Information Operations Newsletter

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

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

ARSTRAT IO Newsletter Online

Table of Contents

Vol. 13, no. 09 (July-August 2013)

British Cops Admit They Monitor Facebook, Twitter

By Paul Wagenseil, TechNewsDaily, June 27 2013

Users of social media are constantly warned to watch what they reveal online. You never know who might read your postings, the argument goes — your grandmother, your boss, potential employers.

To that list of potential readers, you'll have to add the police, at least if you live in Britain.

Wired UK reports that London's Metropolitan Police, or Scotland Yard in popular parlance, has admitted the existence of a team dedicated to monitoring the social media postings of some 9,000 people for signs of political unrest.

The unit has 17 officers and uses what it calls Social Media Intelligence, or SocMint, to scan Facebook, Twitter, YouTube and other social media services 24 hours a day, Wired UK said, adding that the team is developing special tools to smooth the process.

As part of the Metropolitan Police, the unit has jurisdiction in all of England and Wales, and some jurisdiction in the legally distinct "countries" of Scotland and Northern Ireland.

At a security conference in Australia last month, a Scotland Yard official, Umut Ertogral, spoke freely during what he thought was a closed-door meeting.

Social media "almost acts like CCTV [closed-circuit television] on the ground for us, really," Ertogral said, according to the Australian Financial Review.

Etrogral is head of open-source intelligence at Scotland Yard's National Domestic Extremism Unit (NDEU), which means that his team mines publicly available information for home-grown British terrorists, fringe groups and politically motivated troublemakers.

Through a freedom-of-information request, the Guardian learned that the NDEU currently keeps track of at least 8,931 Britons suspected of being "domestic extremists."

"When there's a protest, people go out and record video, and we know two minutes later they'll be on YouTube," Etrogral reportedly said at the Australian conference. "And because people on the Internet are very silly, they'll say 'That's my mate Joe Bloggs.'"

A spokesman for the Metropolitan Police confirmed the existence of the social-media unit to Wired UK, adding that it was necessary to "uphold the law and prevent and detect crime."

Some American police do the same thing, though perhaps less systematically. The New York City police department monitors the Facebook pages and Twitter postings of suspected gang members and juvenile petty criminals in case something incriminating gets posted — and it often does.

All of this is perfectly legal. It's using only data that people have already made public. In a way, it's no different from Googling the name of someone you've just met.

Not everyone, however, sees it that way.

"The perception with this kind of intelligence is that it's in the public domain, so it's no different from, say, searching through newspaper articles," Daniel Trottier, a researcher at the University of Westminster in London, told Wired UK.

"But this analysis shows a lack of familiarity with the technology involved," Trottier added. "With just a few statements from social media profiles, one is able to reasonably determine a user's sexual orientation," among other possibly private details.

Once again, the adage comes up — if you don't want your grandmother to see it, you don't want the police to see it either.

Table of Contents

Hacking for Change – Could Revealing Cyber Capabilities Prevent Cyber War?

By Chandler Harris, Clearance Jobs, June 26, 2013

Revealing the capabilities of the U.S. nuclear arsenal is a key part of the U.S. nuclear deterrence strategy. So when it comes to the U.S. cyber warfare capabilities, the same tactic could be used to deter cyber war, claims a new paper by the Rand Corporation. Offisive cyber operations may be a legitimate deterrence strategy.

The paper, Brandishing Cyberattack Capabilities, was prepared for the Office of the Secretary of Defense, and seeks to identify if demonstrations, or “brandishing” cyberwar capabilities, serve as effective deterrents to a potential cyber war. The paper says that brandishing cyberattack capabilities would accomplish three things: declare a capability, suggest the possibility of its use in a particular circumstance, and indicate that such use would really hurt.

“The most obvious way to demonstrate the ability to hack into an enemy’s system is to actually do it, leave a calling card, and hope it is passed forward to national decision-makers,” the report says. “This should force the target to recalculate its correlation of forces against the attacker.”

“Advertising” cyberwar capabilities may be helpful as a backup a deterrence strategy by dissuading other countries from performing harmful activities. Plus, it could limit a country’s confidence in the reliability of its information, command and control, or weapon systems, the paper says.

However, providing effective cyber warfare capabilities isn’t easy since they are relative to a specific target, which must be fully understood. Even if cyber warriors can reveal the capability of penetrating systems, this is not the same as getting the systems to fail.

Having a successful cyber deterent strategy will take considerable analysis and imagination, since there is not one clear way to suggest the cyber war capabilities of the U.S., the report admits.

“(Brandishing cyberwarfare capabilities) is no panacea, and it is unlikely to make a deterrence posture succeed if the other elements of deterrence (e.g., the will to wage war or, for red lines drawn in cyberspace, the ability to attribute) are weak,” the report says.

[RAND document found at http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf}

Table of Contents

Anonymous vs. Los Zetas: The Revenge of the Hacktivists

By Paul Rexton Kan, Small Wars Journal, Jun 27, 2013

See below for author's note.[1]

The cyber war between Anonymous and Los Zetas has reignited, with some new twists. The initial skirmish occurred in the fall of 2011. In the introduction of my article, “Cyberwar in the Underworld: Anonymous vs. Los Zetas in Mexico” that appeared in the Yale Journal of International Affairs, I provided the following account of the clash:

> Los Zetas, a Mexican drug trafficking organization composed of former members of Mexico’s Special Forces, kidnapped a member of Anonymous, the global hacking group, in Veracruz on October 6th. In retaliation, Anonymous threatened to publicize online the personal information of Los Zetas and their associates, from taxi drivers to high-ranking politicians, unless Los Zetas freed their abductee by November 5th. The release of this information on the Internet would have exposed members of Los Zetas to not only possible arrest by Mexican authorities, but also to assassination by rival cartels. Unconfirmed reports suggest that Los Zetas then attempted to “reverse hack” Anonymous to uncover some of its members and to threaten them with death. As a consequence, a few members of Anonymous sought to call off the operation and disavowed those members who wanted to go forward. With time running out and locked in a stalemate, Los Zetas released their kidnap victim on November 4th with an online warning that they would kill ten innocent people for each name that Anonymous might subsequently publicize. Anonymous called off its operation; each side appeared to step back from the brink.[2]

With the new Anonymous group focusing on the activities of Los Zetas in the small city of Acuña, Coahuila, the hacktivist collective is returning to the brink. The new clash between the two groups began only recently, with Anonymous striking first. In April, four college graduates from Acuña returned to their hometown to find it completely under control of Los Zetas. In response, they decided to form an Anonymous affiliate. According to a spokesperson for the group, “We were not here in 2005 when the Zetas arrived in Acuña. We were already gone to college, but every time we returned to visit, we would see and hear how quickly the situation was worsening in our town”.[3] The group’s goal is to expose the Zetas' activities in the city and the gang's alleged ties to Mexico’s current governing party, Partido Revolucionario Institucional (PRI).[4] The group has branded itself as “Anonymous FreeAcuña” and began publishing photos of homes and businesses it says belong to cartel operatives on its blog, Facebook and Twitter.

Unlike the first clash, there are some notable differences. First, there appears to be no predicate event like the kidnapping of an Anonymous member. Instead, some young people returned to their hometown of Acuña and saw that Los Zetas had tightened their grip on it. Second, along with a video announcement from a masked Anonymous spokesperson declaring the operation, a blog and Twitter account linked to Anonymous FreeAcuña appeared suddenly. Members appeared to spread the word and recruit online in various forums.

In fact, in the comment section of the online version of myYale Journal of International Affairs article, someone claiming to be a part of Anonymous FreeAcuña left the following message on May 11:

> We are an ANONYMOUS cell group in Acuña, Coahuila Mexico, border city with Del Rio, Texas. We are in the middle of cyber warfare with the ZETAS and already tangling with the Gulf Cartel: freeacuna.blogspot.com is a diary of what we are doing. It is a bilingual blog that explains step by step who we are and what we do.
>
> Anonymous FREEACUNA[5]

The third notable difference is the presence of the blog itself and the publishing of information about Los Zetas operations in and around the town of Acuna. The initial clash did not feature a blog that was maintained by Anonymous. Rather, information about Los Zetas and their collaborators appeared to be closely held by a few core members of the collective who communicated with a select few in the media and online. Now, Anonymous FreeAcuña is acting almost like a clearinghouse of information about the drug cartel. According to a spokesperson, “We get literally hundreds of pieces of information and we go through them carefully. If we cannot get at least two confirmations and a visual confirmation, we won't post it.”[6] In some instances, it is feeding information to journalists and to the online media.

Finally, unlike the 2011 incident, there are no demands sought by Anonymous FreeAcuña. There is no captive to bargain for, other than town of Acuna itself. Even so, the group is not demanding that the drug cartel leave town or cease its operations in exchange for stopping the flow of information. It is merely publishing information that comes its way, hoping that some action will be taken. The group does claim a success in the arrest of Alfredo Andrade Parra, a major narcotics trafficker based in Acuña who was wanted on federal charges in Del Rio and San Antonio.

The differences between this current operation and the one in the fall of 2011 reveal the evolution of cyber war in the underworld. Anonymous FreeAcuña has opened another front in the cyber war against Los Zetas in less than two years. An important question is why did an Anonymous group return to battle Los Zetas in cyberspace?

The Crossing of the Red Line in Cyberspace

One answer to the question about why Anonymous FreeAcuña reengaged in operations against Los Zetas is that there was simply nothing to stop it. An initial supposition in my original article was that there might be a type of mutually assured destruction that existed between Anonymous and Los Zetas that deterred each group from attacking each other in the future. Clearly, Anonymous FreeAcuña does not believe that it is crossing a “red line” nor does it believe that since 2011 Los Zetas have been able to develop the technological prowess to uncover the identities of a new group of hacktivists and target them. The group also believes it has adequate safeguards in place. According to its blog:

> Upon entering FREEACUNA ANONYMOUS, we never cease to be ANONYMOUS, because wherever we are, 24 hours a day we are monitoring our environment. That is why personal safety becomes a habit of life. We teach our collective members the importance of not revealing that they belong to ANONYMOUS even to their closest loved ones. We train our group on how to stay anonymous while on the Internet being that Organized Crime as well as the Government have specialized teams whose sole duty it is to try to locate members of groups like ours since they afraid that their corruption will be brought to the light of truth. This is why ANONYMOUS FREEACUNA only has one official voice, that of member FREEACUNA @freeacuna on TWITTER. Why? So that only that person is the target of government, political parties and organized crime. All others within the collective spread the ‘voice’ of FREEACUNA within social networks and media. @FREEACUNA PRESS is the alternate voice of @freeacuna in case an emergency or special situation warrants it.

Moreover, it is apparent that the Mexican government has not increased its capacity to reform and strengthen law enforcement to a level that would preclude the formation of an extralegal group like Anonymous FreeAcuna. If the police in Acuna or in the state of Coahuila were up to the task, Los Zetas would have been unable to strengthen their grip on the town.

Without strong law enforcement institutions, individuals in insecure areas will at times take matters into their own hands. This sort of environment is ripe for the emergence of an Anonymous group. Anonymous is “a classic ‘do-ocracy’”. The term “means rule by sheer doing: Individuals propose actions, others join in (or not), and the Anonymous flag is flown over the result. There’s no one to grant permission, no promise of praise or credit, so every action must be its own reward.”[7] Anonymous FreeAcuña started in this very fashion. A group of students saw an injustice and then linked themselves to Anonymous. It was not directed from the same Anonymous group that started the 2011 campaign nor was it directed from anyone outside the community of Acuña.

Nonetheless, the founders of Anonymous FreeAcuña have clearly embraced the ethos of internet freedom espoused by the larger Anonymous collective. In one of its blog postings that identifies a ranch used by the cartel in Coahuila, there is the following preface,

> The main slogan of ANONYMOUS is “KNOWLEDGE IS FREE” this means that all that is hidden, all that is corrupt, all that is done to keep the people ignorant must come to light. All knowledge must be free, which brings us to today's topic - NARCO RANCHES outside of Ciudad Acuña, Coahuila but whose owners not only live in Acuña but are involved in the political circles of the city with friendly ties to the spheres of power in Saltillo, Coahuil[8]

The publishing of information about property and other features of Los Zetas’ network by individuals previously unaffiliated with Anonymous demonstrates that Anonymous is now a movement, not merely an organization. While the original Anonymous group began as a way to promote internet freedom, a split emerged over whether to pursue “morals motivated” operations to take on groups who were abusive of human rights and freedom or to stay dedicated to operations that promoted the hacktivist creed of “privacy for individuals, transparency for the powerful”. This split may still exist, but little can be done to instill discipline among the membership. It would appear that as long as liberating information leads to human liberation (as defined by the collective), any group can brand itself as Anonymous affiliate. “Cyber vigilantism” now appears to be an accepted approach within the Anonymous movement.

Vigilantes, however, still often pay a price for their activities. No matter the safety protocols that have been put in place by Anonymous FreeAcuña, Los Zetas will respond in a public or private way. Los Zetas have a “criminal brand” that includes their prowess in information operations and electronic warfare.

They have a reflexive need to control information about them. By choosing to “out” the various parts of their organizational infrastructure, Anonymous FreeAcuña have struck Los Zetas in a vulnerable place. Aside from attacking them physically or undermining their finances, striking at their anonymity is acutely painful for the cartel. Los Zetas may now choose to carry through on their 2011 threat to kill ten innocent people or it may choose to issue another similar threat in an effort to coerce the new Anonymous group to cease its operations. A fear during the initial clash in 2011 was that Los Zetas would kill random people, place the symbol of Anonymous—Guy Fawkes masks—on the corpses and make it appear as though they had tracked down some members of the collective. They may also be able to “reverse hack” some members of the Anonymous FreeAcuña group or those who provide it with information.

No matter how Los Zetas respond, it will yet another demonstration of the weakness of the Mexican government; it is once again sidelined in this sort of conflict. The government is unable, or unwilling, to respond by taking action against Los Zetas or to persuade Anonymous FreeAcuña to allow the authorities to respond. Given the corruption of Mexican law enforcement and the penetration of Los Zetas into numerous areas of governmental authority, the actions of FreeAcuña may meet with limited success. However, given the latest split within Los Zetas, the publication of information about the activities of Los Zetas in the town of Acuna may leave it vulnerable to attacks by the opposing faction or rival cartels. The danger is an increased level of violence as one side attempts to protect its assets and as the other side attempts to gain an advantage. This will also have the additional effect of degrading public safety in Mexico even further. The mere creation of Anonymous FreeAcuña and its cyber vigilante activities is evidence that Mexican law enforcement is hollow and brittle.

New Questions, New Concerns

The current iteration of the cyber war between Anonymous and Los Zetas raises serious issues that require additional exploration. In some respects, the Anonymous FreeAcuña group is engaging in tactics that immediately preceded the kidnapping of the Anonymous member in 2011. At that time, Anonymous launched Operation Paperstorm in the Mexican state of Veracruz where portions of the collective felt that local government authorities were actively cooperating and shielding Los Zetas while prosecuting people who posted kidnapping reports on Twitter. Initially, the operation began as a leaflet campaign, denouncing the state government for its collusion with Los Zetas. The Anonymous member who was abducted was believed to have been distributing leaflets at the time. Now, rather than leaflets, Anonymous FreeAcuña is using a blog. However, the anonymity provided by the blog may be short lived. The blog site used by Anonymous FreeAcuña is not sophisticated and Los Zetas have demonstrated their ability to track down bloggers and those who merely post on blogs.

Also, as previously mentioned the new Anonymous group has not issued any demands on its blog; this is curious.The group may believe that it is merely filling the information gap as a type of group of citizen journalists and cyber vigilantes. It may also see itself as having nothing to lose by publishing the information as the cartel has already taken over the town. This was also alluded to in the group’s only known interview with the media.Put simply by the spokesperson, “We are not looking to destroy people, the Zetas and our corrupt government have done quite well doing this for decades."[9] In some ways, it as if the members of Anonymous FreeAcuña see themselves as a resistance group whose town is under occupation. But once again the lack of demands is striking; even resistance groups have goals that they espouse. Moreover, publishing information online about Los Zetas' operations is the only method of coercion that the group has. By "outing" Los Zetas without any explicit demands it is unclear what, if anything, Anonymous FreeAcuña is trying to coerce Los Zetas into doing.

Beyond how the members of Anonymous FreeAcuña see themselves, the larger question about this latest cyber war is how the group acts if Los Zetas retaliated by killing people, whether they were members of the collective or not? The structure of Anonymous has its share of weaknesses that Los Zetas were able to exploit in a limited degree in 2011 incident. It has been assumed that Anonymous' geographically dispersed membership and nebulous structure have been strategic advantages for the collective. But operationally, these characteristics have proven to be troublesome. Due to Anonymous' loose structure, any operation can move forward or be cancelled in a capricious manner. Yet, the posting of information about Los Zetas' operations has already crossed beyond the line drawn in 2011. Although the schism over morals motivated attacks seems to be irrelevant, it may only be so at this stage. In the 2011 clash, Los Zetas took advantage of these divisions by significantly raising the stakes. The attempt to reverse hack Anonymous and the threat to kill ten innocent people in the event of any subsequent release of information about the cartel quickly made it the first Anonymous operation where there was the potential for significant loss of life. This led to several Anonymous members to have serious misgivings about moving forward with the threat against Los Zetas while others wanted to move forward. The killing of people in Acuña by Los Zetas with "corpse messages" stating that the acts by Anonymous FreeAcuña are the reasons for the deaths may significantly alter the calculus by Anonymous FreeAcuña.

Several questions surround the scope and depth of Anonymous FreeAcuña's operations. Can Anonymous FreeAcuña enlist more members from the core of the larger Anonymous movement? The Anonymous FreeAcuña group has said that it has contacts within the larger movement and has called for a broader campaign directed against the federal government of Mexico. Also, will other Mexicans who want to take a stand against Los Zetas or other drug cartels start their own Anonymous groups? In other words, Anonymous FreeAcuña may have paved the way for the possible proliferation of Anonymous groups acting as cyber-vigilantes. The emergence of Anonymous FreeAcuña is evidence itself of the inspirational quality of the Anonymous movement in Mexico.

There is little doubt that this is just the beginning of this clash between Anonymous and Los Zetas.The potential for this cyber war in the underworld to expand or to spill out into real world violence is high. In the meantime, it might be worthwhile to continue to check the comments section of this article….

Notes

[1] The author would like to thank US Army War College interns Kate Branson from Dickinson College and Douglas Steinberg from Bates College for their assistance in preparing this article.

[2] Paul Rexton Kan, "Cyberwar in the Underworld: Anonymous vs. Los Zetas in Mexico" Yale Journal of International Affairs, (Winter 2013), URL: http://yalejournal.org/2013/02/26/cyberwar-in-the-underworld-anonymous-versus-los-zetas-in-mexico/

[3] Jason Buch, "Zetas have Anonymous Foes", San Antonio Express-News, 1 June 2013, URL:

http://www.expressnews.com/news/local_news/article/Zetas-have-Anonymous-foes-4566921.php

[4] Ibid.

[5] Kan.

[6] Buch.

[7] Quinn Norton, "Inside Anonymous", Wired, July 2012, 134.

[8] URL: http://freeacuna.blogspot.com/2013/05/english-language-report-narco-ranch-1.html

[9] Buch

Table of Contents

Taiwan a 'Testing Ground' for Chinese Cyber Army

By Michael Gold, Reuters, Jul 18, 2013

(Reuters) - Taiwan is the frontline in an emerging global battle for cyberspace, according to elite hackers in the island's IT industry, who say it has become a rehearsal area for the Chinese cyberattacks that have strained ties with the United States.

