objectives in a manner that lessens the requirement for combat in many situations," the new doctrine says. "Their products can counter adversary misinformation, disinformation, and propaganda and help commanders gain situational awareness on operations in a way written or verbal reports cannot."

"The products can also provide historical documentation, public information, or an evidentiary foundation… for forensic documentation of evidence and legal proceedings. They can provide intelligence documentation to include imagery for facial recognition and key leader engagements, and support special reconnaissance."

The newly issued COMCAM doctrine supersedes previous guidance from 2007. See Combat Camera: Multi-Service Tactics, Techniques, and Procedures for Combat Camera (COMCAM) Operations, April 2013.

Table of Contents

## Air Force Academy Wins NSA Cyber Defense Title

By Kirsten Bennett, KOAA News, Apr 24, 2013

U.S. AIR FORCE ACADEMY, Colo., - The Air Force Academy has won the National Security Agency's Cyber Defense Exercise for the second year in a row, outscoring teams from other military academies in the U.S. and Canada.

The CDX is a large-scale computer network defense competition to see which team of students can design, implement, and maintain a fully functioning computer network that is attacked by Air Force and NSA "Red Teams." The cyber exercise has been recognized nation-wide for the realistic and valuable training it provides our participants on the cyberspace battlefield.

Cadets in the Computer Sciences 468 Secure Networks course and members of the USAFA Cyber Competition Team competed in the 13th annual inter-service Cyber Defense Exercise, April 16-18. This NSA-run competition required the cadets to build an enterprise network from scratch, including email, web, VOIP and file transfer services. During the exercise, cadets defended the network against NSA red-team members, solved a forensics challenge, and secured a vulnerable bookstore webserver.

"Our second consecutive victory in the Cyber Defense Exercise is a result of the incredible dedication and hard work of our cadets," said Dr. Carlisle. "They understand the critical role cyber plays in our nation's defense, and are proactively learning as much as they can so they will be outstanding leaders in this domain," said Dr. Martin Carlisle, who coached the cyber team, taught the Network Security Class and is director of the Academy Center for Cyberspace Research.

The entire exercise was conducted on virtual, private networks, providing a safe path for the exercise while preventing interference with real-world networks.

Cadet 1st Class Michael Winstead led the USAFA effort, supported by Cadets 1st Class Frank Adkins, Matt Bailey, Ismael Barragan, Jon Beabout, Alex Beveridge, Andre Brito, Josh Christman, Rob Guiler, Nathan Hart, Matt Howard, Peter Jackson, Luke Jones, Kris Kalau, Josiah Lane, Brandon Leet, Matt Melhado, Carl Morgan, Gage Parrott, Ben Payne, Chris Probasco, Ken Sample, James Simons, Brennan Sweeney, Katie Tiedemann, Elliott Unseth, Ramon Villanueva, Taylor Watson, Zach Zeitlin, Cadets 2nd Class Chase King, Keane Lucas, Chad Speer, Ryan Zacher, Cadets 3rd Class Kevin Cooper, Bill Parks, Evan Richter and Clay West. The team was coached by Dr. Carlisle, with assistance from Majors David Merritt, Michael Chiaramonte and David Caswell, 2nd Lt. Jacob Blasbalg and Mr. Sean Harris.

The USAFA team will be awarded the NSA Director's Trophy for Information Assurance at a future date.

That trophy has made its rounds through most of the service academies, with the Air Force Academy earning it in 2012. Previous winners were the Naval Academy in 2005 and 2010, the Merchant Marine Academy in 2004, the Air Force Academy in 2003, 2006 and 2012, and U.S. Military Academy in 2001, 2002, 2007-2009 and 2011.

Table of Contents

## How People in the Middle East Actually Use Social Media

By Everette E. Dennis, Justin D. Martin and Robb Wood, the Atlantic, 24 April 2013

DOHA, Qatar--Since the suicide of an underfoot fruit vendor in Tunisia, the Arab world has generated some of the world's most-followed stories. History will find the news coming out of Arab countries during this time both gripping and plentiful.

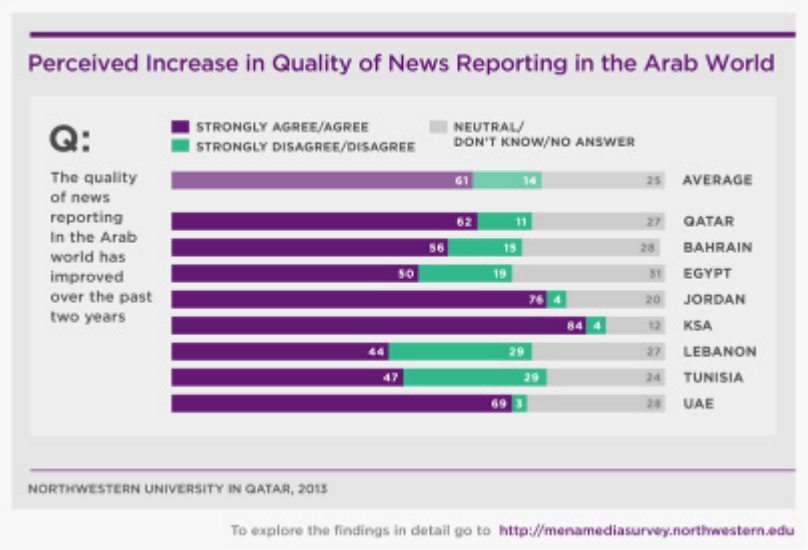
Less is known, however, of the news and information *reaching* Arab countries and communities during this period, and at times much has been speculated of, say, Twitter reliance in Tunisia, satellite TV dependence in Egypt, or tablet use in the highly connected Arab Gulf.

To more rigorously study how people in the Arab world access news and information, rate the credibility of information sources, and use social media, Northwestern University in Qatar commissioned a survey among people in eight Arab countries: Egypt, Tunisia, Bahrain, Qatar, Lebanon, Saudi Arabia, Jordan and the UAE.

Harris Interactive conducted a mix of face-to-face and telephone interviews with 9,693 adults aged 18 and older. Participants were asked a wide range of questions on media--from matters of newspaper use, book reading and blogging to online banking and gaming--with a heavy emphasis on Internet use. Participants were interviewed in late 2012 and early 2013. Northwestern University in Qatar built an **interactive site** to make the data available to the public.

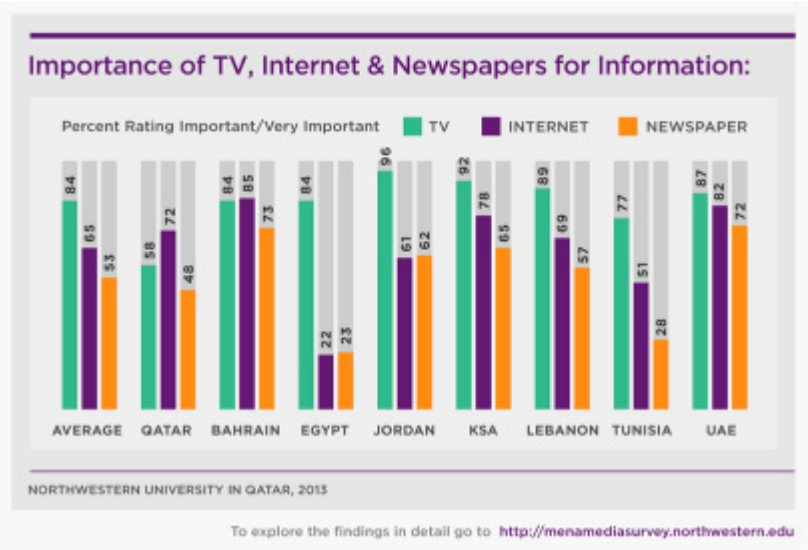
***

People love to lament the quality of journalism, but most respondents in the survey believe things have been changing for the better. Respondents in the Northwestern survey, for example, were asked whether the quality of news reporting in the Arab world had improved over the previous two years, and feedback was overwhelmingly positive. Participants are far more likely to agree than disagree that reporting has improved, by ratios of more than 19 to 1 in Jordan and 21 to 1 in Saudi Arabia.