The self-governing island, they say, has endured at least a decade of highly -targeted data-theft attacks that are then directed towards larger countries.

"We've seen everything," said Jim Liu, the 28-year-old founder of Lucent Sky, a Taiwanese internet security company specializing in resolving dangerous software vulnerabilities that hackers can exploit in order to gain access to a system.

"We'll see a specific attack signature here, and then six months later see the same signature in an attack on the States."

A Pentagon report in May accused China of trying to break into U.S. defense computer networks. It followed another report in February by U.S. computer security company Mandiant that said a secretive Chinese military unit was probably behind a series of hacking attacks that had stolen data from 100 U.S. companies.

Beijing dismissed both reports as without foundation. But Taiwan experts say that hacking methods such as those outlined in the Mandiant report are the same kinds of security breaches that they had seen several years earlier.

Regarded by China as a renegade province it must recover, by force if necessary, it is easy to see why Taiwan might be an ideal target for Chinese hackers: it is close to the mainland, Mandarin- speaking and boasts advanced internet infrastructure.

STOLEN DATA

This cyber war playing out across the narrow Taiwan Strait first came to public attention in 2003, when a Taiwanese police agency realized hackers had stolen personal data, including household registration information, from its computer system.

These attacks differed from traditional hacking attempts - where many casual hackers attempt to disrupt their targets' systems, these hackers went in stealthily, with the intention to plunder rather than destroy.

"Back then it was very rare to see these kinds of social network attacks," said hacking specialist Jeremy Chiu, a contract instructor in IT for Taiwan's intelligence agencies. "They were very, very well organized."

Other indicators, including the ease with which the hackers penetrated an email system written entirely in Chinese, painted a picture of the culprits as a large, coordinated group of mainland Chinese hackers.

"One thing that indicates government support for these attacks is just the sheer volume - how many agencies are being attacked on a daily basis," said Benson Wu, postdoctoral researcher in information technology at Taiwanese think-tank Academia Sinica and co-founder of Xecure Lab, which focuses on responding to advanced persistent threats.

Interviewed at his downtown Taipei office, Wu's set-up fits the classic hacker image: dimly-lit, strewn with wires and humming with computers.

On a projector screen he displayed a list of emails, written in Chinese, with subject headings like "meeting notes", "dinner attendance" and "questionnaire".

"These are all hacking attempts," Wu explained. Once the documents have been opened, they plant a backdoor allowing the hacker virtually unfettered access to the network.

HACKING NINE-TO-FIVE

One such "spearphishing" attack was reportedly used on the White House in October. A Taiwan expert in cyberespionage interviewed by Reuters estimated that thousands of Taiwanese high-level government employees receive as many as 20 to 30 of these emails a month.

"We've been following these Chinese hackers for so long, we can track their daily work schedule," said the expert, who asked not to be identified.

"People expect hackers to be night owls, but these guys work very normal hours - on Chinese national holidays, for example, we don't see any hacking activity at all."

Tracking the exact source of the attacks, however, remains a slippery game of internet sleuth.

"We take the IP address culled from the attack as a springboard, then track it through the internet - perhaps the same IP address was used in a forum registration, or to register a QQ handle," he said, referring to a popular Chinese chat program. "It depends how good they are at covering their tracks."

China denies being behind hacking attacks on other nations and insists it is a major victim of cyber attacks, including from the United States - an argument that Beijing sees as strengthened by revelations last month from a former National Security Agency contractor, Edward Snowden, about top-secret U.S. electronic surveillance programs.

The United States and China held talks focused on cyber issues last week.

According to internet platform Akamai, 27 percent of worldwide hacking activity during 2012 originated in China. The same report, however, also placed Taiwan among the top five digital attack originating countries in 2012.

"Taiwan is one of the key countries where we see a lot of activity," said Singapore-based malware researcher Chong Rong Hwa of network security firm FireEye Inc.

A report issued by SecureWorks, a network safety arm of PC maker Dell Inc, said Taiwan government ministries are swarming with a particularly malicious form of data-nabbing computer virus.

In one year, the Taiwan National Security Bureau encountered more than 3 million hacking attempts from China, according to statements given by bureau director Tsai Teh-sheng in March in response to questions from lawmakers.

Military and technology intelligence was included among the pilfered data. A representative from the bureau declined to comment when contacted by Reuters.

"Taiwan will continue to be the battleground for lots of cyber attacks; it's like we are on our own," Wu said. "China has a huge pool of talent and technical resources."

Table of Contents

U.S. Repeals Propaganda Ban, Spreads Government-Made News to Americans

By John Hudson, Foreign Policy, July 14, 2013

For decades, a so-called anti-propaganda law prevented the U.S. government's mammoth broadcasting arm from delivering programming to American audiences. But on July 2, that came silently to an end with the implementation of a new reform passed in January. The result: an unleashing of thousands of hours per week of government-funded radio and TV programs for domestic U.S. consumption in a reform initially criticized as a green light for U.S. domestic propaganda efforts. So what just happened?

Until this month, a vast ocean of U.S. programming produced by the Broadcasting Board of Governors such as Voice of America, Radio Free Europe/Radio Liberty, and the Middle East Broadcasting Networks could only be viewed or listened to at broadcast quality in foreign countries. The programming varies in tone and quality, but its breadth is vast: It's viewed in more than 100 countries in 61 languages. The topics covered include human rights abuses in Iran, self-immolation in Tibet, human trafficking across Asia, and on-the-ground reporting in Egypt and Iraq.

The restriction of these broadcasts was due to the Smith-Mundt Act, a long-standing piece of legislation that has been amended numerous times over the years, perhaps most consequentially by Arkansas Senator J. William Fulbright. In the 1970s, Fulbright was no friend of VOA and Radio Free Europe, and moved to restrict them from domestic distribution, saying they "should be given the opportunity to take their rightful place in the graveyard of Cold War relics." Fulbright's amendment to Smith-Mundt was bolstered in 1985 by Nebraska Senator Edward Zorinsky, who argued that such "propaganda" should be kept out of America as to distinguish the U.S. "from the Soviet Union where domestic propaganda is a principal government activity."

Zorinsky and Fulbright sold their amendments on sensible rhetoric: American taxpayers shouldn't be funding propaganda for American audiences. So did Congress just tear down the American public's last defense against domestic propaganda?

BBG spokeswoman Lynne Weil insists BBG is not a propaganda outlet, and its flagship services such as VOA "present fair and accurate news."

"They don't shy away from stories that don't shed the best light on the United States," she told The Cable. She pointed to the charters of VOA and RFE: "Our journalists provide what many people cannot get locally: uncensored news, responsible discussion, and open debate."

A former U.S. government source with knowledge of the BBG says the organization is no Pravda, but it does advance U.S. interests in more subtle ways. In Somalia, for instance, VOA serves as counterprogramming to outlets peddling anti-American or jihadist sentiment. "Somalis have three options for news," the source said, "word of mouth, al-Shabab, or VOA Somalia."

This partially explains the push to allow BBG broadcasts on local radio stations in the United States. The agency wants to reach diaspora communities, such as St. Paul, Minnesota's significant Somali expat community. "Those people can get al-Shabab, they can get Russia Today, but they couldn't get access to their taxpayer-funded news sources like VOA Somalia," the source said. "It was silly."

Lynne added that the reform has a transparency benefit as well. "Now Americans will be able to know more about what they are paying for with their tax dollars -- greater transparency is a win-win for all involved," she said. And so with that we have the Smith-Mundt Modernization Act of 2012, which passed as part of the 2013 National Defense Authorization Act, and went into effect this month.

But if anyone needed a reminder of the dangers of domestic propaganda efforts, the past 12 months provided ample reasons. Last year, two USA Today journalists were ensnared in a propaganda campaign after reporting about millions of dollars in back taxes owed by the Pentagon's top propaganda contractor in Afghanistan. Eventually, one of the co-owners of the firm confessed to creating phony websites and Twitter accounts to smear the journalists anonymously. Additionally, just this month, the Washington Post exposed a counter-propaganda program by the Pentagon that recommended posting comments on a U.S. website run by a Somali expat with readers opposing al-Shabab. "Today, the military is more focused on manipulating news and commentary on the Internet, especially social media, by posting material and images without necessarily claiming ownership," reported the Post.

But for BBG officials, the references to Pentagon propaganda efforts are nauseating, particularly because the Smith-Mundt Act never had anything to do with regulating the Pentagon, a fact that was misunderstood in media reports in the run-up to the passage of new Smith-Mundt reforms in January.

One example included a report by the late BuzzFeed reporter Michael Hastings, who suggested that the Smith-Mundt Modernization Act would open the door to Pentagon propaganda of U.S. audiences. In fact, as amended in 1987, the act only covers portions of the State Department engaged in public diplomacy abroad (i.e. the public diplomacy section of the "R" bureau, and the Broadcasting Board of Governors.)

But the news circulated regardless, much to the displeasure of Rep. Mac Thornberry (R-TX), a sponsor of the Smith-Mundt Modernization Act of 2012. "To me, it's a fascinating case study in how one blogger was pretty sloppy, not understanding the issue and then it got picked up by Politico's Playbook, and you had one level of sloppiness on top of another," Thornberry told The Cable last May. "And once something sensational gets out there, it just spreads like wildfire."

That of course doesn't leave the BBG off the hook if its content smacks of agitprop. But now that its materials are allowed to be broadcast by local radio stations and TV networks, they won't be a complete mystery to Americans. "Previously, the legislation had the effect of clouding and hiding this stuff," the former U.S. official told The Cable. "Now we'll have a better sense: Gee some of this stuff is really good. Or gee some of this stuff is really bad. At least we'll know now."

Table of Contents

House Fails To Kill Pentagon's Foreign Websites

By Tom Vanden Brook, USA TODAY, July 24, 2013

WASHINGTON -- The House has failed to kill funding for websites the Pentagon uses to try to influence foreign audiences, an initiative criticized in a recent undisclosed government report.

Rep. Jeff Denham, R-Calif., introduced a measure that would have slashed $19.7 million in funding for the Trans Regional Web Initiative. The legislation failed by a vote of 238-185.

The 10 websites are run by U.S. Special Operations Command and are intended to "highlight the positive aspects of region and host nation counterterrorism efforts that as well as highlighting the negative aspects of adversaries actions'," according to a report on Pentagon propaganda by the Government Accountability Office.

The report, completed in April, was circulated only to select members of Congress and government agencies. USA TODAY obtained a copy. The report concluded the websites are not well coordinated with such government agencies as the State Department, or even the Pentagon's other propaganda programs.

Denham believes the websites are too costly, questions their effectiveness and the Pentagon's ability to measure their performance, according to his press secretary, Jordan Langdon.

"In a budget environment where the Department of Defense is reducing the size of the force, delaying critical training, canceling deployments and furloughing civilian staff, there is no justification for operating news websites of dubious utility," Langdon said in an e-mail. "To put $20 million in perspective, it is equivalent to the amount of money saved by the Army National Guard when it reduced its end strength by 2,000 soldiers."

The automatic budget-cutting process known as sequestration has forced the Pentagon to trim $45 billion from its budget this year. That has resulted in furloughs of civilian employees, cancellation of training missions and delayed maintenance. The result is decreased readiness to fight, according to Pentagon leaders, including Gen. Martin Dempsey, the chairman of the Joint Chiefs of Staff.

Pentagon spending on propaganda programs mushroomed in the middle of the last decade, coinciding with surge in troops and resources sent to Iraq and Afghanistan.

Since 2005, the Pentagon has spent hundreds of million of dollars on what it refers to as Military Information Support Operations (MISO). These propaganda efforts include websites, leaflets and broadcasts intended to change foreigners' "attitudes and behaviors in support of U.S. Government" objectives, according to the GAO.

Some of them, such as the Trans Regional Web Initiative, disclose the U.S. military as the source, although discreetly. Some broadcasts in Afghanistan, on the other hand, are silent about their U.S. funding.

The GAO determined that the Pentagon had "taken some steps to coordinate the websites with some State Department regional bureaus." But some State Department Public Diplomacy officials and senior embassy officials told investigators "that such websites have the potential to unintentionally skew U.S. policy positions or be out of step with U.S. government efforts in a particular country."

Denham had hoped to kill the program so that the Pentagon "would be able to more effectively resource its core mission: building a force that can fight and win our nation's wars," Langdon said.

Table of Contents

Out of Sight

From The Economist, Jul 27th 2013

Every day for up to ten minutes near the London Stock Exchange, someone blocks signals from the global positioning system (GPS) network of satellites. Navigation systems in cars stop working and timestamps on trades made in financial institutions can be affected. The incidents are not a cyber-attack by a foreign power, though. The most likely culprit, according to Charles Curry, whose firm Chronos Technology covertly monitors such events, is a delivery driver dodging his bosses' attempts to track him.

The signals are weak. Mr Curry likens them to a 20-watt light bulb viewed from 12,000 miles (19,300 km). And the jammers are cheap: a driver can buy a dashboard model for about £50 ($78). They are a growing menace. The bubbles of electromagnetic noise they create interfere with legitimate GPS users. They can disrupt civil aviation and kill mobile-phone signals, too. In America their sale and use is banned. In Britain they are illegal for civilians to use deliberately, but not, yet, to buy: Ofcom, a regulator, is mulling a ban. In recent years Australian officials have destroyed hundreds of jammers.

In the right (or wrong) hands, they are potential weapons. Britain's armed services test the devices in the Brecon Beacons in Wales, a military training area. North Korea uses big lorry-mounted versions to block GPS signals in South Korea. Starting with a four-day burst in August 2010, the attacks, which come from three positions inside the North, have lengthened. In early 2012 they ran for 16 days, causing 1,016 aircraft and 254 ships to report disruption.

Mr Curry worries that criminals or terrorists could knock out GPS for an entire city or shipping lane anywhere in a flash. Even without North Korean-sized contraptions, the jamming can be substantial. Suitcase-sized devices on sale on the internet claim a range of 300-1,000 metres.

Malfunctioning satellites and natural interference from solar activity have hit GPS signals and sent ships off course. David Last, a navigation expert, says an accidental power cut, perhaps caused by a jammer taken on board a car ferry, could cause a shipwreck. Generating a false signal—spoofing—is another threat. In December 2011 Iran said it had spoofed an American drone before capturing it (most experts dismiss the claim). So far effective spoofing seems confined to laboratories, but Mr Last says some governments are already taking countermeasures.

One solution is a different means of navigation. In April South Korea announced plans for a network of 43 eLoran (enhanced long-range navigation) ground-based radio towers, based on technology first used in the second world war. It uses a far stronger signal than GPS, and should give pilots and ships' captains a safer alternative by 2016. With Chinese and Russian help, South Korea hopes to expand coverage across the region.

Britain's General Lighthouse Authorities (GLA) are following suit with seven new eLoran stations. Martin Bransby, an engineer with the GLA, says this will replace visual navigation as the main backup for GPS. It will be working by mid-2014, and cost less than £700,000; receivers cost £2,000 per vessel. By 2019 coverage should reach all big British ports.

America's military-research agency DARPA has an experimental “single-chip timing and inertial measurement unit” (TIMU). When finished, according to the project's boss, Andrei Shkel, it will use tiny gyroscopes and accelerometers to track its position without using satellites or radio towers. America's White Sands missile range in New Mexico is installing a “Non-GPS Based Positioning System”, using ground-based antennae to provide centimetre-level positioning over 2,500 square miles. In May the Canadian government said it would splash out on anti-jam upgrades for military aircraft.

A new version of the US air force's bunker-busting bomb, designed in part to destroy Iranian nuclear facilities, includes technology to prevent defenders from blocking its satellite-based guidance systems. MBDA, a European missile firm, is working on similar lines.

But for many users, GPS and other space-based navigation systems—which include Russia's GLONASS, China's partly complete Beidou, and an as-yet unfinished project by the European Union—remain indispensable and ubiquitous. They are also vulnerable. For those whose lives or livelihoods depend on knowing where they are, more resilient substitutes cannot come fast enough.

Table of Contents

Scenario Puts Energy, Politics in Hackers' Cross Hairs

By Joe Gould, DefenseNews, Jul. 23, 2013

WASHINGTON — A US Army cyber official warns that the nation faces a possible cyberwar in which anonymous foreign computer hackers penetrate government networks andcreate friction between Washington and its allies, discredit elected officials, and create political and economic instability if the US fails to adapt.

In a recent academic thesis, Col. Bryant Glando paints a nightmarish picture of how attacks against the US might unfold to influence its political process and national security objectives — without a shot being fired.

To avert catastrophe, Glando argues the Defense Department should elevate cyber from a primary mission to a core mission area, a new strategic approach that would provide a military advantage in cyberspace "over all potential adversaries."

"The threats are real," the thesis reads, before paraphrasing military theorist Carl von Clausewitz. "It is not a matter of if but a matter of when a nation or non-nation state develops a new type of warfare to exploit an Achilles' heel of the United States in order to achieve its own strategic objectives. The nature of war does not change, but warfare does, and those who adapt survive, and those who fail suffer the consequences."

As proposed by Glando, cyberwarfare would have a whole-of-government approach, as supported by DoD's definition of a core mission area. The way it's organized, he said, "potentially degrades the ability to deter, defend, and defeat an adversary in, through, and from cyberspace. Why, because this fundamentally violates the joint principles of unity of command, economy of force, and mass as defined in US Joint Publication 3-0."

Soon to become deputy chief of US cyber Command's J-35 Future Operations Cell, Glando is the former deputy director of the cyberspace proponent for Army Cyber Command/2nd Army, based at Fort Belvoir, Va., and a part of US Cyber Command. In the early 2000s, Glando led an Army task force that was part of the joint response to "Titan Rain," a series of cyber espionage attacks attributed to the Chinese and used to pilfer information from American government agencies and defense contractors.

The 'Art of the Possible'

The 10 years since have seen, among other incidents, the 2007 cyberattacks that swamped Estonian websites amid a dispute with Russia; the hacking of Ossetian media and government websites during the 2008 Georgia-South Ossetia war; the 2010 Stuxnet malware attack on an Iranian nuclear enrichment facility; and cyber espionage efforts originating from China, including spying against military, commercial, research and industrial corporations.

Peering into the future, Glando's "art of the possible" scenario sees country "ABC" launch a sophisticated 3 ½-year string of cyberattacks against the US and country "XYZ," which it hopes to take over. ABC penetrates the US defense sector, sows disinformation in the American political system, attacks critical government services and fuels civil unrest with leaks and tension between Washington and its allies.

Hackers, presumably from ABC, launch anonymous attacks and, at one point, steal the plans for the F-35 Joint Strike Fighter. Later, ABC reveals its plans for a similar jet.

The attacks get personal, exposing the extramarital affair of a US senator who supports a bilateral defense agreement with XYZ.

In an eerie case of academics imitating life, Glando's scenario has a new Pentagon directive for counter-cyber espionage that outrages the public because it calls for increased monitoring of US public communications.

Disinformation is a key part of the cyberattacks. When the hacker collective Anonymous leaks the directive online, "Pentagon officials report that some of the information posted was incorrect or was modified. US public is outraged and demands justice. Litigation is initiated by a group of concerned US citizens to prevent this directive from being implemented."

The month before 2014 elections, unknown hackers gain access to various political websites, Twitter and Facebook accounts and manipulate the statements of key political officials on sensitive political issues. Later, US Senate and House majorities change, spurring a new emphasis on domestic issues and relations in the Western Hemisphere. Some members of Congress begin pushing "for a new strategic shift to look inward and are requesting a review of all bilateral defense agreements."

Over the next year, a software glitch crashes a US attack helicopter, America experiences power outages, water and sewage systems in Illinois suffer power outages and XYZ's critical infrastructure experiences outages. Cyberattacks are the implied cause.