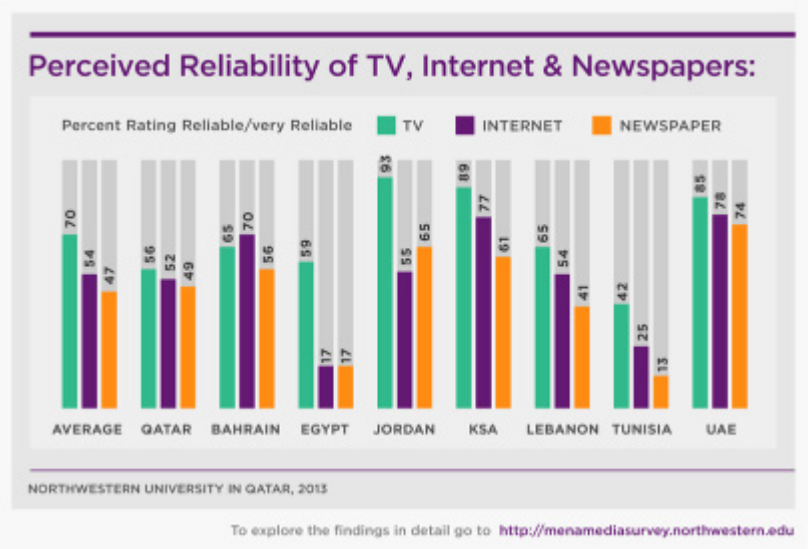


Tunisia and Egypt, which overthrew censorial regimes in 2011, are nonetheless far less impressed. Lebanon, home to one of the freest press systems in the Arab world, was also less moved by journalists' record over the past two years.

Television remains the most important source of news and information in all countries, except Bahrain and Qatar. Qatar has at least 2.3 million cell phones in a country of around 2 million people, according to the CIA World Factbook, which may help explain the country inching away from television. Incidentally, Qatar also reported the highest level of tablet ownership, 34 percent, of any country surveyed. Internet reliance is lowest in Egypt, which is consistent with past research on both Internet penetration and illiteracy in that country.




While respondents across the Arab world are pleased with journalistic progress in their region over the past two years, they demur somewhat when asked to rate the reliability of news they receive from TV, in newspapers, online and on radio.




Among respondents from the revolution-emergent countries, Egypt and Tunisia, the outlook is bleak for all media but television (which still comes out bruised). Qataris, Bahrainis and Lebanese are slightly more confident in TV, newspapers, and the Internet. Respondents in the UAE, host to a broad range of regional outlets and western enterprises, such as CNBC, BBC, Rolling Stone, Google, and Forbes, find all media sources reliable. Local newspapers in the UAE tend to receive high reliability ratings; papers in the country are all government-owned, and respondents still rate broadsheets favorably.

Asked more generally whether media in their countries are credible, majorities in five countries--Jordan, Saudi Arabia, Qatar, the UAE, and Bahrain--affirmed.

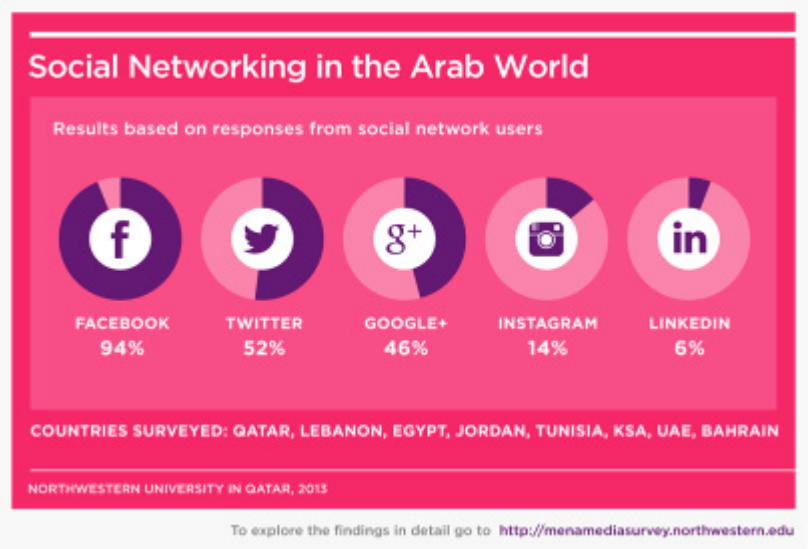
***

The notion that the influence of social media in Arab political change has been overstated during the Arab uprisings has itself been repeated so often it's nearly cliché. Nevertheless, social media are forceful channels in Arab countries.

Participants in the Northwestern survey spend an average of 3.2 hours a day on social networks. Tunisian and Bahraini Internet users are the most voracious social networkers, each devoting 4.1 hours daily. (Bahrain, it should be said, had the highest overall media consumption; more respondents in Bahrain read books, newspapers, magazines, and listen to radio than any other Arab country surveyed).

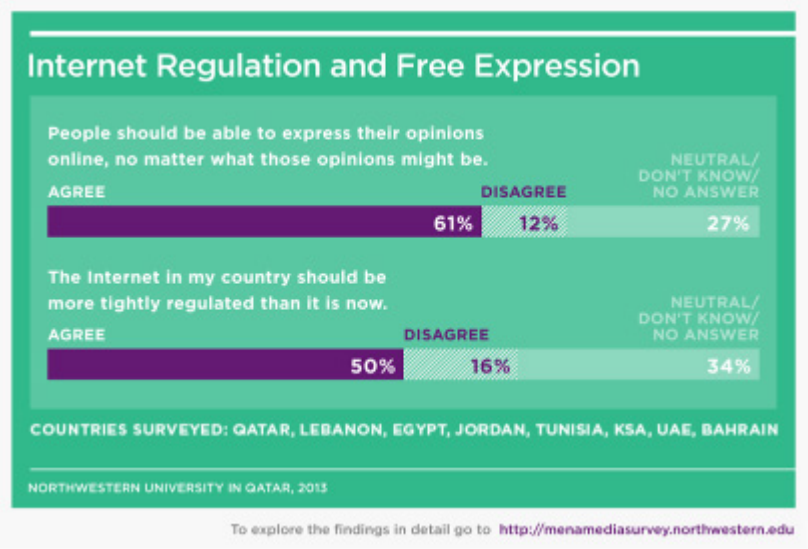
More than 90 percent of Internet users in all countries use social networking sites, except Qatar and Egypt, at 74 and 86 percent, respectively. Qatar's relative coolness toward social media is perhaps surprising, as the country was second in general Internet use only to the UAE, and has the largest percentage (79) of wireless handheld users.

Qatar, though, has the smallest national population by far of any country surveyed--less than half the size of the next largest country by citizenry, Bahrain. Qatari nationals in the survey listed interpersonal contacts--friends, family, colleagues--as more important sources of news and current events than the Internet. Region-wide, interpersonal contact was second only to television as a source of news and current events.




Facebook is by far the most popular social network in Arab countries surveyed, with 94 percent of social network users active on the network. More than half of social network users in the sample are active on Twitter, 46 percent employ Google+, and around one in seven use Instagram. Just 6 percent of social networkers use LinkedIn--intuitive perhaps, given professional introductions are still often fueled by tea and handshakes in Arab countries.

Attitudes toward freedom of speech online are mixed, with the overall majority of participants clearly favoring online freedom of expression.




When the data are examined by nation, majorities in seven countries believe people should be able to express their opinions online, even if those views are potentially incendiary, and a hefty plurality of Egyptians also agreed. Three-fourths of participants in Saudi Arabia, a Wahabbist-leaning country, voiced support for free speech online.

Asked whether their countries should more tightly regulate the Internet, however, participants showed less libertarian sentiment. Majorities or pluralities in every Arab country surveyed support greater control of the web, even more so, oddly, in countries most supportive of online freedom of speech. Survey participants seem to be saying, then, that while it's okay for webizens to say what they wish, there's considerable support for government surveillance of the Internet in respondents' own countries and communities.

Northwestern University in Qatar's survey of Arab media use didn't include a few of the most politically and militarily charged countries in the region, such as Syria, Libya, and Palestine.

Nonetheless, the survey represents one of the most comprehensive multi-country studies of media use in the Arab world available in the public domain. And though Arab media habits examined in the survey are only narrowly reported here, those wishing to drill further down into the data can summon, say, figures on women blogging in Lebanon, Twitter use in Egypt versus Tunisia, or the most popular TV news channels in Saudi Arabia on a site available to the public.

Table of Contents

## New Electronic Warfare Tool Offers Innovative Approach

By U.S. Army Research Laboratory Public Affairs, April 11, 2013

WHITE SANDS MISSILE RANGE, N.M. -- Army electronic warfare teams recently developed a powerful new tool to investigate survivability, lethality and vulnerability in Defense Department systems.

Scientists from the U.S. Army Research, Development and Engineering Command's research laboratory came up with the Optimized Modular EW Network, or OMEN.

By controlling waveforms, power, timing and digital signal processing capabilities, the teams accurately replicate the electromagnetic environment in which DoD systems must operate.

"In the current environment, with advancements in technology, telecommunications and electronics, we cannot build single-point solutions to test or analyze systems," said Shane Cunico, Experimental Support Branch chief at White Sands Missile Range. "The technology that we are trying to counter is moving so fast that we cannot play catch-up."

OMEN represents a paradigm shift away from developing single-point solutions towards creating flexible, upgradable systems. This approach allows systems to be easily adapted for use across a variety of tests and experiments.

The device is made up from a waveform generator and an amplifier, which together occupy roughly two cubic feet, making the system highly portable.

The system is reprogrammable. One moment it can generate a waveform that replicates a complex radar system, then it switches to emitting a waveform that can jam a radio.

Multiple OMEN systems can be linked in the field or hardwired into a lab test or anechoic chamber to produce a highly controllable, dynamic and complex EW environment.