The stock market and employment numbers plummet after unknown hackers remove $2 trillion from electronic circulation.

December 2016 brings the grand finale, as key military systems in XYZ and the US fail because of software glitches; utilities at US military bases near XYZ fail, which delays US forces from responding to ABC's imminent invasion of XYZ.

At home, a coordinated cyberattack on critical infrastructure within the US and XYZ shuts down key government services, "creating chaos across the public and private sectors."

"Country ABC launches a massive invasion of country XYZ," the thesis reads. "The ability of the US to respond with sufficient military power is delayed due to the crippling effects of a concentrated cyberspace warfare campaign directed against the United States, its allies and country XYZ."

Hard and Soft Power

Jeffrey Carr, founder of cybersecurity consultancy Taia Global and author of "Inside cyber Warfare," faulted Glando's scenario and called the proposed solution "irrelevant to the actual threat landscape." He wrote in an email that the scenario "goes from being vastly under-stated (a 20-minute power outage?) to vastly overstated (casting doubt in an electorate's mind) and demonstrates a lack of understanding about what's technically possible, not to mention realistic."

Glando responded to the criticism by agreeing that more devastating cyberattacks are possible, but said in his scenario, the adversary was using stealthier "brownouts" to confuse efforts to attribute the attacks and the response. Otherwise, Glando disagreed that cyberattacks could not be used to influence an electorate and cited current events.

"During the Arab Spring, modern technology was used to spur dissent, and not just in a single country," he said.

Christopher Bronk, a former diplomat with the State Department and a fellow specializing in information technology policy at Rice University's Baker Institute, said cyber operations can enable the application of hard power and soft power, as suggested by Glando.

"The scenario has it all, the kind of kinetic attacks that makes the oil and gas industry go kaboom to influence games like, 'Oh, this country's going to lose some senatorial support,' " Bronk said.

According to Bronk, the military must make cybersecurity part of its culture "because computing pervades everything the military does now. It's all ones and zeroes, and digital technology is embedded all the way down to a rifle company."

Table of Contents

Private Cyber Retaliation Undermines Federal Authority

By Jan Kallberg, Defense News, 28 Jul 2013

During the last year, several op-eds and commentaries have proposed that private companies have the right to strike back if cyber attacked and conduct their own offensive cyber operations.

The demarcation in cyber between the government and the private spheres is important to uphold because it influences how we see the state and the framework in which states interact. One reason we have a nation state is, in a uniform and structured way, under the guidance of a representative democracy, to deal with foreign hostility and malicious activity.

The state is given a monopoly on violence by its citizenry. The state then acts under the existing laws on behalf of the citizens to ensure the intentions of the population it represents. These powers grant the federal government an authority to enforce compliance of the laws and handle foreign relations. If the federal government cannot uphold that authority, confidence in government will suffer.

The national interest in protecting legitimacy and maintaining the confidence in the federal government is far stronger than the benefits of a few private entities departing on their own cyber odysseys to retaliate against foreign cyber attacks.

The importance of demarcation between government and private entities can be visualized with an example. A failed bank robbery leads to a standoff where the robbers are encircled by government law enforcement. The government upholds its monopoly on violence and, on behalf of the people, engages the robbers in a potential shootout.

All other citizens are instructed to leave the area. The law enforcement officers seek to solve the situation without any violence. This is how we have designed the demarcation between the government and the private sphere in the analog world.

If the US allowed companies to strike back following a foreign cyber attack, it would be abandoning this demarcation.

Going back to the example of bank robbers surrounded by law enforcement, the logic of private cyber retaliation would allow any customer who had an account in the robbed bank to show up and open fire at the robbers at their own discretion, leaving the police to sort out the shootout and the aftermath with no responsibility for the triggering event.

Abandoning the clear demarcation between government and private spheres leads to entropy, loss of control, and is counterproductive for the national cyber defense and the national interest.

The counter argument says private companies are defenseless against cyber attacks and therefore have the right to self defense. The independent Commission on the Theft of American Intellectual Property recently published a report that strongly supported allowing private companies to retaliate against cyber attackers. According to the commission, these counterstrikes should be conducted as follows: “Without damaging the intruder’s own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information.”

The proponents for private cyber retaliation base their view on several assumptions. First, that the private company can attribute the attack and determine who is attacking them.

Second, that the counterstriking companies have the cyber resources to engage, even if it is a state-sponsored organization on the other end, and that there will be no damages.

And third, that the events do not lead to uncontrolled escalation and that the cyber interchanges only affect the engaged parties.

An attacker has multiple options and can target other entities and institutions in reprisal. If the initial attacker is a state-sponsored organization in a foreign country, multinational companies could have significant business and interests at risk if the situation escalates. Private companies would not be responsible for the aftermath, and the entropy that could occur would undermine the American stance and cost its higher ground in challenging the state sponsors behind the cyber attacks in the framework of the international community. The answer to who should hack back, if deciding to do so, is simple: It should be the federal government for the same reason that you would not fly on a passport issued by your neighbor across the street. Only the federal government is suitable to engage foreign nations and the private entities.

The unaddressed core problem is that we have not yet been able to create mechanisms to transfer cyber incidents from the private realm to the authorities. This limited ability during the short time frame when an attack occurs initially gives the attacker an advantage, but this will be solved over time and does not outweigh the damages from an undermined federal authority due to entropy in cyber.

Table of Contents

US Spends $24 Million on ‘Propaganda Plane' Few Can See or Hear

By John Hudson, Foreign Policy, July 28, 2013

For the last six years, the U.S. government has spent more than $24 million to fly a plane around Cuba and beam American-sponsored TV programming to the island's inhabitants. But every day the plane flies, the government in Havana jams its broadcast signal. Few, if any, Cubans can see what it broadcasts.

The program is run by the U.S. Broadcasting Board of Governors, and for the last two years, it has asked Congress to scrap the program, citing its exorbitant expense and dubious cost-effectiveness. "The signal is heavily jammed by the Cuban government, significantly limiting this platform's reach and impact on the island," reads the administration's fiscal year 2014 budget request.

But each year, hard-line anti-Castro members of Congress have rejected the recommendation and renewed funding for the program, called AeroMarti. Now, under the restrictions of government-wide belt-tightening, AeroMarti may finally die, but its fate has yet to be sealed.

"It's hard to believe we are still wasting millions of taxpayer dollars on beaming a jammed TV signal - that fewer than 1 percent of Cubans can see - from an airplane to the island," Sen. Jeff Flake (R-AZ) tells The Cable.

For Flake and fellow critics of the program, AeroMarti has called into question America's decades-long information war against the Castro regime. But other Castro critics say the U.S. must continue to find ways to disseminate messaging onto the autocratic island.

At the moment, the AeroMarti twin-engine Gulfstream 1 plane is grounded in Georgia due to the automatic spending cuts known as sequestration. But the program's ultimate fate will be determined by the House and Senate Appropriations Committees.

Under ordinary circumstances, the plane flies a figure eight pattern near the Communist island beaming hours and hours of TV and Radio Marti, a U.S.-financed broadcaster akin to Radio Free Europe. From 2006 to 2010, AeroMarti burned through $5 million every year. In 2010, its budget was reduced to around $2 million per year. One iteration of the program involved a C-130 military plane and another involved a blimp attached to a cable 10,000 feet above the Florida Keys. All told, the flights have racked up a tab well over $24 million to U.S. taxpayers.

"Proponents of the program say we can't stop doing it because it would send a bad message to the Cuban government that we're capitulating," John Nichols, a communications professor at Penn State University, tells The Cable. "That's bogus: It's ineffective, it wastes a huge amount of money and the compromise we make to keep it on air, knowing it violates international law, is not at all worth it."

Since its inception, the U.S. government has spent well over half a billion dollars to fund Marti programming, which first aired on radio in 1985 and on TV in 1990. The programming includes everything from baseball games to local news to weather reports to interviews with anti-Castro dissidents. Its staunchest supporters in the House and Senate include Sen. Robert Menendez (D-NJ), chairman of the Senate Foreign Relations Committee, and Rep. Ileana Ros-Lehtinen (R-FL).

Ros-Lehtinen, in particular, is known for insisting that AeroMarti continue flying despite its dubious effectiveness. When repeatedly asked about the program this month, she declined to comment.

Menendez is not known to have advocated for the plane specifically, but he is a supporter of Radio and TV Marti in general.

"I will continue to stand behind the mission of Radio and TV Marti until the Cuban government ceases to deprive its citizens of objective and uncensored media sources," he told The Cable. "The Martis play a critical role in providing information to the Cuban people about events in and outside of Cuba, connecting with nearly a million Cubans every week. In this day and age, there are numerous platforms, new media tools, and technologies available to the Martís to fulfill and continue this integral mission, and I believe we should use every possible medium to break through the Castro regime's censorship barriers."

As it stands, the administration's budget request specifies not continuing AeroMarti. It is now up to the congressional committees to object to the proposal, which none have done thus far.

But regardless of what happens, it won't stop the programming of Radio and TV Marti as a whole. The BBG is enthusiastic about moving forward with other methods of getting its programming to Cuban viewers and listeners: disseminating DVDs, doling out flash drives, broadcasting via satellite and even offering a new smartphone app. The various work-arounds all carry Marti's programming.

"We have evolved to what our market demands," Carlos Garcia-Perez, director of the BBG's Office of Cuba Broadcasting, tells The Cable. "We're no longer just a TV and radio and internet operation, we're a multimedia operation."

In the past, Marti has come under criticism by critics such as Nichols who say its purpose is to peddle "anti-Castro propaganda."

"Even if the propaganda plane reached its audience, there's little evidence the Cuban people are going to spend their leisure time watching Cuban exiles snarl about Castro," said Nichols.

Senator Flake told The Cable he is similarly opposed to the channel. "While the president's most recent budget request would stop funding the flights, Congress should do the same with the TV Marti program as a whole," he said.

Garcia-Perez rejects the notion that Cuban listeners aren't interested in Marti's offerings, and ticked off a range of news events -- from the Venezuelan elections to the death of Osama bin Laden to the health struggles of Hugo Chavez -- where audience records were broken. "In November 2010, our website got 500 hits per day," he said. "Now it's 7,000 per day, and when there's a huge event going on it gets up to 15,000." For a typical media organization, that's not much to write home about, but Garcia-Perez says it's a lot considering that Havana blocks its web pages, requiring readers to access copies of the site on proxy servers. He also claimed that his system of e-mails, text messages, flash drives and DVDs is capable of reaching 1 million Cubans on the island. "We're here to provide the free-flow of information," he said, noting the Castro regime's draconian censorship of the press.

As for the content of Marti, other independent observers say its programming has improved in recent years under Garcia-Perez's leadership, which has steered away from more transparent anti-Castro messaging. "I have been impressed with the reforms at Radio Marti and Marti Noticias since the new director took over and shifted away from propaganda toward a more hard news and debate format," Ted Henken, a professor of Latino studies at Barch College, told The Cable. "They constantly interview people on the Island via phone and that's made the reporting far more grounded."

But despite differences about the value of Radio and TV Marti, there's one thing almost everyone agrees on: Spending millions of dollars a year to fly a plane around Cuba is not the savviest use of taxpayer money.

Table of Contents

Cyber-Sabotage Is Easy

BY Thomas Rid, Foreign Policy, July 23, 2013

Hacking power plants and chemical factories is easy. I learned just how easy during a 5-day workshop at Idaho National Labs last month. Every month the Department of Homeland Security is training the nation's asset owners -- the people who run so-called Industrial Control Systems at your local wastewater plant, at the electrical power station down the road, or at the refinery in the state next door -- to hack and attack their own systems. The systems, called ICS in the trade, control stuff that moves around, from sewage to trains to oil. They're also alarmingly simply to break into. Now the Department of Homeland Security reportedly wants to cut funding for ICS-CERT, the Cyber Emergency Response Team for the nation's most critical systems.

ICS-CERT's monthly training sessions in Idaho Falls put 42 operators at a time into an offensive mindset. For the first three days in last June's workshop, we learned basic hacking techniques, first in theory, then in practice: how to spot vulnerabilities, how to use exploits to breach a network, scan it, sniff traffic, analyse it, penetrate deeper into the bowels of the control network, and ultimately to bring down a mock chemical plant's operations. There was something ironic about Department of Homeland Security staff teaching us how to use Wireshark, an open-source packet analyzer; Metasploit, a tool for executing exploit code; man-in-the-middle attacks; buffer overflow; and SQL-injection -- all common hacking techniques -- and then adding, only half-jokingly: "Don't try this on your hotel's Wi-Fi!"

So it may come as a surprise to learn that attackers have never been able to engage in cyber-sabotage against America's critical infrastructure -- not once. ICS-CERT has never witnessed a successful sabotage attack in the United States, they told me. Sure, there have been network infiltrations. But those were instances of espionage, not destructive sabotage. Which raises two questions: one obvious, and one uncomfortable. If it's so easy, why has nobody crashed America's critical infrastructure yet? And why isn't the Defense Department doing more to protect the grid?

The questions only loomed large on the fourth day of the training -- a 10-hour exercise. We split into two groups, a large blue team and a small red team. The blue team's task was to defend a fake chemical company, with a life-sized control network complete with large tanks and pumps that would run production batches, a real human-machine interface, a so-called "demilitarized zone," even simulated paperwork and a mock management with executives that didn't understand what's really happening on the factory floor -- just like in real life. The red team's task was to breach the network and wreak havoc on the production process. By 5 pm they got us: toxic chemicals spilled on the floor, panic spread in the control room. Good thing for us this was only an exercise, and the gushing liquid was just water.

That exercise in Idaho was not unrealistic -- control system-related incidents can have serious consequences. In March 1997, a teenager in Worcester, Massachusetts, used a dial-up modem to disable controls systems at the airport control tower. In June 1999, 237,000 gallons of gasoline spilled out of a 16-inch pipeline in Bellingham, Washington, killing three people when it ignited. An ICS performance failure limited the controller's ability to understand what was happening and react swiftly. In August 2006, two disgruntled transit engineers sabotaged the traffic light controls at four busy L.A. corners for four days, causing major traffic jams. One of the most serious accidents happened in 2009 at the Sayano-Shushenskaya hydroelectric dam and power station in Russia, when a remote load increase caused a 940-ton turbine to be ripped out of its seat. The accident killed 75 people, pushed up energy prices, and caused damage in excess of $1.3 billion. In Idaho I heard two more stories from participants: one maintenance issue paralysed 600 ATM machines for 6 hours, and one innocent network scan in a manufacturing plant caused a large and powerful robotic arm to swirl around as if in rage, potentially injuring anybody near it.

Attacking such systems just got easier, for a number of reasons. One is that vulnerabilities are easier to spot. The search engine Shodan, dubbed the "Google for hackers," has made it easy to find turbines and breweries and large AC-systems that shouldn't be connected to the Internet but actually are. One project at the Freie Universität Berlin has enriched the Shodan data and put them on a map. The rationale of this "war map," as project leader Volker Roth called it tongue-in-cheek, is visualizing the threat landscape with colored dots, yellow for building management systems, orange for monitoring systems, and so on. The U.S. eastern sea board looks like a butt on a paintball range after a busy shooting session.

But so far, attackers have lacked either the necessary skill, intelligence, or malicious intention to use that map as a shooting range. That may be changing. While the more sophisticated ICS attacks are actually harder than meets the eye, many nation states as well as hackers are honing their skills. Some are also busy gathering intelligence; earlier this year, for example, the U.S. Army Corps of Engineers' National Inventory of Dams was breached, possibly from China. And any political crisis may change an attacker's intention and rationale to strike by cyber attack.

All of which keeps the federal government's main organization in charge of critical infrastructure protection busy. ICS-CERT employs between 80 and 100 staff, depending on contractors. Three of its activities stand out.

The first is incident response. At the request of asset owners, ICS-CERT can deploy so-called fly-away teams to meet with the affected organization. They'll review network topology, identify infected systems, image drives for analysis, and collect other forensic data. Last year, the government's control system experts responded to 177 incidents. That included 89 site visits and, in the most extreme cases, 15 deployments of on-site teams to respond to advanced persistent threat incidents in the private sector, the DHS told me. The fly-aways are controversial, with some critics pointing to a lack of focus and a waste of scarce government resources. One prominent critic is Dale Peterson of Digital Bond, a leading consultancy on critical infrastructure protection. "It doesn't scale," he says about the fly-away teams, "It's a band-aid." Still, a band-aid is better than no treatment at all.

The second main activity is keeping the operators vigilant and informed. ICS-CERT is doing this through vulnerability alerts and advisories: one recent alert, for instance, warned about a range of 300 medical devices that had hard-coded passwords, which could enable an attacker to gain remote access to surgical and anaesthesia devices or drug infusion pumps.

But for some, the warnings don't come fast enough, or don't produce a strong enough response. So more and more independent security researchers publish information on faulty design without notifying vendors and their clients first. Many at the Department of Homeland Security think some of these revelations are irresponsible or premature -- Digital Bond disagrees. The consultancy organizes a leading industry event, the S4 conference, where devices get hacked for good effect. A lot of people in the ICS community, Peterson tells me, "are getting gradually more aggressive because there has been so little progress."

Then there are those five-day-training sessions for those who are really at the front line of potential cyber attacks: the plant and factory owners and operators. That program is the least controversial. After three days of lectures and hands-on practice, and after one day of spilling chemicals by cyber attack, the participants in my class had a chance to discuss lessons learned on the fifth day. One or two may have expected a slightly different technical focus, yes, but the rest loved it. The Department of Homeland Security understood a crucial thing: if the asset owners understand the offense, they are able to improve -- and better invest in -- their network defense.

The reverse does not apply. The National Security Agency and its military twin, U.S. Cyber Command, are investing in all kinds of offensive measures that do nothing to make the nation's critical infrastructure more secure: They're discovering and buying previously unknown zero-day vulnerabilities -- holes in software that hackers can use to wiggle their way into a system. They're gathering target intelligence on foreign infrastructure, and clandestinely developing bespoke cyber weapons for high-profile attacks from Fort Meade. All of this may have theoretical benefits at some point. But such offensive investments do not translate into more efficient information-sharing at home, into safer logic controllers, or into better-trained asset owners. To the contrary: the offense can suck up skills needed on the defense. And while it would make all of us more secure to close up those software holes, the NSA and CYBERCOM would rather they stay open as avenues of espionage and attack.

One reason why, perhaps, is that, so far, there's only been one publicly-acknowledged destructive ICS attack anywhere, ever. The only successful cyber-sabotage strike that targeted control systems (and that was not an insider attack) was an American intelligence operation: the famous Stuxnet worm that targeted Iran's nuclear enrichment program in Natanz -- without achieving its goal. The White House, it seems, has learned some lessons from this episode. In a recently leaked secret document, the administration highlighted the "unintended or collateral consequences" of offensive cyber operations that may affect U.S. national interests. Apparently the White House sensed that Stuxnet had a counterproductive effect on "values, principles, and norms for state behavior." Cyber sabotage, they fear, could come back to haunt them.

In cyber security, it seems, a good offense is bad defense -- certainly made worse by sequestering the critical training of those who really keep the nation's infrastructure safe: the asset owners, engineers, and operators who make the monthly trek to Idaho Falls from all fifty states. Idaho National Labs has its own "war map" with red and blue and green and white pins: it's a large chart of the entire United States (and a smaller with allied nations), up in the first floor lunch area of the training facility. Every participant of the ICS training places a pin into their home town by sector: white if they come from the government, red for energy, blue for water, and so on. This is the map that really counts. The more dots and the more color, the better. But unless there's a radical change in how the U.S. secures its power plants and factories, there's never going to be enough push pins to stave off calamity.

Table of Contents

China Launches New Online Portal for Petitioners

From BBC News, 2 July 2013

China has started a new online platform to accept petitions from its citizens.

Officials say the website, which was launched by the State Bureau of Letters and Calls on Monday, will help "broaden the channels" for public opinion.

However, some potential users expressed fears that the website would be used to expose petitioners.

Chinese microblog users also raised questions about the effectiveness of the site after it reportedly crashed on its first day.

In China millions of people petition government offices every year, in a tradition that dates back to imperial times when the emperors would listen to the complaints of common people.

But these petitioners - whose grievances range from land disputes to employment violations to unsolved crimes - are often seen as an embarrassment to local officials, with some intercepted and detained illegally.

The State Bureau has accepted online complaints on agricultural issues, social welfare and construction before now. However, it says it will now accept complaints on all types of issues online.

The bureau chief, Shu Xiaoqin, said the department would take all online comments and complaints seriously, so that "all issues would be settled, all cases would receive a reply".

The move was "an effort to improve the bureau's credibility" and "continue to broaden the channels through which public opinion could be expressed," she was quoted in Chinese media reports as saying.

'Fishing exercise'

Continue reading the main story“Start QuoteWould you dare submit a petition on this website?”

Ma JuncaoWeibo user

However, the site requires users to register their details, including their real name, ID or passport number, home address and telephone numbers, leading some to fear that petitioners could face retribution from local officials.

"Would you dare submit a petition on this website?" Ma Juncao wrote on Sina Weibo, a Chinese microblog similar to Twitter. "Opening up online reporting is a good thing, but what's the point of asking for people's address? Maybe so they can retaliate against you."

Another user, Tears in Snow, described the website as a "fishing" exercise.

Many Chinese microblog users also expressed scepticism about the effectiveness of the site, after reports it crashed on its first day due to the high volume of visitors.

"The state bureau allows online complaints... and then the website crashed," Sina Weibo user Maxims and Smart Words said.

"It looks like there are a lot of grievances from citizens!" OscarUI, another user, wrote.

Online users also said they noticed errors on the site, which reportedly listed Monday's date as "1 July 19113", and were unhappy that the portal was only compatible with the Internet Explorer browser.

"It feels like the State Bureau weren't sincere enough when they made this site," user i Gao Haobo wrote on Sina Weibo.

"People may feel hopeful [when they learn about the new portal], but when you see the date of the website it's obvious that you're just being conned," user Hai Lan Lan said.

Table of Contents

How the Nature of Warfare is Changing in the Information Age

By Rear Admiral James H. Rodman Jr., FedTech Magazine, July 26, 2013

"A revolution is an idea that has found its bayonets." — Napoleon Bonaparte

History is never kind to warriors who miss tectonic shifts in warfighting doctrine. That is especially true when the shifts are caused by breakthroughs in technology. Just ask the soldiers at Gettysburg felled by newly rifled muskets or the infantrymen overtaken by the treads of lightning-fast armored vehicles. These shifts typically follow major changes in global economic focus — revolutions where the old order is swept away and replaced by new norms, new powers and new bayonets.

The digital revolution known as the Information Age quietly arrived in the late 1970s as computer miniaturization took root and proliferated through the industrial economy. Mechanical systems were quickly modernized or replaced by digital devices that made almost every task easier, from remotely monitoring and controlling industrial equipment to flying jet aircraft. Software became its currency, and the Internet its enabler. Networking technology expanded its global reach into every facet of society. The Navy was not immune: Digital systems transformed the way we think about, plan for, defend and fight the nation's wars.

The revolution is here. It is time to hone our cyber bayonets.

Data Creates Opportunities and Challenges

Cyberpower fundamentally changes the nature and focus of modern warfare. It provides both opportunity and vulnerability, and we have to man, train and equip Navy forces to deal with both simultaneously. Let's focus first on opportunity. Cyber provides a nonkinetic means to deny, degrade, disrupt or even destroy an adversary's ability to fight and function. Bits instead of bombs can render an adversary's command and control, critical infrastructure or logistics useless — without firing a shot. We have to redesign the way we think about warfighting doctrine and operational planning to fully integrate cyber into the combat commander's arsenal.

Bits instead of bombs can render an adversary's command and control, critical infrastructure or logistics useless — without firing a shot.

The U.S. Cyber Command and Navy mission partner Fleet Cyber Command/10th Fleet are performing that redesign today. At the same time, cyber opens unlimited possibilities in information superiority. As technologies rapidly evolve, we can tap the potential to share, integrate and utilize data in unimaginable ways. Our warfighters will see more, hear more and know more than our adversaries, giving us an asymmetric advantage on the battlefield. The Navy's Information Dominance Corps was established to leverage that technology promise, but at the very core, every soldier, sailor, airman, Marine and Guardsman is a cyberwarrior. We have to think that way; we have no other choice.

New Threats Surface in the Information Age

There is a dark side, however, because the cyber vulnerabilities we exploit are the same vulnerabilities we have built into our own systems. From the microchip to the operating system, cyberthreats abound and proliferate at lightning speed among nation-state actors, terrorist cells, organized crime syndicates, hackers and others. Some of the threats we see and thwart — but some are clandestine, hidden in the digital clutter -performing their covert thievery or just waiting for the right moment or vulnerability to strike. Our cyberdefense strategy must deal effectively with both. We need to think differently about the way we eye, buy and fly our cybersystems, so defense is agile, adaptable and built in from the ground up.

The Space and Naval Warfare Systems Command and the other Navy systems commands are knee-deep in that fight. By adopting a common defense-in-depth framework and enforcing information assurance through expanded technical authority, we are starting to address the fundamental cyber issues that exist in Navy systems. We are also working closely with resource sponsors to align funding to the biggest cyber risk areas. It is a long fight, but one we absolutely must win to ensure the Navy survives and thrives in the Information Age.

Table of Contents

Tweet Offensive: Social Media Is Israeli Military's Newest Weapon

By Michael Borgstede, DIE WELT/Worldcrunch, 21 July 2013

TEL AVIV - Avital Leibovich's business card contains all the usual information: name, rank (lieutenant colonel), position. She is head of the Israel Defense Forces' Interactive Media Branch, and in addition to listing her phone numbers and email address, the card also includes some less traditional data: her Twitter address and Facebook page.

Working out of a modest office building in Tel Aviv, Leibovich and her team of 30 soldiers are responsible not only for the social network presence of Israel's armed forces — the IDF — but also for making sure that it makes a good impression.

"We are the only army in the world that puts this much effort into an Internet media offensive," she says with pride. Several hundred postings in six languages are made to nearly all social networks and a blog every month.

The endeavor began small during the Gaza War in late December 2008 when a conscript had the idea of making some filmed content available to the media on YouTube. It was a great success, and not just with journalists.

Today, everything from aerial shots of targeted killings to a short introduction in English to Krav Maga (a self-defense system developed in Israeli based on martial arts) can be found on YouTube. When an Israeli F-16 jet fighter with a technical defect crashed, it was only a matter of hours before video of the dramatic IDF rescue of the pilot and navigator was posted.

Viewer figures for some videos are out there for all to see. The short clip showing how militant Hamas leader Ahmed Jabari was killed in an Israeli air attack on his car was viewed nearly five million times. But even unspectacular videos, like one sending messages of goodwill to those in the Arab world observing Ramadan, can appeal to large numbers of viewers, says Leibovich.

So far, there are pages and channels in Hebrew, English, French, Russian, Spanish and Arabic, she explains. And postings on each one are different. New immigrants to Israel are usually in charge of these not only because they speak the language of the target group but because of their intuitive understanding of their native culture and therefore the approach to take when presenting content.

Knowing your audience

In a large office space, three soldiers are discussing the best way to present a statement in Arabic from Hassan Nasrallah, leader of the Lebanese Shi'ite militia Hezbollah. Two of the women soldiers migrated to Israel from Egypt seven years ago, and now, in Arabic, they're trying to give the Arab world another picture of the IDF.

One young female soldier in charge of the Russian Facebook page points out that in Russia the VK social network is at least as important as Facebook "so of course we're present there too." In general, Russians like hardcore military information, she says, and weapons and explosions are not at all taboo. The titles on their Russian YouTube channel therefore depict a rocket being fired, though this wouldn't be a good idea on the French channel, which instead shows two soldiers in camouflage clothing.

"We like to play up the human angle," a soldier named Anthony says — stories about new immigrants from France serving in the Israeli army, for example. Or showing a pretty girl in uniform with a caption reading, "The true face of the IDF."

But these postings don't come at the expense of news and political coverage. When rockets from Gaza hit the southern part of the country, the news was on Twitter in nearly real time. The number of relief trucks admitted to the Gaza strip every month is presented as an infographic, and just recently a new webpage with information about the history, ideology and terrorist activities of Hezbollah were posted.

Using the example of a village in southern Lebanon, they show how Hezbollah deliberately stockpiles weapons near schools and medical facilities. Programmers and layout designers spent over six months on the project.

The Israeli armed forces have often felt mistreated by the international media, and it has been a sore subject for a long time. So the online offensive is intended to reach people directly by bypassing traditional media as transmitters of information. How well it works is difficult to assess.

Comments that IDF postings receive on social networks are mostly from two groups: those who consider Israel's forces to be treacherous murderers selling a pack of lies, and those who regard Israeli soldiers as heroic.

Lieutenant Colonel Leibovich and her soldiers firmly believe that their efforts haven't been in vain. Leibovich waxes enthusiastic about her subordinates' creativity. "These are 19-year-olds! They've grown up with this technology and have integrated it — internalized it — completely." They believe that the Internet is the battlefield of the future.

Sometimes the verbal sparring does feel like a battlefield. During the most recent Gaza offensive in November 2012, the Israeli army tweeted a warning to all Hamas leaders not to "show their faces above ground in the days ahead."

They got a swift reply from @AlQassamBrigade, the militant wing of Hamas: "@IDFspokesperson — Our blessed hands will reach your leaders and soldiers wherever they are (You Opened Hell Gates on Yourselves)."

Table of Contents

Cyber Attacks in Space

By Tal Inbar, Israel Defense, 29/7/2013

The cyber realm in general and cyber warfare in particular have gained a position of prominence in public-defense discourse in recent years. They are often linked to nearly every field of activity, whether a connection exists or whether such a connection is very feeble indeed. One of the fields regarding which this linkage is made often is space – where the connection between cyber terrorism threats and actual damage to space-borne assets is very direct.

In recent years, it has become clear to anyone involved in this field that space-borne assets can be damaged in various ways, including the option of inflicting damage on the computers that command the satellites, and not necessarily on the computers onboard the satellite. Cyber attacks may be staged against the ground station controlling the satellite and dictating its operation, thereby damaging the system located in space, hundreds or thousands of kilometers above the earth.

A system-wide vulnerability may be identified here, and the ground control stations may be damaged in various ways. At this point, and in all probability in the foreseeable future as well, only the superpowers possess the ability to inflict serious damage on satellites. So far, only three states have demonstrated the ability to physically damage satellites by intercepting them: Russia, the US and China.

In order to overcome cyber attacks against satellites – and the more satellites a country operates, the greater the potential damage an attack can inflict – it should be understood that the damage inflicted by a cyber attack is not confined to the results of information and data having been stolen. It can have a physical manifestation, namely the damage inflicted on the satellite can be real, up to complete destruction. A scenario may be described where a state or a non-state organization dominates a satellite control channel and causes the satellite to activate its maneuvering engines in a way that would cause it to lose altitude and burn off upon reaching the atmosphere.

The damage can also have an ‘awareness’ effect, namely someone gaining access to a satellite control channel and executing some harmless operations merely to demonstrate their ability (US spokespersons have attributed such incidents to the Chinese, who had staged a cyber attack against a Norwegian ground station out of which NASA satellites were controlled).

Every satellite operating in space relies on communication with the ground (or with a naval or aerial platform). This communication may also be disrupted in order to interrupt the normal functioning of the satellite. Using the cyber attack option, satellite operation may be interrupted by attacking the electrical power infrastructure supplying power to the ground section of space-borne systems.

Another way to attack satellites (as well as other products) is by inserting fake components into the system so that it will contain a hostile element, while the satellite operators remain unaware of this fact (this opens a ‘back door’ through which the perpetrator can access the system and perform various operations therein). In the US, the authorities found thousands of fake components (mainly chips) intended for installation in the next generation of US navigation satellites.

Attacks against satellites are lucrative to states and other players, as in many cases the source of the attack is very difficult to trace. On the other hand, the databases containing information about the orbits of communication satellites or satellites in even lower orbits are not classified, and any smartphone user can view the positions of those satellites on the display screen of his smartphone, with the display updated at 30-second intervals. As the locations of satellites and the frequency ranges they use cannot be concealed, a greater emphasis should be placed on the physical protection of ground control stations (and on concealing the backup stations), as well as on preventing the leakage of information from the satellite manufacturers.

In order to defend against cyber attacks on satellites, awareness must be heightened among members of the space community, developers and consumers. Furthermore, tests must be added for immunity to such attacks as an integral part of the tests satellites undergo during the manufacturing process, before being launched into space. The aforementioned measures should complement the introduction of diversified protective elements, on board the satellites as well as in the ground stations controlling them.

The employment of multiple satellites will enable redundancy in the event of a cyber attack. A costly but feasible recovery concept can include the use of launching by demand, using standby satellites and a launcher that may be readied for launching at short notice. This concept was theoretically developed in the US primarily, but it has not yet been implemented. Moreover, methods for managing the satellite layout intelligently and backup provided to the ground control stations will contribute to the reinforcement and strengthening of the satellite layout against various types of cyber threats.

Table of Contents

Moscow Subway to Use Devices to Read Data on Phones

From Radio Free Europe/Radio Liberty, July 29, 2013

The head of police for Moscow's subway system has said stations will soon be equipped with devices that can read the data on the mobile telephones of passengers.

In the July 29 edition of "Izvestia," Moscow Metro police chief Andrei Mokhov said the device would be used to help locate stolen mobile phones.

Mokhov said the devices have a range of about 5 meters and can read the SIM card.

If the card is on the list of stolen phones, the system automatically sends information to the police.

The time and place of the alert can be matched to closed-circuit TV in stations.

"Izvestia" reported that "according to experts, the devices can be used more widely to follow all passengers without exception."

Mokhov said it was illegal to track a person without permission from the authorities, but that there was no law against tracking the property of a company, such as a SIM card.

Based on reporting by "Izvestia" and ITAR-TASS

Table of Contents

Online Jihad

By Arnaud De Borchgrave, UPI, Aug. 7, 2013

WASHINGTON, Aug. 7 (UPI) -- The enemy now knows that a simple message of disinformation about a major al-Qaida terrorist operation will close U.S. embassies from North Africa to the Middle East to the Arabian Peninsula.

We can't seem to remember elementary information about al-Qaida's modus operandi. The Middle East Media Research Institute, monitoring media reports from Washington, reminds us al-Qaida and its many associated movements, from Nigeria clear across the African continent to Somalia and on to Yemen, Syria, Iraq, and Pakistan, live online.

Al-Qaida terrorists proselytize online, plan online encoded prayers, tweet, post images on Instagram, and last, but by no means least, they are skilled players of disinformation -- the ability to take a kernel of truth and wrap it with a tissue of half-truths and lies.

Mercifully, the National Security Agency has big global eyes and ears that pay little heed to the claptrap about individual rights going down the proverbial tube. If one of our news sources happens to be an al-Qaida operative in the disinformation game wouldn't we like to know?

The current conflict in Syria, MEMRI points out, "highlights the global jihad movement's total dependence on the Internet and on U.S.-based social media companies."

Hello? Have we already forgotten about the Internet's multipurpose global reach?

About one-third of humanity is on the worldwide 'Net and by 2015 China will outstrip the United States in Internet and social media use. At 27 percent of total Internet users, English is still the dominant language, a slight lead over Chinese with 24 percent.

Spanish is in third place with 8 percent.

The use of social media in the Syrian civil war demonstrates the global jihad movement's total dependence on the Internet and on U.S. social media companies, says MEMRI.

Other points made by the research organization:

-- Skype is being used by the jihadi group Al-Haq Brigade (part of the Syrian Islamic Front) to recruit for the Al-Ansar Battalion training camp.

-- Jihadis fighting in Syria use Facebook, YouTube and Twitter to communicate, plan attacks, raise funds and keep in touch with family and friends.

-- Circulate death pictures and eulogies for jihadis killed in action.

-- A eulogy posted on Facebook for Abu Qasura Al-Tunisi, a Tunisian from the al-Fallujah forum who traveled to Syria to fight alongside the al-Qaida-affiliated Jabhat al-Nusra noted: "He joined jihad with no help but Allah and Google Earth."

-- Flickr, for Internet photo sharing, is widely used by jihadis for recruitment propaganda.

-- Foreigners "martyred" in Syria were on YouTube and Flickr. They included "martyrs" from Australia, Albania, Azerbaijan, Algeria, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Saudi Arabia, Yemen, Tunisia, Turkey, the United Arab Emirates, Bahrain, Dagestan, Chechnya, France, Ireland, Sweden, Spain, the United States, United Kingdom and Denmark.

-- Typical examples from 360 photos on Flickr: "Rafael Gendroun, martyr from France, was martyred April 14, 2013. He was a member of the Syrian Hawks Brigade in northern Syria."

-- "Sammy Salma, Melbourne, Australia, martyred on the outskirts of Aleppo April 17, 2013."

-- "Mohammed Ali Abu Hammur, Salt, Jordan, martyred April 15, 2013, a Swedish resident."

-- "Hasam Al-Sham, a French national of Lebanese origin. God gave him abundant knowledge ... in forensics, military and political analysis ... At dawn Wednesday, the sixth day of Ramadan, he was wounded in a bombing in one of the suburbs close to the Lebanese-Syrian border and was martyred immediately."

-- Nu'man Damoli, a martyr from Kosovo, fighter of Kosovo's Liberation Army against the Serbian army, was wounded in the mountains of Kosovo in 1999. Thirteen years later he joined the mujahedin of the al-Nusra Front in Syria to fight against the Assad regime, and martyred in one of the battles of Talbisah (Homs province) on Nov. 8, 2012.

MEMRI reports that the Flickr account, which was opened in February before the Facebook page was shut down, includes 360 photos of martyrs (most of them included in this latest report).

The "mujahedin" who were killed in action in Syria were recruited directly or indirectly by al-Qaida and its Associated Movements. Many of them are Arabs who immigrated to Western countries.

The Syrian civil war, now in its third year, has claimed more than 100,000 killed. The country is no longer a unitary state and is divided into roughly three parts.

Sunni-led al-Qaida volunteers have come in from Lebanon and Turkey. The Syrian regime is led by Bashar Assad, 43, whose Alawite sect is affiliated with Shiite Islam (i.e., Iran).

Saudi Arabia, the United Arab Emirates and Qatar have lined up behind the revolutionaries. The fact that al-Qaida and its affiliated groups play a key role on the same side is less important to them than the fact the Assad regime is closely allied with Shiite Iran.

The Obama administration would be wise to resist the temptation to become engaged beyond arms aid to the anti-Assad camp. Hard to figure out the good guys in the anti-Assad camp.

In any event, the unitary state of Syria appears to be headed for some kind of de facto partition.

In Egypt, where wise heads prevailed and pulled Egypt back from the edge of civil war, U.S. Sens. John McCain, R-Ariz., and Lindsey Graham, R-S.C., breezed into Cairo – and pushed the country back to the edge.

Release Egypt's Islamists, the senators said peremptorily. "Delusional" and "a blatant interference in Egypt's internal affairs," they were told. "Threatening to suspend U.S. aid is tantamount to blackmail ... a condescending lecture, as rude as it was shallow."