In developing OMEN, The U.S. Army Research Laboratory's Survivability and Lethality Analysis Directorate adopted what officials called, "a better, faster and easier" approach, which resulted in a modular design that is highly adaptable.

Its systems and subsystems operate within an open-architecture format: all subsystems are independently upgradable and have associated interface control documentation to allow for future modification and growth.

Because the OMEN's computer and receiver can be upgraded individually -- a key first -- OMEN's functionality can continually increase, which ensures that it will be capable of replicating the electromagnetic environment of the battlefield of tomorrow.

In contrast, the typical approach to building an EW-test system has been to identify the functions required to execute a specific test and then design a system with the sole purpose of performing identified functions.

This approach resulted in single-point-solution systems that, although highly effective within a specific test, lacked flexibility, breadth of utility and efficiency.

For most systems, adding additional functions requires significant modifications or a redesign--if the system is even capable of such adaptation.

Designing a multifunction-solution system requires a high investment of resources and time, so subsystems are independently upgradable. But the result, officials said, is a flexible and easily adaptable system that, while complex in its development, is necessary for operating in the rapidly changing threat environment.

As one of the first multifunction solutions at ARL, OMEN exemplifies an advanced approach to system design. Developed upon ARL/SLAD's unrivaled expertise and experience in EW SLV analysis, OMEN's modular design and open-architecture format ensure that it will remain a fundamental resource for ARL's EW capability in the future. "We have to have adaptability and be agile enough to develop modular, upgradable systems," Cunico said. "If we don't, we will always be behind the power curve and chasing the adversary who will always have the upper hand."

Table of Contents

## Jihadi Twitter activism – Introduction

By Nico Prucha, Jihadica, 27th April 2013

Ali Fisher and I have recently exchanged thoughts and data regarding the increasing Jihadi use of Twitter. By taking an interdisciplinary approach of social-media analysis and cluster network assessment, we decided to start a series on Jihadica on the parts of the overall jihadi, primarily Arabic language propaganda resonating among the audiences online. We plan on delivering updates on the subject as we move along and kick-off the series with an overall introduction to the theme.

In future posts in the series, we will highlight and decipher some of the core content most often shared on Twitter, allowing conclusions to be drawn about the parts of jihadist propaganda which resonate with a wider audience (and hence shared over and over again).

**Introducing the theme**

The recent essay by Abu Sa'd al-'Amili on the state of global online jihad (discussed here) lamented a general decline in participation in jihadi online forums. Furthermore, al-'Amili issued a "Call (nida') to the Soldiers of the Jihadi Media" demanding that they "return to their frontiers (thughur)" elevating their status. Al-'Amili himself is one of the high-profile clerics, a "prolific "Internet Shaykh" (Lia) on the forums, but is also quite active on twitter (@al3aamili).

Two interrelated causes identified by Abu Sa'd al-'Amili were the periods when forums were offline and the migration of users to social networking sites such as Twitter and Facebook. This is exacerbated by the movement of "major [jihadi] writers and analysts" (kibar al-kuttab wa-l-muhallilin) from the forums to social media platforms. This has perhaps increased the momentum of members of tier-one jihad forums to expand onto twitter while twitter as a massive communication relay has become the basis for a new generation of sympathizers, posing another intersection. Twitter is a further medium of choice to (re-) disseminate propaganda material in general and is a platform where activists, sympathizers, and actual fighters upload audiovisual and other types into the jihadi hub.

Jihadists have aggressively expanded the use of twitter, in addition to Facebook and YouTube, especially since the outbreak of violence in Syria. During 2011 members of Jihadist forums issued media-strategies and advisory to fellow members prior, as for example is stated in this posting here of the al-Ansar forum. The posting, initiated by the member Istishhadiyya is basically a very elemental guide, comprehensive and for beginners, highlighting the effective and fast communication capability. The same posting was copy-and-pasted by Shumukh member Basha'ir shortly afterwards. A handbook, compiled by Twitter user @osamh ended up on the jihadi forums to further underline the importance of Twitter as well as its difference to Facebook, where jihadists already have a strong presence.

It took a while for jihadi activism to fully unravel on Twitter, and they have maintained a cohesive as well as detailed presence on this social media platform since the Syrian conflict turned violent in 2012.

Twitter, and as such social media in general, is in the meantime an integral part of jihadists' media endeavors on the Internet, with the majority of jihadi forums having their official account advertised for on the main pages of the forums.