"Uncouth and ignorant about all things concerning Egypt," said an official spokesman.

Now Egypt is considering canceling yearly military maneuvers with the United States. And a new movement has been launched -- "To Hell With U.S. AID."

Table of Contents

If The Chinese Army Is Trying To Hack A Missouri Water Plant, What Else Is It Infiltrating?

By Gwynn Guilford, Quartz, August 6, 2013

The question of whether the Chinese military is on a hacking offensive has largely been answered—and, despite Chinese government protestations, it sure looks like a pretty big “yes.” However, beyond the widely reported infiltration of foreign companies, the question of what else it’s hacking remains hazy.

But new research confirms one of the scarier possibilities: that the Chinese army is going after critical US infrastructure.

This all came out of a project by Kyle Wilhoit, a researcher at a security company called Trend Micro, that set up decoy “honeypots,” as decoy infrastructure systems are known, in 12 different countries. Wilhoit’s construction of a rural Missouri water plant honeypot attracted the notorious APT1, a crackerjack Chinese military hacking team sometimes known as Comment Crew, according to research he presented at the Black Hat security conference in Las Vegas. The group gained access in December 2012 through a Microsoft Word document containing malware unique to APT1.

“I actually watched the attacker interface with the machine,” he told the MIT Technology Review, referring to APT1. “It was 100% clear they knew what they were doing.”

Wilhoit noted to CBSNews.com that systems like power grids and water plants are inherently vulnerable to hacking threats because they’re using outdated technology and don’t necessarily prioritize security. Of the “critical” honeypot attacks—meaning those that could have taken control of the system—half came from China. Examples include turning the pump’s water temperature to 130° Fahrenheit and shutting down the system.

This suggests that Chinese hackers are taking control of critical infrastructure. ”These attacks are happening and the engineers likely don’t know,” Wilhoit told MIT Technology Review. Here’s a look at APT1′s past activity:

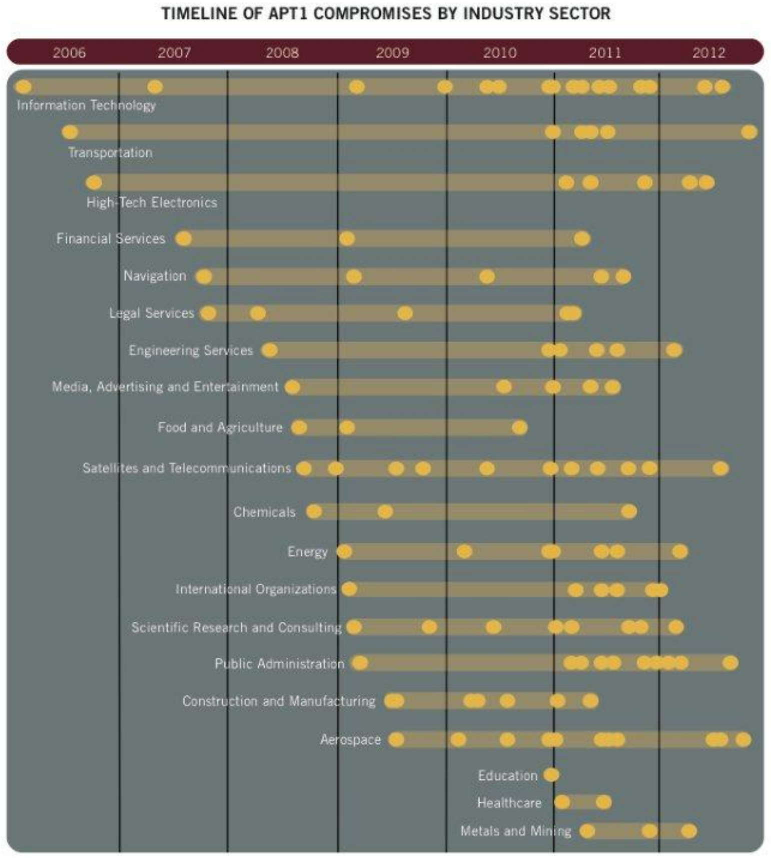

FIGURE 12: Timeframe of APT1’s cyber espionage operations against organizations by industry. The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry.

Mandiant

To date, the only publicly disclosed cyberattacks on US control systems have been on a factory and a state government building, both in New Jersey, reports MIT Technology Review. It’s unclear where those attacks originated.

Table of Contents

NSA Leaks Make Plan for Cyberdefense Unlikely

By Christopher Gregory, New York Times, August 12, 2013

WASHINGTON — Even while rapidly expanding its electronic surveillance around the world, the National Security Agency has lobbied inside the government to deploy the equivalent of a “Star Wars” defense for America’s computer networks, designed to intercept cyberattacks before they could cripple power plants, banks or financial markets.

But administration officials say the plan, championed by Gen. Keith B. Alexander, the director of the National Security Agency and head of the Pentagon’s Cyber Command, has virtually no chance of moving forward given the backlash against the N.S.A. over the recent disclosures about its surveillance programs.

Senior agency officials concede that much of the technology needed to filter malicious software, known as malware, by searching incoming messages for signs of programs designed to steal data, or attack banks or energy firms, is strikingly similar to the technology the N.S.A. already uses for surveillance.

”The plan was always a little vague, at least as Keith described it, but today it may be Snowden’s biggest single victim,” one senior intelligence official said recently, referring to Edward J. Snowden, the former N.S.A. contractor who released documents revealing details of many of the agency’s surveillance programs.

“Whatever trust was there is now gone,” the official added. “I mean, who would believe the N.S.A. when it insists it is blocking Chinese attacks but not using the same technology to read your e-mail?”

On Friday, the N.S.A. reported for the first time that it “touches about 1.6 percent” of all the traffic carried on the Internet each day. In a statement, it said it closely examines only a tiny fraction of that information. But General Alexander’s plan would put the agency, or Internet-service providers acting on its behalf, in the position of examining a far larger percentage of the world’s information flows.

Under this proposal, the government would latch into the giant “data pipes” that feed the largest Internet service providers in the United States, companies like A.T.&T. and Verizon. The huge volume of traffic that runs through those pipes, particularly e-mails, would be scanned for signs of anything from computer servers known for attacks on the United States or for stealing information from American companies. Other “metadata” would be inspected for evidence of malicious software.

“It’s defense at network speed,” General Alexander told a Washington security-research group recently, according to participants. “Because you have only milliseconds.”

This summer, the N.S.A. has begun assembling scores of new cyber “offense” and “defense” teams, the agency’s most concrete step toward preparing the Pentagon and intelligence agencies for a new era of computer conflict. Erecting a national cyberdefense is a key element of that plan. At an interagency meeting that discussed the flood of cyberattacks directed daily at American networks, from Chinese efforts to steal corporate secrets to Iranian efforts to cripple financial institutions, General Alexander said, “I can’t defend the country until I’m into all the networks,” according to other officials who were present.

The appeal of such a program is its seeming simplicity: The worst malware could be blocked before it reaches companies, universities or individual users, many of whom may be using outdated virus protections, or none at all. Normal commercial virus programs are always running days, or weeks, behind the latest attacks — and the protection depends on users’ loading the latest versions on their computers.

The government has been testing a model for a national defense against cyberattack with major defense contractors including Lockheed Martin, Boeing and Raytheon. Early results were disappointing, but participants in the program — the specific details of which are heavily classified — say they are getting significantly improved results. Each company in the defense industrial base program now shares data on the kinds of attacks it is seeing, anonymously, with other participating companies.

But for the N.S.A., which is building a target list of servers used by the most aggressive cyberattackers, monitoring all Internet traffic would also be an intelligence bonanza. It would give it a real-time way to watch computer servers around the world, and focus more quickly on those it suspects are the breeding ground for governments or private hackers preparing attacks.

Even before the Snowden revelations, General Alexander had encountered opposition. Top officials of the Department of Homeland Security, which is responsible for domestic defense of the Internet, complained that N.S.A. monitoring would overly militarize America's approach to defending the Internet, rather than making sure users took the primary responsibility for protecting their systems.

The deputy secretary of defense, Ashton B. Carter, described in speeches over the past year an alternative vision in which the government would step in to defend America's networks only as a last line of defense. He compares the Pentagon's proper role in defending cyberattacks to its "Noble Eagle" operation, in which it intercepts aircraft that appear threatening only after efforts by the airlines to identify the passengers and by the Transportation Safety Administration to search passengers and luggage have failed.

It appears unlikely that, with the administration divided, and faced with a backlash against the N.S.A. in Congress, any proposal for a formal plan for national cyberdefense will be submitted soon. Members of the Intelligence Committees in the House and Senate said that they were only vaguely aware of General Alexander's plan, but that it would almost certainly require Congressional approval.

That is a fight the White House is not interested in having while it struggles to get a much more modest cybersecurity bill through Congress after years of arguments over privacy concerns and corporate America's fears that Washington will dictate how companies protect data and how much they must spend on new defenses. The bill failed last year, and passage this year appears in doubt.

Before the Snowden revelations, General Alexander's idea appeared to be gaining some ground because of concerns over the cyber-enabled Chinese theft of critical corporate secrets, including some designs for the F-35 Joint Strike Fighter. Internal intelligence reports, based on N.S.A. analysis, attributed an attack on American banks to Iran's cybercorps, a unit of the Revolutionary Guards.

"After the Iranian attacks, we were looking at these ideas pretty hard," said a recently departed senior official in the Obama national security team, who like other officials declined to be identified because of the sensitivities of the government's discussions about building Internet defenses.

But this summer, the mood in Congress has changed. The White House only narrowly avoided a House vote to cut off the collection of metadata about telephone calls in the country. Suddenly a national debate emerged; along the way the N.S.A. admitted that until 2011 it had collected about 1 percent of all e-mails in the United States, until the program was canceled after being judged ineffective.

"Cyberissues usually change so rapidly because of the advance of technology," said Peter D. Feaver, a Duke University professor who worked in the National Security Council in the George W. Bush administration.

"But the biggest change in the last year has been political: Public skepticism about U.S. cyberoperations is dramatically higher today, and it could result in political constraints that were off the table even a year ago."

Table of Contents

Winning without Fighting: The Chinese Psychological Warfare Challenge

By Dean Cheng, the Heritage Foundation, 12 July 2013

Abstract

Beijing hopes to win future conflicts without firing a shot. How? By using psychological warfare to manipulate both a nation's leaders and its populace—affecting the thought processes and cognitive frameworks of allies and opponents alike. Indeed, the PRC's psychological warfare operations are already underway despite the fact that there is no active conflict. It is therefore essential that the United States counter such psychological operations now while preparing to use its own arsenal of political warfare weapons should a conflict ever arise.

One of the elements distinguishing the Chinese People's Liberation Army (PLA) from many of its counterparts is its continued role as a Party army. The PLA is, first and foremost, the armed wing of the Chinese Communist Party (CCP). This distinction both obligates the PLA to help maintain the CCP's grip on power and gives it an additional set of tools with which to defend the CCP and the Chinese state. At the moment, the PLA is not only planning for operations on the physical battlefield; it is also preparing to conduct "political warfare," including what is termed the "three warfares": public opinion warfare, legal warfare, and psychological warfare.

Psychological warfare is in some ways the most far-reaching of the "three warfares." It involves the application of specialized information and media in accordance with a strategic goal and in support of political and military objectives.[1] Such efforts are aimed at a variety of potential audiences and usually involve operational missions against an opponent's psychology and cognitive capacities. Specifically:

There are myriad targets and objects of psychological warfare; it is applied against the enemy, but also against friends; it targets externally, but also internally; it must deal with allied countries, but also the entire globe, and one must rely on the media acting in multiple directions jointly, with effective coverage of many areas, in order to comprehensively realize the various goals.[2]

The goal of psychological warfare is to influence, constrain, and/or alter an opponent's thoughts, emotions, and habits while at the same time strengthening friendly psychology.[3]

Psychological Warfare and Information Warfare

Psychological warfare operations are integral to the broad concept of information warfare (xinxi zhanzheng). A product of the Information Age, information warfare is the struggle to dominate the generation and flow of information in order to enhance and support one's own strategic goals while degrading and constraining those of an opponent. The ability to triumph in future "Local Wars Under Informationized Conditions"—the most likely form of wars in the Information Age—rests upon the ability to secure "information dominance (zhi xinxi quan)." This in turn requires the ability to collect, manage, and exploit accurate information more quickly than an opponent.

Information dominance rests on two primary factors: modern information technology, which is integral to information collection and transmission, and the ability to degrade the quality of information, whether by slowing down transmission or by introducing false or inaccurate data. But in the Chinese conception of psychological warfare, the users of information—both high-level decision-makers and lower-level policy implementers (individual soldiers, clerks, etc.)—are as important as the computers and networks and the software that runs them. Efforts to secure information dominance, therefore, will target not only the physical information infrastructure and the data that pass through it, but also the human agents that interact with those data, especially those who are making decisions.

Given the nature of modern technology and informationized societies, operations designed to influence a rival nation can no longer be aimed solely at military leaders or reserved for wartime. The interconnected nature of information, as well as information systems, makes clear-cut classifications of "military" and "civilian" almost impossible. Similarly, information collection, and even exploitation, is not necessarily restricted by "wartime" versus "peacetime" categorizations. As one Chinese volume observes, information warfare is constant and ongoing, whether in wartime or peacetime. Because of the complex, intertwined nature of modern international politics and economics:

> [I]t is necessary in peacetime to undertake information warfare in the political, economic, technical, and military realms, as only then can one scientifically establish operational plans, appropriately calculate gains and losses in a conflict, appropriately control the level of attack, precisely strike predetermined targets, and seek the best strategic interest and long-term benefit.[4]

This philosophy is echoed in other PLA writings, which emphasize that modern information technology blurs the lines between peacetime and wartime, between military and civilian, and among strategy, operations, and tactics.[5] Rather than trying to draw artificial boundaries among these categories, the implication is that information should be treated as an integrated whole.

In this context, psychological operations are seen as an essential part of future conflicts, affecting the very perceptions that inform decision making, from the context to the biases. Successful psychological operations will therefore have repercussions at every level of operations, influencing the course of the conflict. To be effective, however, psychological warfare operations cannot be limited to wartime. Instead, peacetime psychological operations are necessary, both to understand an opponent better and to lay the groundwork for effective wartime operations.

Peacetime applications of psychological warfare techniques involve influencing and altering an opponent's unconscious, implicit views in order to make that opponent more susceptible to coercion. By employing various forms of strategic communications, including diplomatic efforts, one can foster a positive national image and increase foreign sympathy and support for one's own policies and goals. At the same time, such techniques attempt to isolate opponents, undermining their positions, portraying them as fostering ill intentions, and forcing them to react to a variety of charges so that their energy is dispersed.

In addition, employing all the tools of communications, including various forms of media, emphasizes one's own strengths as well as a willingness to employ that strength to deter and coerce opponents more effectively. All the while, one must be working to counter opponents' efforts to foster their own image of strength and unity. It is also likely that an opponent will attempt to demoralize one's populace and that appropriate defensive measures will have to be taken.

In wartime, psychological operations shift emphasis towards more specifically military targets and goals. The primary objective of such efforts is to generate confusion, doubt, anxiety, fear, terror, regret, and exhaustion in an opponent, especially among senior military and civilian leaders. Ideally, such a campaign will induce neglect and maximize the chances of an opponent making mistakes. Wartime psychological warfare operations also aim to generate a sense of uncertainty and indecisiveness at all levels, thereby degrading opposition decision-making processes. The ability to interfere with an opponent's information systems, coupled with efforts to influence decision makers, can create a strong psychological impact.

Another facet of wartime psychological operations is the sowing of discord and a sense of hopelessness in the enemy. Not only will this help generate war-weariness among enemy forces and populations and discourage resistance, but once the conflict is concluded, such operations may facilitate peace negotiations and induce more concessions. "When one defeats the enemy, it is not solely by killing the enemy, or winning a piece of ground, but is mainly in terms of cowing the enemy's heart."[6] In order to undermine the opponent's morale, one must emphasize information favorable to oneself through various forms of media as well as through third parties, friendly elements in the opponent's society, and similar outlets.

Finally, offensive psychological warfare operations must be complemented by defensive measures, since an opponent will also be trying to undermine one's own forces, population, and leaders. One must therefore attempt to solidify popular support for the conflict, highlight one's successes and the enemy's failures, and instill confidence and support for the Party and the state. Such defensive measures require tight control of information flows in one's own society and the insulation of one's decision-makers and decision-making processes from enemy information warfare efforts. This need for control explains Beijing's efforts to limit cyber access to the larger population, including the "Great Firewall of China."

Chinese Concept of Psychological Warfare Tasks

For the PLA, psychological warfare is the resposibility of the General Political Department (GPD), working in coordination with the rest of the PLA. The GPD not only ensures political orthodoxy within the PLA, but also is responsible for maintaining morale, personnel administration (e.g., assessing promotions), and countering psychological warfare attacks. As one of the four "General Departments," its purview covers the entire PLA, and its authority is second only to the war planners of the General Staff Department (GSD).

The "three warfares" of psychological warfare, legal warfare, and public opinion warfare are part of the GPD's responsibility as laid out in the 2003 and 2010 "political work regulations" of the PLA. For the GPD, Chinese writings suggest that there are five broad tasks associated with psychological warfare.[7]

- Presenting One's Own Side as Just. Winning future wars will require efficient political mobilization. Failure to mobilize the populace will make them vulnerable to war-weariness and moral collapse such as occurred in the 1990s Balkan conflicts. Consequently, the foremost role of psychological warfare is to emphasize the justice of one's cause, for only by portraying one's own goals as just and the enemy's as unjust can one hope to secure popular support and garner international sympathy and aid.[8] At the same time, successfully inculcating one's own population and forces with a sense of a just cause will reduce the effectiveness of enemy propaganda and allow them to weather the inevitable setbacks associated with any conflict.

- Emphasizing One's Advantages. Psychological warfare is intended to support larger diplomatic, political, economic, and military ends. Consequently, it is essential to emphasize one's own advantages in each of these respects. Such emphasis will bolster the confidence and will of one's own side while simultaneously influencing the other side's perceptions. In this regard, propaganda efforts—part of public opinion warfare—will extend beyond the superiority of one's military forces and equipment to note advances in science and technology, culture, and economic capacity.

- Undermining the Opposition's Will to Resist. This is one of the fundamental tasks of wartime psychological warfare. Because the will of an enemy is a key determinant of ultimate victory, it is essential to degrade his morale and unravel his alliances and support from third parties. Psychological warfare efforts must therefore not only bolster one's own side, but "cause the enemy to lose heart and disperse, so that even though they appear whole, they cannot exploit that." Such a campaign can involve such diverse measures as implementing policies of benign treatment of prisoners (to promote a willingness to surrender) and developing base areas in the enemy's rear (to make the enemy feel constantly insecure).

- Encouraging Dissension in the Enemy's Camp. This task is distinct from the previous one, insofar as such measures are more indirect than those associated with undermining the opposition's will to resist. Instead, sparking dissension involves fostering anti-war elements and encouraging war-weariness. Such an approach is similar to the creation of "united front" tactics, wherein various local elements within the opponent's camp are unified against the leadership without necessarily being openly supported by the PRC.

- Implementing Psychological Defenses. Since psychological warfare can have such far-reaching impacts, in the Chinese view, it is assumed that an opponent will mount psychological attacks. Consequently, in addition to negating or neutralizing such attacks, it is necessary to expose them, both to defeat them and to demoralize an opponent by demonstrating the ineffectiveness of his efforts. Thus, not only must there be counter-propaganda activities, but one must also publicize enemy machinations and techniques, thereby exposing and highlighting their futility.

It is worth noting that none of these tasks is necessarily limited to actual wartime. Erecting psychological defenses, fostering efforts to bolster popular and military support for the Party's leadership, and emphasizing the justness of one's own cause are all long-term endeavors that can be undertaken in part in peacetime.

Principles Governing Psychological Warfare Operations

Chinese analyses of military affairs are informed by the idea of military science; i.e., that there is a proper scientific approach to the analysis of military affairs. This method entails identifying underlying principles that govern individual aspects of military operations, including those aimed at fulfilling the key tasks of psychological warfare operations.

- Principle #1: Maintain direction. The principle of direction refers to the need to follow the Party's direction and leadership, incorporating its commands regarding policies, parameters, and limitations into all psychological warfare activities—whether strategic, operational, or tactical and whether aimed at foreign or domestic audiences. It closely parallels the military axioms of unity of command and effort. The principle of direction dictates that psychological warfare activities should be planned and assessed based on (1) their support of broad national interests and goals, (2) their relation to specific political and diplomatic efforts, and (3) their support of integrated operational military activities. Direction is achieved through unified, integrated command and operational implementation—something facilitated by the existence of the GPD, which spans the entire PLA.

- Principle #2: Adopt a systematic approach. Psychological warfare is not a single instance or even an accumulation of instances, but must instead be organized and integrated into a systematic, coherent whole. This approach requires coordination of psychological warfare operations between higher and lower levels so that the resulting unified construct will have maximum impact. Such coordination in turn requires that psychological warfare be tailored against opponents: There cannot be a "one size fits all" mentality. Rather, the character of the implementing force, as well as of the intended targets, must be taken into account with a suitable division of labor among the various components. The psychological warfare effort, moreover, should include both military and civilian entities. Given the authority and span of the GPD, Chinese psychological warfare operations are likely to be integrated into broader military operations and incorporated into the earliest stages of military planning.

- Principle #3: Seize and retain the initiative. As Chinese writings on public opinion warfare and legal warfare have emphasized, with regard to political warfare, the side that gets its message out first has an enormous advantage. The same principle is true for psychological warfare. In order to seize the initiative, PLA writings stress that advance preparation is essential; only through early research can the most effective messaging be delivered, the most vulnerable targets be identified, and the best approach be determined. Securing the initiative significantly increases the likelihood of creating shifts and trends in one's own favor. At the same time, being proactive in the implementation of psychological warfare activities compels an opponent to spend time and resources countering one's own messages rather than implanting his own program. This principle again highlights the importance of undertaking some elements of psychological warfare in peacetime.

- Principle #4: Assume an objective outlook. In the view of the PLA, psychological warfare operations are governed by certain objective laws (including these principles). Therefore, effective implementation of psychological warfare cannot be subject to hunches and hopes; rather, it requires a full consideration of all existing conditions and contemporary realities. To this end, psychological warfare efforts should not be based on outlandish or unrealistic ruses, but instead should be consistent with larger contexts. The most effective psychological warfare efforts will reinforce preconceptions.

  In this regard, Chinese analysts are making an observation comparable to that of Allied planners in World War II, whose deceptions before D-Day played to German (and especially Hitler's) expectations that the main attack would be at the Pas de Calais. Just as it is difficult to dislodge preconceived notions, it is far easier to exploit those same notions. Effective psychological warfare activities will therefore not try to substitute a preferred narrative, but rather will exploit the prejudices and assumptions of the other side.

- Principle #5: Recognize linkages. To be effective, psychological warfare techniques must be mutually reinforcing. This requires careful pre-planning, coordination among the various elements engaging in activities, and the creation of a single, unified plan and command authority. Psychological operations therefore also demand a dedicated, professional cadre and cannot be conducted as an afterthought by amateurs. At the same time, local authorities and resources may well have specific—even superior—understanding of potential psychological warfare targets; consequently, their knowledge and resources should be leveraged to maximize effect. Similarly, psychological warfare operations cannot be undertaken in isolation from other activities (e.g., military attacks or diplomatic and economic maneuvers); they must be coordinated with and supportive of those operations.[9] Finally, offensive and defensive psychological warfare operations must be mutually complementary.

■ Principle #6: Retain flexibility. Psychological warfare activities must always pay attention to the enemy, recognizing and accommodating changes in the enemy's psychology, the battlefield environment, and the relative stance of oneself and the enemy. Those responsible for implementing psychological warfare must be prepared to exploit changes in the situation in order to extract maximum effect.

Typology of Psychological Warfare Operations

In examining the long history of psychological warfare operations—foreign and domestic, historical and contemporary—one group of PLA analysts has created a typology of psychological warfare operations. In assembling a selection of 100 case studies, the authors have broken them down into coercive, deceptive, alienating, and defensive psychological warfare.[10]

Coercive psychological warfare is aimed at causing an opponent to surrender or otherwise abandon a fight by leveraging his thinking, emotions, and/or will and persuading him that resistance is futile. It requires the possession of substantial, actual military capabilities, but the objective is to obviate the necessity to use those capabilities. Coercive psychological warfare involves manipulating the psychological workings of the opponent's leadership and population through displays of martial capability and the insinuation of violence. If this manipulation is effective, one can degrade an opponent's willingness to resist to the point where he will surrender without necessitating the full employment of actual capabilities.

Coercive psychological warfare is the preamble to actual conflict. That is, if it is not successful, then conflict will occur; successful coercion will mean that conflict is avoided because the opposition will have given way. In many ways, it harkens back to Sun Tzu's observation that the apex of achievement is to win without fighting. Successful coercive psychological warfare is the realization of ends for which one is prepared to go to war without having to take that final step and engage in active, kinetic, destructive warfare. From the Chinese perspective, given the destructiveness of nuclear weapons and even conventional forces, there is also significant incentive to develop coercive psychological approaches in order to achieve strategic ends without having to resort to the use of force.

Coercive psychological warfare can be implemented through military exercises, weapons tests, and other displays of capabilities. A triumphant history of previous wars is also important, as such success demonstrates the capabilities at one's disposal and, along with other displays of martial prowess, leaves one's opponent feeling overmatched and outclassed. Interestingly, Chinese analysts suggest that this approach is used most by the United States, which sees great benefit in achieving its political aims without having to engage in actual combat. The range of annual military exercises, both national and multinational, not only allows the United States to experiment with a variety of new weapons and tactics, but also demonstrates American military effectiveness, thereby intimidating both real and potential opponents.

Chinese computer network activities should be seen as attempts to exert coercive psychological pressure. The constant reconnoitering of computer networks raises serious questions about the security of information systems and potentially affects state and non-state actors' willingness to communicate. In a crisis, such activities may well raise questions about operational security and the extent to which the PRC may already have penetrated national information systems and databases.

Deceptive psychological warfare entails the use of various ruses and other steps including camouflage, dummies, disguises, and the like to give wrong impressions and generate mistaken assessments. It is rooted in the idea of "garbage in, garbage out"; if misleading or deceptive information is fed to decision-makers, the resulting decisions will themselves be wrong. It is another aspect of the struggle for information dominance (zhi xinxi quan), which is seen as the keystone for fighting and winning future "Local Wars Under Informationized Conditions." While the advances in modern information technology allow for more rapid acquisition, transmission, and exploitation of information, deceptive psychological warfare degrades the quality of such information available to an opponent. Thus, it is an important complement to modern information systems.

Although deceptive psychological warfare has long been a staple of military operations (more than 2,000 years ago, for example, Sun Tzu observed that "all war is deception"), its impact is described in terms of modern psychology. The purpose of deceptive psychological warfare is to employ stratagems and other deceptive measures to implant psychological and informative barriers in the cognitive processes of opponents.

Not only will this make it harder to differentiate between what is true and what is false; it will also complicate decision making. For example, perhaps opposing commanders are given incorrect information, or perhaps their thought processes are retarded as they try to reconcile accurate data with inaccurate data. Either way, the result is the same: a military advantage.

Deceptive psychological warfare depends upon creating false impressions while masking reality, much as the deceptive measures for D-Day entailed both hiding the mountains of supplies and various actual forces and creating false formations upon which the Germans would fixate. Such a strategy in turn requires that the deceptive information be both credible and consistent with the opponent's psychological activities and patterns. In the Allied deception efforts prior to D-Day, for example, the Allied planners not only encouraged German preconceptions of an invasion at the Pas de Calais, but even "assigned" General George S. Patton to command the assault forces embodied within the fictitious "First US Army Group."[11]

An essential element for deception operations is to exploit "confirmation bias," or "the tendency of individuals to look for, and attach more importance to, information that validates their existing beliefs," while dismissing or explaining away information that invalidates or contradicts those same beliefs.[12] As Chinese authors note, an opponent will be looking for deceptions and false leads. Deceptive psychological warfare efforts will therefore be much more likely to succeed—i.e., the ideas presented will be accepted—if they support or are consistent with preconceived notions and frameworks, since they will then fit more readily into the opponent's cognitive and psychological framework and be subjected to less careful scrutiny.

Alienation psychological warfare is aimed at generating dissension and discord in the opponent's camp, creating friction and fracturing links between the population and the leadership, among leaders or between allies, and between the military and civilian population. By generating mutual suspicion, one causes the opposition to become more suspicious of each other, which forestalls effective cooperation. As one Chinese volume observes, "castles are inevitably easier to attack from within."[13]

Alienation psychological warfare requires a thorough understanding of an opponent at both the individual and group levels. It requires grasping group dynamics, understanding fault lines between individuals and within groups, and identifying and exploiting individual personality and character traits, as well as underlying jealousies and suspicions, in order to tailor specific operations against them as effectively as possible.

This type of psychological warfare builds on the belief that people's activities are often constrained by their underlying nature or character, especially the passive aspects. Often manifested as weaknesses or flaws in their character, such passivity is an essential vulnerability to be exploited. By emphasizing the propensities to which those passive aspects are linked, one can misguide and mislead an enemy commander with relative ease. As important, such emphasis can generate divisions within the top leadership or between the leaders and the led.

Consequently, this type of psychological warfare demands much more extensive research into an opponent as one seeks to determine weaknesses in individual character and group solidarity, as well as methods of exacerbating those weaknesses and vulnerabilities. By creating more interest groups—many of which have divergent interests—globalization facilitates alienation psychological warfare. This in turn generates ever more fault lines, which can cause an opponent to be much more brittle and easily disrupted.

Defensive psychological warfare seeks to counteract an opponent's attempt to employ coercive, deceptive, and alienation psychological warfare against one's own side. It entails a variety of methods, given the complexity of psychological offense. Some of the more important methods include:

■ Strengthening indoctrination to immunize one's leadership and population against the enemy's messaging efforts.

■ Preempting the enemy's psychological warfare efforts in order to create a broad consensus among one's own population, forces, and leaders that an opponent will find it harder to undermine. This often will involve undertaking psychological operations in peacetime or at least before the formal onset of hostilities. It also includes strengthening psychological warfare training to heighten awareness of enemy efforts, thus lowering domestic susceptibility.

■ Controlling public opinion through such means as control of the media and strategic communications, as well as discouragement of rumor-mongering. This will limit the opportunities for an opponent to exploit differences (as in alienation psychological warfare) or otherwise undermine one's own military and popular morale.

■ Forging greater internal consensus to increase national solidarity and unify the various social and political groups. This includes greater enforcement of laws and regulations in order to reduce the temptation to break the law and thereby create opportunities for enemy psychological warfare activities.

PLA analyses recognize that the faster tempo and operational rhythms of modern warfare impose greater pressures on both military and civilian populations. Consequently, they acknowledge the need to improve safeguards against and treatment for psychological pressure and damage, including post-traumatic stress syndrome. Moreover, as one volume observes, because of the one-child policy, young people are pampered and may therefore be more psychologically brittle and less capable of handling stress. Defensive psychological measures are therefore seen as an essential means of limiting the impact of wartime pressures on them.

PLA Assessment of Psychological Warfare in the Iraq War

The PLA has not engaged in a conflict since 1979. Consequently, its analysts have examined foreign military experiences to derive likely lessons and trends in modern warfare. The second Gulf War, with the American defeat of the Iraqi military, is seen as the epitome of conventional modern warfare, including in the application of psychological warfare operations.

In the view of PLA analysts, psychological operations were conducted at an unprecedented scale and intensity, from the tactical to the strategic levels, and engaged a range of both military and non-military measures. In particular, Chinese analysts believe the United States factored psychological warfare into all of its thinking, from strategic decisions to operational plans to actual tactical employment and military battles.

According to this analysis, the U.S. began psychological warfare operations long before March 2003. Indeed, at the strategic level, psychological warfare efforts began almost upon the conclusion of Operation Desert Shield/Desert Storm. Two decades of international sanctions had not only limited Iraq's ability to maintain its forces, but also created a siege mentality among the Iraqi population. This isolation was reinforced by the repeated charges that Iraq possessed weapons of mass destruction, dating back to the George H.W. Bush Administration.[14]

This strategic isolation, both diplomatic and economic, coupled with the imposition of a strategic information blockade by denying Iraq access to international media and communications, imposed significant pressure on the Iraqi leadership and population long before the outbreak of hostilities.[15] Senior U.S. leaders also openly discussed post-war Iraqi reconstruction plans even before hostilities had begun—an attempt to demonstrate that Iraq's defeat was a fait accompli.

The strategic psychological pressure on the Iraqis was sustained even after hostilities commenced—not only through the continued isolation of Iraq, but even through the naming of allied operations. As one Chinese assessment noted, the decision to title the war "Operation Iraqi Freedom" was a masterful psychological ploy. It implied that the United States undertook this war in order to liberate the Iraqi people, with no ulterior motives.[16]

Chinese analysts believe that as the onset of open hostilities drew closer, the United States engaged in alienation psychological warfare at the strategic level by calling senior Iraqi officers directly on their personal cell phones and sending e-mails to their personal accounts, trying to induce them to surrender or otherwise not operate at full effectiveness. Such measures sowed seeds of discord and mistrust within the senior Iraqi leadership, thereby dissipating solidarity at the very top.[17] Such chaos was further exacerbated by American engagement of a variety of exiles and dissidents in order to foment additional discord and create divisions among Iraqis.[18]

Once the war began, the United States, according to Chinese assessments, employed coercive psychological warfare methods, mostly at the tactical level. These operations included such measures as "decapitation (zhanshou xingdong)" efforts against Iraq, which sought to kill Saddam in the first hours of the conflict. Although these attacks failed to achieve that objective, coalition forces regularly claimed that Saddam had been killed; the spread of false information and rumors is a basic component of psychological warfare. Along these lines, one PLA assessment suggests that the dispatch of relatively small armored detachments into Baghdad in April was not an unnecessary military risk, but rather an attempt to erode Iraqi military will further by showing that U.S. forces could operate at will and generating additional uncertainty within the Iraqi leadership.

However, coalition forces hardly had a monopoly on psychological warfare. Chinese authors observe that within the more constrained resources available to it, the Iraqi government also sought to employ psychological warfare both to inspire greater resistance against the invaders and to garner more support from abroad—or at least condemnation of the Anglo–American leaders of the coalition. Thus, in the Chinese view, the Iraqis chose to assume an almost passive stance in the months leading up to the outbreak of hostilities, allowing U.N. inspectors into Iraq and making clear that Baghdad had no intention of commencing hostilities.[19] Once the war began, Saddam was regularly televised, undermining coalition efforts to claim that he had been killed.

What the United States Should Do

It seems clear that the Chinese take psychological warfare very seriously and believe that America's use of such tactics is a major factor in the recent success of U.S. military operations.[20] It is ironic that the Chinese see the United States as pursuing a much more coherent, integrated approach to psychological operations when Western analyses and policy approaches seem to treat psychological operations as discrete entities.

Many Western policymakers differentiate between psychological warfare at the strategic level, involving national tools such as strategic communications and public diplomacy, and more tactical-level efforts waged by dedicated psychological warfare units. Indeed, the renaming of the latter as "military information support operations (MISO)" underscores this significant but artificial divide in the American approach. Given the radical advances in information technology and the attendant globalization and permeation of information, psychological operations need to be seen in a more holistic light.

Consequently, reducing obstacles to information flow and public outreach is the most important thing America can do to improve its psychological warfare capabilities. Whether at the strategic or tactical level, there needs to be an overarching communications plan, incorporating all of the relevant agencies and entities, to convey to the rest of the world that the United States is a reliable ally and steadfast partner, willing to cooperate with other states to advance our mutual interests but fully prepared to counter aggression against friends and allies. Whether the United States government is seeking to deter, persuade, coerce, or placate others, it can succeed only by presenting a coherent message. To this end, the U.S. government, and especially Congress, should continue to break down such barriers, as was done recently with modernization of the Smith–Mundt Act.[21]

At the strategic level, this entails improving inter-agency strategic communications, including coordination of messages and efforts among the major foreign policy departments—State, Defense, Commerce, Treasury, and even the Departments of Justice and Agriculture, both of which regularly interact with foreign governments and non-governmental organizations. Only by creating and transmitting unified messages can the United States gain the initiative in influencing foreign governments and populations, whether allied, adversary, or neutral. The Pentagon, which does not necessarily have the expertise, should not head this inter-agency effort. Furthermore, such an operation should also extend beyond the State Department and might well involve the reestablishment of the United States Information Agency, drawing upon the public diplomacy resources of the entire government.

Another aspect of strategic psychological warfare operations is the effective use of alliances and relationship building, which should emphasize current relations while moving beyond traditional allies. In the Asia–Pacific region, for example, the United States possesses a significant foundation of strong alliances with Japan, South Korea, Thailand, the Philippines, and Australia as well as special relationships with Taiwan, Singapore, and New Zealand and a revision of relations with India. The array of bilateral and increasingly multilateral relations among these states sends a strong signal to potential antagonists and adversaries that hostile actions will likely generate a concerted response from a powerful set of nations.

By exposing Chinese psychological warfare activities, America can enhance its other information flow operations. Just as the recent Mandiant report on Chinese cyber activities reveals the extent to which the Chinese military is actively engaged in both traditional national intelligence gathering and commercial espionage, the U.S. should publicize examples of Chinese efforts to influence foreign public opinion, whether through use of Chinese state-owned media, cyber espionage, or other national means. The growing Chinese assertiveness on maritime territorial disputes, including not only the Spratlys and Senkakus, elsewhere in the East and South China Sea, is as much psychological posturing as physical action and should be countered by American diplomatic and economic, as well as military, moves.

At the operational and tactical level, the U.S. military should recognize the importance of its psychological warfare capabilities. Labeling them "military information support operations" would seem to undercut the holistic nature of psychological warfare activities, which are neither solely the purview of the military nor focused only on military-related information. Indeed, successful psychological warfare operations cannot take a stovepiped approach; they must incorporate military and civilian public affairs specialists, press secretaries and public affairs officers, and individual military and civilian personnel.

This holistic approach entails not only integrating MISO activities into all aspects of military planning and activities, but also recognizing that American psychological warfare assets are likely to be a major target for the PLA in times of crisis and especially conflict. Given the limited numbers of such assets, neutralizing them, whether through cyber activities, kinetic attacks, or other means, would affect the course of the conflict. The Chinese military is therefore likely to commit significant resources to countering such units early in any conflict. American planners should recognize this threat and incorporate both active and passive security measures into their own preparations.

War in a Time of Peace

The Information Age provides unparalleled ability to influence both a nation's leaders and its population. The core of the Chinese concept of psychological warfare is to manipulate those audiences by affecting their thought processes and cognitive frameworks. In doing so, Beijing hopes to be able to win future conflicts without firing a shot—victory realized through a combination of undermining opponents' wills and inducing maximum confusion.

Indeed, although it is a time of peace, psychological warfare is already underway, employing a variety of both military and civilian means. It is therefore essential that the United States counter such psychological operations now while preparing to use its own arsenal of political warfare weapons should a conflict ever arise.