The role of the media activists, or in jihadist speak the "media mujahid" has since the death of Osama bin Laden in May of 2011 been promoted, highlighted and approved. AQ related documents have made this role model prominent. The role model of the "media martyr" any "media mujahid" can be become, is backed by the call to take the fight on a greater level on al channels online issued by al-Fajr in their response of the killing of bin Laden:

"The Internet is a battlefield for jihad, a place for missionary work, a field of confronting the enemies of God. It is upon any individual to consider himself as a media-mujahid, dedicating himself, his wealth and his time for God." (Analysis here, Arabic original here)

At first, the strategies to promote Twitter among members of jihadi forums failed to develop substantial traction, but this changed drastically during 2012. When jihadists in and outside of Syria started to use and incorporate twitter as a medium to disseminate and re-post al-Qa'ida and other propaganda material.

**Twitter activism and jihadi supporters**

At first Syrian non-violent activists used, and continue to use, twitter as a medium to document human rights abuse and war crimes of the Assad regime, but jihadists quickly adapted that content and the platform for their propaganda.

Social-media smart and professional jihadists adopted this treasure grove for their propaganda. By rebranding and reframing the content created by civil society activists, jihadi propaganda used these grievances to support a key jihadist self-perception; the obligation to respond by force to defend and protect the Sunnites in Syria.

Due to the effect and success of the Syrian based Jihadi groups, other jihadi groups as well as the main forums are adopting the twitter activism, advertising official forum accounts on the main pages with users within the forums using twitter hashtags (#) or references to twitter users (for example: @al_nukhba). A list of "The most important jihadi and support sites for jihad and the mujahideen on Twitter'" was recently posted on the Shumukh al-Islam forum, allowing users to identify key accounts they might wish to follow.

Individual sympathizers and all those feeling inclined to contribute to the media jihad re-disseminate authoritative files of al-Qa'ida on twitter on a larger scale. Now all major jihadi media departments, part of militant networks, have their own channels on Twitter, linking to content from the jihadi forums and other social media platforms, primarily YouTube, Facebook, and pictures in general.

Twitter has turned into a primary hub for the distribution of jihadi agitprop files. These Jihadi information sharing networks using Twitter coexist, autonomously, with the classical forums. These networks carry, for example, samples of the wide range of jihadi propaganda files, in some cases placed first on Twitter, posted via mobile phones from the front lines. As a brief overview, a few samples consisting of:

- martyrs in general and martyrdom operatives (istishhadiyyun) announced and identified by their hashtag and Twitter account;
- calls for donations with phone numbers and social media contact information; taking care of the orphans of the martyrs among other civil elements;
- general material of incitement, and the impact of online attained propaganda files used offline are popular and gain plenty of traction,

**What are they sharing?**

In addition to disseminating their own propaganda, jihadi media activists repurpose content from social movements and non-jihadi groups for their own purposes, framing the non-jihadi actions or demonstrations as

part of the global militant struggle. This has created another 'grey area' where analysts have to carefully monitor and decipher such content. The forum administrators and media-activists also are starting to incorporate and misuse Twitter for their purposes, in coordinated attempts to virtually infiltrate legitimate social movements by using the same hash tags and a similar rhetoric to create ideological cohesion – and placing extremist views and files in that virtual sphere while claiming to fight on the ground for the sake of the people.

To analyze jihadi media networks, their sympathizers and followers we have used a combined approach focused on a unique interdisciplinary analysis of the data acquired by technical means and the subsequent and immediate analytical process of its content.

Using these methods we have asked a range of questions, how have jihadi propagandists been able to gain traction and a foothold online? How do they disseminate propaganda content to a global, multilingual audience and what resonates most with that audience? What are the networks through which their content flows and what are the different roles users play within these networks? Ultimately do the different jihadi twitter accounts reach a range of different communities, or is it a small densely interconnected echo chamber?

Table of Contents

## SPAWAR Leadership on Information Warfare and the Growing Cyber Threat

By Tina Stillions, DVIDS, 25 April 2013

SAN DIEGO - "Information Dominance will become a recognized warfare area on par with other traditional warfare areas and is becoming one of our most powerful assets," said Space and Naval Warfare Systems Command (SPAWAR) Chief Engineer Rear Adm. James Rodman during a panel discussion on information and non-kinetic warfare and the growing cyber security threat.

"We need to look at the warfare arena differently," said Rodman. "We need to know what arrows we have in our quiver and then define those non-kinetic elements so that we can treat them in a more level set environment."

SPAWAR Commander Rear Adm. Patrick Brady echoed Rodman during his follow on keynote address discussing the importance of technical authority in information warfare during the 35th Annual C4ISR Symposium April 23-25 in San Diego.