References

[1] Guo Yanhua, Psychological Warfare Knowledge (Beijing, PRC: National Defense University Press, 2005), p. 1.

[2] Nanjing Political Academy, Military News Department Study Group, "Study of the Journalistic Media Warfare in the Iraq War," China Military Science, No. 4 (2003), p. 30.

[3] Academy of Military Science, Operations Theory and Regulations Research Department and Informationalized Operations Theory Research Office, Informationalized Operations Theory Study Guide (Beijing, PRC: Academy of Military Science Press, November 2005), p. 404.

[4] Li Naiguo, New Theories of Information War (Beijing, PRC: Academy of Military Science Press, 2004), p. 154.

[5] Yuan Wenxian, The Science of Military Information (Beijing, PRC: National Defense University Press, 2008), pp. 77–79.

[6] Guo, Psychological Warfare Knowledge, p. 14.

[7] Ibid., pp. 14–16.

[8] Wang Yongming, Liu Xiaoli, et al., Research on the Iraq War (Beijing, PRC: Academy of Military Science Press, 2003), p. 229.

[9] Wang Yuping, "Strengthen Research into Psychological Warfare Under Informationized Conditions," People's Liberation Army Daily, May 18, 2004, http://news.xinhuanet.com/mil/2004-05/18/content_1475394.htm (accessed June 14, 2013).

[10] Ci Weixu, ed., 100 Questions About Psychological Warfare (Beijing, PRC: Liberation Army Press, 2004), esp. pp. 1–2, 103–104, 236–237, and 302–303.

[11] For a more extensive discussion of the D-Day deceptions, see Roger Hesketh, Fortitude: The D-Day Deception Campaign (Woodstock, N.Y.: The Overlook Press, 2000).

[12] Uri Bar-Joseph, "Intelligence Failure and the Need for Cognitive Closure: The Case of Yom Kippur," in Paradoxes of Strategic Intelligence, ed. Richard Betts and Thomas Mahnken (London, U.K.: Frank Cass Publishers, 2003), p. 173.

[13] Ci Weixu, ed., 100 Questions about Psychological Warfare, p. 236.

[14] Nanjing Political Academy, Military News Department Study Group, "Study of the Journalistic Media Warfare," p. 28.

[15] Fan Gaoming, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare, the Three Major Combat Methods to Rapidly Achieving Victory in War," Global Times, March 8, 2005.

[16] Hu Fengwei, Psychological Warfare in the Iraq War (Shenyang, PRC: White Mountain Press, 2004), pp. 94–95.

[17] Wang et al., Research on the Iraq War, p. 86.

[18] Fan, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare."

[19] Wang et al., Research on the Iraq War, p. 205.

[20] Hu Fengwei, Ai Songru, et al., Psychological Warfare in the Iraq War (Shenyang, PRC: Baishan Publishing House, 2004), p. 321.

[21] Helle Dale, "Smith–Mundt Modernization: Better Late than Never," The Heritage Foundation, The Foundry, May 22, 2013, http://blog.heritage.org/2012/05/22/smith-mundt-modernization-better-late-than-never/; BBG Strategy, "New Law Ends Smith–Mundt Ban on Domestic Dissemination of Content," January 4, 2013, http://www.bbgstrategy.com/2013/01/new-law-uends-smith-mundt-ban-on-domestic-dissemination-of-content/ (accessed June 14, 2013).

Table of Contents

China Prepares for Psychological Warfare

By Aaron Jensen, the Diplomat, August 14, 2013

The recent unveiling of China's new PSYOP (Psychological Operations) aircraft, the Gaoxin-7(高新七号), marks an important step forward for People's Liberation Army's (PLA) psychological warfare capabilities.

Based on a Y-8 airframe (similar to the U.S. Military's C-130), the Gaoxin-7's primary mission is to conduct PSYOP missions against enemy forces. Although specific details are few and far between, People's Republic of China (PRC) media has compared the Gaoxin-7 to the U.S. Air Force's (USAF) EC-130J "Commando Solo" in terms of its mission and capability. The EC-130J Commando Solo is essentially a flying broadcast station which can transmit media in AM, FM, HF, TV and military communication frequencies to enemy positions. Its transmission capability is so powerful that it is required to operate at least 200 miles off the coast of the United States during training missions so as to avoid interfering with civil communications.

PSYOP has had an important role in numerous U.S. Military operations and Chinese military planners have paid close attention to these developments. The EC-130J Commando Solo has also played a central part in these operations. In Desert Storm and Operation Iraqi Freedom, Commando Solo was used broadcasted messages in Arabic which urged Iraqi soldiers to surrender. In both conflicts, large numbers of Iraqi troops surrendered to coalition forces without fighting. More recently, Commando Solo participated in the Libyan Air War and broadcasted messages which urged Libyan soldiers to avoid fighting and return to their homes.

The Gaoxin-7 would play a significant role in any future hostilities or heightened tensions. One area where the Gaoxin-7 could be particularly effective would be in a conflict with Taiwan. PLA psychological warfare efforts could potentially have a devastating effect on Taiwanese troops. As some observers have noted, Taiwan's military does not have particularly high morale and the public generally lacks confidence in the military's ability to defend the island. Prior to, and during, a conflict with Taiwan, the Gaoxin-7 would likely be used to broadcast messages to demoralize Taiwanese troops, and persuade them to surrender. Important PLA psychological warfare concepts such as the humane treatment of POW's policy (优待俘虏/Yōudài fúlǔ) would likely have a powerful impact on Taiwanese soldiers. Going back to the Mao Era, this policy seeks to encourage enemy soldiers to surrender without fighting in return for fair and humane treatment. When combined with fear-inducing PSYOP measures, and the PLA's military superiority, the appeal of humane treatment in exchange for surrender would be even stronger.

China has already laid a strong foundation for psychological warfare against Taiwan with the establishment of the PLA's General Political Department's 311 Base in Fujian Province. In 2011, this base was designated as the focal point for all psychological warfare efforts against Taiwan, including help transmit China's Voice of the Straits radio.

Additionally, the PLA has also stepped up PSYOP training against Taiwan. In 2006, the PLA included psychological warfare units in exercises held in the Nanjing Military Region. During the exercise, these units dropped leaflets on mock enemy positions and broadcast PSYOP messages in Taiwanese and English. The addition of the Gaoxin-7 will greatly enhance and extend the reach of the PLA's PSYOP activities against Taiwan.

In addition to Taiwan, the Gaoxin-7 could also play a key role in the event of hostilities in the South China Sea against countries like The Philippines and Vietnam. Like Taiwan, the Vietnamese and Philippine militaries are significantly out-gunned by the PLA. Here again, the PLA's policy of humane treatment for POWs could have a powerful impact on soldiers and sailors who have little expectation of victory. With its medium sized airframe, the Gaoxin-7 could operate from some of the PRC-controlled islands in the South China Sea.

With the introduction of the Gaoxin-7, the PLA now wields a powerful new psychological weapon which can be deployed to produce fear and confusion in the minds of enemy troops and leaders. If used effectively, the Gaoxin-7 could greatly reduce the amount of resistance that the PLA would otherwise encounter in future battles.

Table of Contents

China Launches Three ASAT Satellites

By Bill Gertz, Washington Free Beacon, August 26, 2013

China's military recently launched three small satellites into orbit as part of Beijing's covert anti-satellite warfare program, according to a U.S. official.

The three satellites, launched July 20 by a Long March-4C launcher, were later detected conducting unusual maneuvers in space indicating the Chinese are preparing to conduct space warfare against satellites, said the official who is familiar with intelligence reports about the satellites.

One of the satellites was equipped with an extension arm capable of attacking orbiting satellites that currently are vulnerable to both kinetic and electronic disruption.

“This is a real concern for U.S. national defense,” the official said. “The three are working in tandem and the one with the arm poses the most concern. This is part of a Chinese ‘Star Wars’ program.”

China’s 2007 test of an anti-satellite missile shocked U.S. military and intelligence leaders who realized the U.S. satellites, a key to conducting high-performance warfare, are vulnerable to attack. Officials have said China could cripple U.S. war-fighting efforts by knocking out a dozen satellites. Satellites are used for military command and control, precision weapons guidance, communications and intelligence-gathering.

The official discussed some aspects of the Chinese anti-satellite (ASAT) program on condition of anonymity after some details were disclosed in online posts by space researchers.

“The retractable arm can be used for a number of things – to gouge, knock off course, or grab passing satellites,” the official said.

The three satellites also could perform maintenance or repairs on orbiting satellites, the official said.

Details of the small satellite activity were first reported last week in the blog “War is Boring.”

The posting stated that one of the satellites was monitored “moving all over the place” and appeared to make close-in passes with other orbiting satellites.

“It was so strange, space analysts wondered whether China was testing a new kind of space weapon—one that could intercept other satellites and more or less claw them to death,” the report said.

The U.S. official said: “It is exactly what was reported: An ASAT test.”

According to space researchers who tracked the satellites movements, one of the satellites on Aug. 16 lowered its orbit by about 93 miles. It then changed course and rendezvoused with a different satellite. The two satellites reportedly passed within 100 meters of each other.

One space researcher was quoted in the online report as saying one satellite was equipped with a “robot-manipulator arm developed by the Chinese Academy of Sciences.”

The Chinese appear to be testing their capability for intercepting and either damaging or destroying orbiting satellites by testing how close they can maneuver to a satellite, the U.S. official said.

“They are learning the tactics, techniques and processes needed for anti-satellite operations,” the official said.

The Chinese have given a code name to the satellites and numbered the satellites differently. The code name could not be learned. The official said the designation used in the blog, SY-7 was not correct.

A Pentagon spokesman had no immediate comment about the Chinese satellites.

The official said the Obama administration is keeping details of the Chinese anti-satellite warfare program secret as part of its policies designed to play down threats to U.S. national security.

“There is a Star Wars threat to our satellites,” the official. “But the official said the administration does not want the American people to know about it because it would require plusing up defense budgets.”

The use of satellites for space warfare appears to be a departure from past Chinese ASAT efforts. China faced international condemnation in 2007 for firing a missile that blasted a Chinese weather satellite in space, leaving tens of thousands of debris pieces.

A recently translated Chinese defense paper on the use of a kinetic energy anti-satellite missile revealed that China is making progress with its anti-satellite warfare program. The report reveals that a U.S. software program called Satellite Tool Kit is being used by the Chinese military for its ASAT program.

“Kinetic energy antisatellite warfare is a revolutionary new concept and a deterrent mode of operation,” the 2012 translation of the report stated. “The construction of the corresponding information flow is certainly important to the effectiveness of the kinetic energy antisatellite operation. The STK package, being a powerful professional space simulation platform, will play an active supporting role in research on information flow in kinetic energy antisatellite warfare.”

A joint State Department and Pentagon report on export controls published last year stated that China is working on several types of anti-satellite warfare systems.

“China continues to develop and refine its ASAT capabilities as one component of a multi-dimensional program to limit or prevent the use of space-based assets by potential adversaries during times of conflict,” the report said.

“In addition to the direct-ascent ASAT program, China is developing other technologies and concepts for kinetic and directed energy for ASAT missions.”

The report said China has said that to support its manned and lunar space program, it is “improving its ability to track and identify satellites—a prerequisite for effective, precise counter-space operations.”

“The People’s Liberation Army (PLA) is acquiring a range of technologies to improve China’s space and counter-space capabilities,” the report said.

A recent PLA analysis concluded that space is the “commanding point” for the modern information battlefield.

“Battlefield monitor and control, information communications, navigation and position guidance all rely on satellites and other sensors,” and Chinese military writings emphasize, “destroying, damaging, and interfering with the enemy’s reconnaissance … and communications satellites.”

The military writings suggest that satellites could be part of an initial attack aimed at blinding the enemy. “Destroying or capturing satellites and other sensors … will deprive an opponent of initiative on the battlefield and [make it difficult] for them to bring their precision guided weapons into full play,” the PLA report said.

Rick Fisher, a Chinese military affairs specialist, said the maneuvering satellites are a significant element of China’s military space program.

The satellite with the robotic arm is a clear dual-use, military-civilian satellite, said Fisher, with the International Assessment and Strategy Center.

“The robot arm will develop a larger arm for China’s future space station, but this satellite can also perform ‘co-orbital’ surveillance or attacks against target satellites,” Fisher told the Free Beacon. “It is essentially China’s version of the 2007 DARPA Orbital Express satellite that was criticized by liberals as step toward ‘militarizing’ space.”

According to Fisher, the satellites are part of a space surveillance and targeting system that will monitor space debris and also allow interception of space targets.

Elements of the satellite system also will be used for China’s missile defense system, which is linked to China’s anti-satellite missiles.

“But despite any potential ‘peaceful’ uses, the main point for the United States is that the PLA owns these programs and will use them as weapons against American space assets when it so chooses,” Fisher said. “All future U.S. military satellites require low-cost stealth or defense capabilities if the U.S. is to keep its essential military space architecture.”

The space weapons program in China shows that no amount of American restraint will halt Beijing’s drive for military advantage in space.

“Today China’s dictatorship rejects all forms of strategic arms control that could deny the Communist Party a capability that it deems essential to the survival of its dictatorship,” Fisher said. “When China gains superiority in any strategic category it will be even less willing to bargain away capability for the sake of ‘stability.’ China will not ‘reward’ any future U.S. nuclear weapon reductions or restraint in developing space weapons.”

China also conducted a maneuvering small satellite test in 2010, according to defense officials, which also was deemed an ASAT-related experiment.

Two Chinese satellites rendezvoused several hundred miles above Earth in August 2010 as part of what was viewed by officials as a contribution to the anti-satellite weapons program.

The Pentagon said at the time, “Our analysts determined there are two Chinese satellites in close proximity of each other. We do not know if they have made physical contact. The Chinese have not contacted us regarding these satellites.”

The two satellites also maneuvered during the Aug. 22, 2010 encounter. Based on the behavior, it appeared one of the satellites made contact with another satellite causing it to change orbits. The two satellites were estimated to have been as close as 200 meters to each other.

Table of Contents

Electronic Warfare Development Targets Fully Adaptive Threat Response Technology

From R&D Magazine, 08/19/2013

When U.S pilots encounter enemy air defenses, onboard electronic warfare (EW) systems protect them by interfering with incoming radar signals—a technique known as electronic attack (EA) or jamming. Conversely, electronic protection (EP) technology prevents hostile forces from using EA methods to disable U.S. radar equipment assets.

Defeating hostile radar helps shield aircraft from ground-to-air missiles and other threats, so it's a military priority to ensure that EW systems can defeat any opposing radar technology.

At the Georgia Tech Research Institute (GTRI), which has supported U.S. electronic warfare capabilities for decades, a research team is developing a new generation of advanced radio frequency (RF) jammer technology. The project, known as Angry Kitten, is utilizing commercial electronics, custom hardware development, novel machine-learning software and a unique test bed to evaluate unprecedented levels of adaptability in EW technology. Angry Kitten has been internally funded by GTRI to investigate advanced methods that can counter increasingly sophisticated EW threats.

"We're developing fully adaptive and autonomous capabilities that aren't currently available in jammers," said research engineer Stan Sutphin. "We believe a cognitive electronic warfare approach, based on machine-learning algorithms and sophisticated hardware, will result in threat-response systems that offer significantly higher levels of electronic attack and electronic protection capabilities, and will provide enhanced security for U.S. combat aircraft."

When an EW encounter begins, the Angry Kitten system chooses an optimal jamming technique from among many available options, explained Sutphin, who leads a GTRI development team that includes senior research engineer Roger Dickerson and senior research scientist Aram Partizian.

As the engagement progresses, the next-generation system is designed to adapt. It will assess how effective its jamming is against the threat and quickly modify its approach if necessary.

Angry Kitten research also includes investigation of cognitive learning algorithms that allow the jammer to independently assess and respond to novel opposing technology. The team is developing techniques to enable an EW system to respond effectively should it encounter unfamiliar hostile radar techniques.

Moreover, the flexibility of the Angry Kitten system allows it to represent a range of threat EA systems. That will help to support the development of new and improved EP measures.

Adaptive digital technology

Traditionally, Sutphin explained, radar jamming has consisted of two basic approaches. One employs mechanical techniques that reflect radar beams back at the sender using chaff material spread through the air behind the carrying platform. The other uses electronic techniques to emit powerful electromagnetic signals that interfere with incoming hostile radar beams. But these techniques are relatively basic, and they involve overt suppression strategies that are often obvious to the other side.

Today's top EW systems are more subtle, thanks to digital techniques. The most advanced technology today—digital radio frequency memory (DRFM)—can deceive an enemy by recording his received radar signals, manipulating them and sending back false information that seems to be real.

"A DRFM jammer is a very effective way of adding clutter to the scene without just using unsophisticated noise-jamming techniques," Sutphin said. "You can create false targets, or hide real targets, using the enemy's own waveforms against him."

The GTRI team believes that countering such techniques will lead to the development of increasingly more precise digital techniques for radar electronic protection (EP). That could spark an equivalent race for more advanced jammer techniques.

“We need an approach to more quickly evaluate advances in digital RF signal generation, and to rapidly field countermeasures without expensive hardware upgrades,” said Tom McDermott, GTRI’s Dir. of Research.

In the first phase of developing a next-generation system, the GTRI team completed an advanced jamming system prototype. This custom hardware utilizes a wideband tunable transceiver system, and is built using open architecture/open source approaches that are low-cost and enable operators to quickly modify the system in response to changing conditions.

The team is currently developing machine-learning algorithms that will allow the Angry Kitten system to continually assess its environment and switch among the best methods for jamming incoming threats. The ultimate goal is a robust platform that will characterize any threat emitter and respond in real time in the most effective way.

A unique test bed

Today, DRFM jammers employ a computer-based "library" of known threats that are used to identify and neutralize incoming signals, Sutphin explained. DRFM equipment may also include an electronic-intelligence (ELINT) capability, which monitors and collects information on enemy signals and jammers. The ELINT data gathered may eventually be used—possibly weeks, months, or years later—to improve U.S. threat-response techniques.

To support the current effort, the researchers are utilizing a GTRI-designed tool called the enhanced radar test bed. Devised by a team led by Partizian, the test bed simulates opposing radar signals and enables convenient, low-cost and highly realistic testing of jammers.

The test bed is an important asset in the development of the Angry Kitten system, Sutphin said. It offers the ability to collect realistic, representative jammer data on advanced waveforms. It can be used to represent virtually any known threat—and even hypothetical radar systems that don't currently exist.

The test bed allows the team to rapidly prototype a software approach, test it out against simulated enemy hardware, and come up with high-fidelity data. The researchers can perform this work without having to build or acquire actual hardware radar systems or jammers, or engage in expensive flight tests.

Table of Contents

Military Education Falls Short on Cybersecurity Training

By Brittany Ballenstedt, NextGov, August 12, 2013

Most of the six military graduate programs have not fully integrated cybersecurity education into their curricula or aligned their programs with the strategic goals of the nation's cyber defense strategy, a new study suggests.

The study, "Joint Professional Military Education Institutions in an Age of Cyber Threat," released last week by Pell Center Fellow Francesca Spidalieri, noted that while most military leaders do not need specific training in computer science or engineering, it is still imperative that they have a deep understanding of the cyber threat landscape. Yet this remains an area where most military graduate programs continue to fall short.

"Even professional military institutions studying national security and strategy have only recently begun to integrate cybersecurity education in their curricula, despite more than a decade's worth of experience suggesting that networks and information technologies are both essential to operations and vulnerable to attack," the report stated.