"The value of a unified technical authority is that it helps us identify security gaps in our networks," said Brady. "It creates better situational awareness, more resilient information technology (IT) architectures and standardized platforms so that we can gain a better understanding of the impact of cyber vulnerabilities on our critical warfighting systems."

To support this cyber imperative and achieve power in an information warfare arena, a greater level of information sharing will be required.

As in the civilian world, the Navy continues to operate in a highly interactive environment regarding global networks, interconnected applications and services. To help combat the emerging cyber threat, the Department of the Navy routinely interacts with the other services, government agencies, allied and coalition partners, commercial organizations and universities to combat the security challenges faced in the world of networks, the cloud and cyberspace.

This is cyber warfare in the information age, a form of non-kinetic warfare on a virtual global battlefield that will change warfare as we know it. It is low-intensity warfare that is often systemic in nature, such as a hacker setting loose a virus on a network system. Though it may not cause an immediate and direct impact to loss of life, it can still wreak havoc on the lives of individuals and organizations that encounter it, including the Department of Defense (DOD).

SPAWAR Systems Center Pacific Commanding Officer, Capt. Joseph Beel reiterated by stating that warfighting is about effects.

"Whether there is a kinetic or non-kinetic effect to achieve, in the long run it is cheaper, less risky and better to use a non-kinetic effect," said Beel. "Information warfare is really where you bring in the potential for non-kinetic effects."

That kind of non-kinetic impact makes information warfare the ideal warfighting arena.

"When the United States went into Iraq in the 90s, if we wanted to take down the enemy's air traffic control and defense systems, we could bomb them, which we did very effectively," said Beel. "The difference today is that everything is so networked. With Information Warfare, the capability may exist to take them down by

introducing a virus into some sort of cyber attack scenario, without risking bombers or sending people ashore for battle."

The DOD makes more than one billion Internet connections daily and passes 40 terabytes of data. DOD networks are scanned and probed by cyber adversaries on average six million times per day, so identifying weak links and potential attacks can be a challenge. Many lessons have been learned over the years about the value of information sharing.

According to Rodman, had DOD been able to connect the dots more quickly prior to 9/11, some of the events might have been prevented.

"There is a tremendous need to make the availability of information seamless so that the warfighter can access it more quickly," said Rodman. "To achieve that level of power, we need to find a better way of sharing information."

The rapid elasticity of the cloud makes it a seductive choice; however, there is the potential for loss of privacy and an increased risk to security should information get into the wrong hands. Whereas in the past a threat was isolated to a single server system, a cloud-based environment makes it easier to compromise everyone, and all types of data hosted at a particular location are vulnerable on the back end of a breach.

The Navy frequently adapts commercial software for operational purposes; however, in doing so there is the potential for hackers to compromise systems, which could then threaten national security. Better training and certification of Navy IT systems and operators through a technically rigorour process is vital to combating that kind of threat, according to Brady.

"Technical authority's focus on standardization and variance reduction makes it easier to certify systems and reduce the training burden on operators so they can focus on cyber warfighting," said Brady. "SPAWAR's technical authority initiative is instrumental to the Navy's cyber posture and to our warfighting effectiveness in a non-kinetic environment. It puts SPAWAR in the lead to develop architectures and systems with built in defense in depth attributes."

Though it can be challenging to identify or classify the typical cyber threat, most run the gamut from non-professional to nation-state sponsored hackers; sometimes it is an internal threat of lax security choices on the part of the IT user. Whether malicious or unintentional, the threat is never static and the complexity of today's systems and networks presents significant security challenges for the Navy's producers and consumers of IT.

"We have to look at information like we did with aviation when it first started in the twenties. If you look at how naval aviation evolved, we are in the stand up phase right now with regard to Information Dominance and information warfare," said Rodman. "Because it's still in its infancy, we have to examine it and determine how we will mature the warfare area. In some cases, we will see that we may be able to use information to destroy our adversary's capabilities so that we never get to the kinetic part of warfare."

Despite doubt about the potential for a digital Pearl Harbor, the threats are real and the potential for destruction great. The nation's virtual and physical infrastructures fall under the national security umbrella and will require greater cooperation between industry and government to fight the growing cyber menace in the information warfare arena. Whether a virtual Sea Treaty is necessary or possible will depend largely upon the cooperation of a yet undefined population of information owners and those users who give up their privacy information freely in a virtual world. How that information is protected and defended will continue to evolve and will keep SPAWAR on the leading edge.

As the Navy's Information Dominance systems command, SPAWAR designs, develops and deploys advanced communications and information capabilities for the warfighter. With more than 8,900 acquisition professionals located around the world and close to the fleet, the organization is at the forefront of research, engineering and support services that provide vital decision superiority for the warfighter.

Table of Contents

## Pentagon Paying China — Yes, China — To Carry Data

By Noah Shachtman, Wired, 04.29.13

The Pentagon is so starved for bandwidth that it's paying a Chinese satellite firm to help it communicate and share data.

U.S. troops operating on the African continent are now using the recently-launched Apstar-7 satellite to keep in touch and share information. And the $10 million, one-year deal lease — publicly unveiled late last week during an ordinarily-sleepy Capitol Hill subcommittee hearing — has put American politicians and policy-makers in bit of a bind. Over the last several years, the U.S. government has publicly and loudly expressed its

concern that too much sensitive American data passes through Chinese electronics — and that those electronics could be sieves for Beijing's intelligence services. But the Pentagon says it has no other choice than to use the Chinese satellite. The need for bandwidth is that great, and no other satellite firm provides the continent-wide coverage that the military requires.

"That bandwidth was available only on a Chinese satellite," Deputy Assistant Secretary of Defense for Space Policy Doug Loverro told a House Armed Services Committee panel, in remarks first reported by InsideDefense.com. "We recognize that there is concerns across the community on the usage of Chinese satellites to support our warfighter. And yet, we also recognize that our warfighters need support, and sometimes we must go to the only place that we can get it from."

The Apstar-7 is owned and operated by a subsidiary of the state-controlled China Satellite Communication Company, which counts the son of former Chinese premier Wen Jiabao as its chairman. But the Pentagon insists that any data passed through the Apstar-7 is protected from any potential eavesdropping by Beijing. The satellite uplinks and downlinks are encrypted, and unspecified "additional transmission security" procedures cover the data in transit, according to Lt. Col. Damien Pickart, a Defense Department spokesperson.

"We reviewed all the security concerns, all of the business concerns with such a lease," Loverro said. "And so from that perspective, I'm very pleased with what we did. And yet, I think the larger issue is we don't have a clear policy laid out on how do we assess whether or not we want to do this as a department, as opposed to just a response to a need."

Every new drone feed and every new soldier with a satellite radio creates more appetite for bandwidth — an appetite the military can't hope to fill with military spacecraft alone. To try to keep up, the Pentagon has leased bandwidth from commercial carriers for more than a decade. And the next decade should bring even more commercial deals; in March, the Army announced it was looking for new satellite firms to help troops in Afghanistan communicate. According to a 2008 Intelligence Science Board study (.pdf) — one of the few public reports on the subject — demand for satellite communications could grow from about 30 gigabits per second to 80 gigabits a decade from now.

The Chinese are poised to help fill that need — especially over Africa, where Beijing has deep business and strategic interests. In 2012, China for the first time launched more rockets into space than the U.S. – including the Chinasat 12 and Apstar-7 communications satellites.

Relying on Chinese companies could be a problematic solution to the bandwidth crunch, however. U.S. officials have in recent years publicly accused Chinese telecommunications firms of being, in effect, subcontractors of Beijing's spies. Under pressure from the Obama administration and Congress, the Chinese company Huawei was rebuffed in its attempts to purchase network infrastructure manufacturer 3Com; in 2010, Sprint dropped China's ZTE from a major U.S. telecommunications infrastructure contract after similar prodding. Last September, executives from the Huawei and ZTE were brought before the House intelligence committee and told, in effect, to prove that they weren't passing data back to Beijing. "There's concern because the Chinese government can use these companies and use their technology to get information," Rep. Dutch Ruppersberger, said at the time. The executives pushed back against the charges, and no definitive links to espionage operations were uncovered. But the suspicion remains. And it isn't contained to these two firms.

"I'm startled," says Dean Cheng, a research fellow and veteran China-watcher at the Heritage Foundation. "Is this risky? Well, since the satellite was openly contracted, they [the Chinese] know who is using which transponders. And I suspect they're making a copy of all of it."

Even if the data passing over the Apstar-7 is encrypted, the coded traffic could be used to give Chinese cryptanalysts valuable clues about how the American military obfuscates its information. "This is giving it to them in a nice, neat little package. I think there is a potential security concern."

For his part, Loverro says the Department of Defense will be reviewing its procedures to ensure that future satellite communications deals both let troops talk and let them talk in private. The Pentagon will get another opportunity shortly: the Apstar-7 deal is up on May 14, and can be renewed for up to three more years.

Table of Contents