More specifically, the report found that the Joint Professional Military Education at the six U.S. military graduate schools -- a requirement for becoming a Joint Staff Officer and for promotion to the senior ranks -- has not effectively incorporated cybersecurity into specific courses, conferences, war gaming exercises or other forms of training for military officers. While these graduate programs are more advanced on cybersecurity than most American civilian universities, a preparation gap still exists.

The study, which ranked the military graduate programs on a 4-point Likert scale, found National Defense University in Washington, D.C., to have the most advanced cyber curriculum, receiving a score of 3.5 out of 4. The U.S. Naval War College and the Naval Postgraduate School each received a score of 3 on cyber education, followed by the U.S. Air Force Air War College (2), Marine Corps War College (1) and the U.S. Army War College (0.5).

In response, the report recommended that military graduate programs revise their curricula to include cybersecurity education, and expand such programs not only to military officers but to Defense civilian employees, other federal agencies and international officers.

"The question will not be whether or not the U.S. can develop the best and most powerful cyber capabilities to accomplish a certain feat, but whether our military – and our nation's leaders – will be equipped with knowledge necessary to confront a wide array of cyber threats and establish both a competitive and security advantage on the modern battlefield," the report stated.

[download report at http://pellcenter.salvereginablogs.com/files/2013/08/JPME-Cyber-Leaders-Final.pdf]

Table of Contents

Why It's Important to Herd the Social Media Sheep

By Steve Cooper, Forbes, 28 August 2013

"Click velocity" is a term that's been batted around for years, which defines a measurement of how quickly something is getting clicked over a period of time. When it comes to social media, early clicks are king!

New research published in the journal Science found when their scientists had given a fake positive score, such as "liking" a story (even though they may not have really liked it), the first person to engage with the story was 32 percent more likely to also "like" the story. These early positive reviews accumulate over time to generate 25 percent more likes than stories that did not get the early boost. The research collected and analyzed data on more than 100,000 posts after website administrators were the first to arbitrarily comment or vote positively or negatively (or not at all).

This is obviously not a new concept. When Forbes overhauled their website last year, including their homepage, they included a Most Popular page and a trending widget on all of their article pages based on Forbes Velocity, an algorithm that weighs page views, sharing and comments. This would seem to expedite the process since the items most shared are also getting seen the most.

Interestingly, while the researchers describe the early positive feedback and likes as the “herding effect,” the “sheep” apparently aren’t that influenced when discovering content through search. Recent findings by SurveyMonkey and iAcquire, a digital agency focused on search, found that only 12 percent of users say they are influenced by likes and +1s.

This would seem to indicate that early click velocity of social sharing acts more as a booster of traffic rather than a driver. In other words, you must already have your flock of sheep before you can herd them.

Another interesting point about the research published in Science is that while positive feedback generated other positive responses, negative social mentions garnered swift response to “correct” the contrary points of view. So whether a piece of content is talked about positively or negatively, as long as visitors are expressing their opinions publicly it will serve to herd the masses and boost overall engagement. The study’s lead author notes that—unlike the positive mentions—the false negative comments had a relatively small long-term impact.

The old adage that “there’s no such thing as bad publicity” has even further support from a new Indiana University study that tracked tweets for Republican and Democratic candidates in 2010 and 2012 races for the U.S. House of Representatives. The winners could be predicated by those candidates who received the most tweets, regardless of the tweets being negative or positive toward the candidate.

Whether it’s real votes or social votes, it’s all about getting buzz and making what you say matter. “Even if you don’t like somebody, you would only talk about them if they’re important,” says Fabio Rojas, an associate professor of sociology at IU, commenting about the university study.

So, whether you hate this article or love it, don’t be afraid to like and share this with your friends.

Table of Contents

Syrian Rebels Also Fighting Al Qaeda, Other Hard-Liners for Villagers’ Hearts and Minds

By Kristina Wong, Washington Times, August 27, 2013

The Syrian opposition isn’t fighting just a brutal Iranian-backed regime accused of killing civilians with chemical weapons; it’s also battling within itself.

Moderate Syrian rebel groups are locked in combat with al Qaeda-linked extremists who have joined the opposition against Bashar Assad’s regime and are fighting other rivals to win the hearts and minds of villagers as they try to gain support in the countryside.

“Those different groups with those competing agendas are starting to fight one another. They’re fighting for control over territory. They’re fighting for control over people. They’re fighting for control over wealth. They’re fighting to fight their way,” said Kenneth M. Pollack, a former CIA official who now serves as a senior fellow at the Brookings Institution's Saban Center for Middle East Policy.

Moderate rebels began to realize the threat from al Qaeda-backed insurgents after one of those groups, the Islamic State of Iraq and the Levant, killed a leader of the Free Syrian Army, the opposition umbrella group led by Syrian army defectors, according to several organizations in Washington that maintain contact between Syrian rebels and the U.S. government.

Syria’s moderate rebels refer to this realization of the danger posed by the Islamists as the “sahwa,” or awakening.

“It was a watershed moment. After that, moderate rebels [realized that] al Qaeda in Syria is a threat almost on par with the Syrian regime,” said Oubai Shahbandar, vice president for Middle East operations for the Syrian Support Group, which is charged with distributing U.S. aid to rebels.

Al Qaeda gains strength

The al Qaeda affiliates are gaining strength in the 2-year-old war against Mr. Assad. Thanks to funding and weapons from wealthy Persian Gulf states, the Islamists are the most organized, equipped and effective fighters of the opposition groups, which consist of a loose confederation of hundreds of militias.

Al Qaeda also is gaining support by providing villages with health care, blankets, fuel, wheat and other supplies captured from regime stores. They also have implemented courts under Shariah, or Islamic, law, which some villagers welcome as a sense of order amid the chaos of the civil war, which has cost an estimated 100,000 lives.

Moderate rebel groups under the Free Syrian Army are distributing aid and providing services through local government councils that have sprung up in places they control. However, those efforts lack sufficient funds and support to compete with al Qaeda, said Mouaz Moustafa, director of the Washington-based nonprofit Syrian Emergency Task Force, who travels frequently to Syria to support these councils.

He said the United States should realize that it has an opportunity to do more to help the moderate rebels in their campaign to spread their influence in the countryside.

“There’s huge room to empower the good guys and marginalize the bad guys all while fighting a very cunning regime,” said Mr. Moustafa, a former congressional aide to Blanche Lincoln, an Arkansas Democrat who served in the Senate. “The other two options are either warlords or religious extremists.”

Mr. Mouaz said more than 100 local civilian-run councils have sprung up at the town, village and provincial levels in areas controlled by the rebels. Their structures vary from place to place but are linked loosely with a partnership with local military units under the Free Syrian Army.

They consist of small teams of about 20 leaders who oversee education, finance, relief and aid distribution, infrastructure, human rights, public safety, media relations and judicial administration. They exist in Aleppo, the suburbs of Damascus, Idlib, northern Latakia, Hama and other areas controlled by moderate rebels.

The system would provide Syrians with an alternative to al Qaeda and could fill a void in government if the Syrian regime is toppled, Mr. Mouaz said. The United States has provided $117 million in communications and medical equipment to the opposition, as well as training to at least 1,500 leaders of these councils.

Doubts about ‘awakening’

However, he said, more needs to be done. For example, he said, the United States should channel all humanitarian aid through these councils to bolster their credibility against al Qaeda, as well as equip civilian police with uniforms and weapons, and support civil law and judicial systems.

“We must empower the emerging awakening against the transnational terrorist groups,” said Mr. Shahbandar, a former Defense Department official.

“Empowering moderate rebels is in America’s national security interests at a time when al Qaeda sees Syria as the front lines of an international terror campaign,” he said. “It’s still not too late.”

He likens the situation to the Sunni Awakening during the Iraq War in 2006, when moderate Sunnis began to reject al Qaeda extremists.

Although supporting these councils is a part of the U.S. policy in Syria, intelligence officials are skeptical about an “awakening” of moderate rebels. Pentagon officials doubt that any rebel groups would promote U.S. interests, even if Washington backed them.

Syria has about 1,000 armed rebel groups, 80 percent of which are under the Free Syrian Army umbrella, Mr. Mouaz said.

But with no end in sight to the civil war, supporting the local councils is the only prudent measure against al Qaeda extremists, advocates say.

“Right now, we still have a chance to support the right people in a situation that we simply can’t ignore,” said Mr. Mouaz, who recently met with high-ranking Pentagon officials.

Table of Contents

Applications of the Memetic Perspective in Inform and Influence Operations

By Erick Waage, Small Wars Journal, Aug 13 2013

The purpose of this article is to create awareness of the memetic perspective and postulate its potential applications in Inform and Influence Activities (IIA). The concept of memetics parallels that of Biological Evolution (BE) in process, however, where BE passes genes, the memetic process passes packets of information or culture called memes. Most BE practitioners assert that if you have the rudiments of genetic variation, selection, and heredity then one must have evolution.[i] One can apply this same evolutionary algorithm and other BE characteristics to the transmission of memes.[ii] Memetic Theory can potentially provide mathematical modeling tools and concepts to assist Information Operations (IO) officers when conducting IIA. To better understand the potential applications of Memetic Theory, one must first understand its history and characteristics.

First conceptualized in his 1976 book, The Selfish Gene, zoologist Richard Dawkins theorized that, much like the transmission of genetic information from parent to child or from a virus to its host, thoughts, ideas, and culture are replicated and transmitted from one mind to another using a process similar to that of BE. He named the unit of transmitted information "meme".[iii]

We need a name for the new replicator, a noun that conveys the idea of a unit of cultural transmission, or a unit of imitation. 'Mimeme' comes from a suitable Greek root, but I want a monosyllable that sounds a bit like 'gene'. I hope my classicist friends will forgive me if I abbreviate mimeme to meme. ... Examples of memes are tunes, ideas, catch-phrases, clothes fashions, ways of making pots or of building arches. Just as genes propagate themselves in the gene pool by leaping from body to body via sperms or eggs, so memes propagate themselves in the meme pool by leaping from brain to brain via a process which, in the broad sense, can be called imitation.[iv]

Memetics, therefore, is the proposed science that studies the replication, evolution, and diffusion of memes into a population, with replication being the key element to the concept.

Following Dawkins' model, a replicator, either a gene or a meme, is a "system that is able to make copies of itself, typically with the help of some other system".[v] So, a meme, or unit of information, acts as a replicator when it is communicated or imitated from one mind, or host, to another. Further, in accordance with Dawkins, effective replicators should possess three characteristics: longevity, fecundity, and copying-fidelity. Longevity is valuable in that the longer a replicator remains active, the more imitations or copies can be made of it. Next, a replicator's fecundity is important as a faster rate of copying translates into a more extensive dispersion. Lastly, copy-fidelity means the more exact an imitation is to its replicator, the more likely the imitation will remain accurate after several iterations of copying.[vi] With the latter three characteristics in mind, one must now look to the stages of the replication loop to gain further insight into Memetic Theory.

Building on Dawkins' work, Francis Heylighen and Klaas Chielens conjectured on the dynamics of meme replication and spread stating that to replicate successfully a meme must pass through four subsequent gates in its life-cycle, which consist of: assimilation, retention, expression, and transmission. The first stage, assimilation, begins with the "infection" of the carrier or host of the meme, and is followed by the second stage, retention, in which the host maintains possession of the meme. The third stage, expression, is the shaping and selecting of the meme from the host's memory into a comprehensible unit of information, i.e. language, writing, painting, ect. The final stage is the transmission or communication of the meme, via a chosen conduit, from the host to one or more individuals.[vii] With this general conceptual understanding of Memetic Theory and the memetic life-cycle or replication loop one can, using computational models, predict memetic patterns such as, but not limited, to memetic fitness. According to Heylighen and Chielens, fitness is the "overall success rate of a replicator, as determined by its degree of adaptation to its environment, and the three requirements of longevity, fecundity and copying-fidelity".[viii] Using a meme as the replicator, below one can express memetic fitness, F, as a function applying the memetic life-cycle with assimilation A, retention R, expression E, and transmission T.

$F(m) = A(m).R(m).E(m).T(m)$

A, being the number of memes assimilated by a host, is greater than or equal to one. R, equaling the proportion of memes retained to memory by a host, is less than or equal to one. E representing the number of times a meme is expressed to a host and, lastly, T equating to the number of potential new hosts the meme is expressed to.[ix] A, R, E, and T cannot individually equal zero, otherwise the product and the meme's fitness will be zero. IO officers can potentially apply such mathematical models, and certainly the memetic perspective, to IIA in a multitude of ways.

Memetic fitness is paramount when synchronizing our themes, messages, and talking points. Most IIA professionals no doubt prefer the information they transmit to their target audiences to possess longevity, fecundity, and copy-fidelity. For example, the memetic fitness function, F(m), can potentially provide IO officers one of many potential mathematical modeling tools to weigh and value the memes they desire to leverage against the audience, adversary, or enemy decision-maker they wish to inform or influence. However, the IO officer would have to assess and identify the values of A, R, E, and T. Determining the meme's fitness would provide the IO officer with some measure of prediction for the overall success rate of the meme prior to transmission. To assist in the meme or message design process, he or she would then be able to compare the effectiveness of different memes and mediums against each other given his or her unique information environment. Besides the modeling applications identified by this example, the concepts presented in Memetic Theory can assist in constructing IIA in the cognitive dimension.

Though Memetic Theory has a place at the Strategic and Operational levels of war, tactically, to assist in conceptual framing, IO officers can apply the principles of Memetic Theory when crafting themes, messages, and talking points in IIA. For example, concerning measures of performance (MOP), one might determine that a target failed to retain the meme because the handbill or medium for transmitting the message did not thoroughly express the meme. Alternatively, concerning measures of effectiveness (MOE) an IO officer might determine that the copy-fidelity of a meme delivered by his or her commander to the local clergy at a senior leader engagement was poorly translated culturally, resulting in the clergyman issuing an inaccurate meme to his congregation and community.[x] Analysis of MOPs and MOEs are just two examples of the many potential applications gained from the memetic perspective when conceptually framing IIA. Despite the above examples of memetic applications to IIA, there still remains much to be done in the field of Memetic Theory.

Some argue that there is little empirical data to support Memetic Theory, and that without such data memetics is rather a method of thinking than a formal scientific field of study. This viewpoint is somewhat justified, however, this multifaceted and ever evolving field continues to tread forward in its development. Although there have been several empirical studies of meme propagation conducted, there is still little consensus on the memetic selection criteria or holistic collection of characteristics that makes memes successful. A commonly agreed upon set of criteria would enable researchers and scientists to weigh and measure various memes and create a scientific method for predicting future memetic behavior.[xi] So, researchers continue to develop and socialize ontologically-based criteria which they could potentially use in further analysis of memetics. Further, reassuringly, no studies have yet to falsify Memetic Theory.[xii] Many organizations, such as the Global Brain Institute, which is a composite of influential futurists, cognitive scientists, Artificial Intelligence genii, and graph computing professionals, continue to put forth the intellectual horsepower required to expand the field into a formal science. Regardless of current empirical support, Memetic Theory offers a non-traditional cognitive framing tool that IO officers can use to better understand and conduct IIA.

As the Army pivots towards operational design as an approach to solving complex problem sets on present and future battlefields, it remains in our best interest to keep abreast of emerging thought; especially thought that is wedded to technologies and ways of thinking that are evolving at an accelerated pace.[xiii] IO officers can leverage and apply the mathematical models and the cognitive structure of Memetic Theory to assist in framing their information environment, their information-related problems, and ways and means of solving their information-related problems. Though not the quintessential "Silver Bullet" of Information-related problems, interested military leaders should self-educate themselves on Memetic Theory and, pending their desired effects, mathematically and conceptually design advantageous and friendly memes while deconstructing detrimental or adversarial memes in accordance with IIA.

End Notes

[i] Susan Blackmore, Susan Blackmore: Memes and “Temes”, 2008, TED Talks.

[ii] Daniel Dennett, Is Evolution an Algorithmic Process, 1998, Washington State University, Danze Lecture Series.

[iii] Richard Dawkins, “The Selfish Meme.” (Oxford, UK: Oxford University Press, 1976), 192.

[iv] Ibid.

[v] Francis Heylighen and Klaas Chielens, “Cultural Evolution and Memetics.” Encyclopedia of Complexity and System Science (2008): 5.

[vi] Ibid.

[vii] Ibid. 10-11.

[viii] Ibid. 2.

[ix] Ibid. 12.

[x] Department of the Army, JP 3-13, Inform and Influence Activities. (Washington, DC: Government Printing Office, January 2013), 7-2 to 7-4.

[xi] Heylighen, “Cultural Evolution and Memetics,”4, 22.

[xii] Ibid. 21.

[xiii] Department of the Army, ADRP 3-0, Unified Land Operations. (Washington, DC: Government Printing Office, May 2012), 4-1 to 4-3.

Table of Contents

Here’s How One Hacker Is Waging War on the Syrian Government

By Andrea Peterson, Washington Post, August 28 2013

As President Obama weighed U.S. air strikes in Syria this week, a lone American hacker was waging his own attack on the Syrian government. He works a white-collar job in the United States by day, while at night he’s on the digital front lines of the civil war in Syria, where hacktivists on both sides of the conflict are fighting to deliver their messages over cyberspace.

The American, who identified himself with the pseudonym “Oliver Tucket,” contacted me over the weekend. He shared copies of two Syrian government documents he said he had gleaned from a hacked server. The shy, earnest, clean-cut young professional of about 30 says he doesn’t have any specific ties to the Syrian conflict but was upset about the actions of the Syrian government and wanted to embarrass the Assad regime.

Online attacks have become one more front in modern warfare. But the Internet's global reach gives those cyber battles a more freewheeling character than conventional warfare. Smart hackers around the world can insert themselves into volatile situations to embarrass enemies, draw attention to pet causes, or cause mischief.

Tucket says he was surprised at just how weak the Syrian regime's network defenses were. Evidently, as the government has become overwhelmed with the country's raging civil war, network security hasn't been a priority. And with the U.S. government on the brink of launching airstrikes in the country, the security of Syria's IT systems might not be improved any time soon.

A digital protest

The Syrian government has never been great at securing its network. In 2012, Wikileaks released a cache of over 2.4 million e-mails from 680 Syria-related entities or domains including those associated with the ministries of presidential affairs, foreign affairs, finance, information, transport and culture. But the regime does have some hackers in its corner. A group calling itself the Syrian Electronic Army (SEA) has garnered international publicity by targeting news sites (including The Washington Post) and prominent Twitter accounts. On Tuesday, the SEA claimed responsibility for DNS hijacking attacks affecting the New York Times and Twitter Web sites.

Mike Kun, a security engineer with the customer security incident response team at cybersecurity company Akamai, notes the SEA is “pretty successful at what they're trying to do, which is share their propaganda” using social engineering attacks that target prominent social media accounts. SEA used a compromised Associated Press Twitter handle to tweet false reports of bombings at the White House earlier this year, causing a $136 billion drop in the stock market and a rash of news interest.

Tucket says he's had access to servers associated with the Syrian National Agency for Network Services for more than two months, but the SEA's recent antics drove him to approach The Washington Post. He was irritated by the amount of coverage the SEA received for an attack on The Post Web site, which briefly caused some of the online pages to redirect to a Web site supportive of the Syrian government. Tucket believes the SEA “is obviously an organized group, probably with affiliation to the Syrian government.” But he said he is “not impressed at all” with their hacking ability, which he sees as opportunistic and publicity-seeking.

Tucket also says he was motivated by reports of chemical weapons use and other acts of oppression by the Assad regime and sees his hacking prowess as his “only tool to act against repressive regimes.” Hacktivist group Anonymous claimed similar motivation for their Operation Syria activities in 2011, which took over the Syrian Defense Ministry Web site.

According to Reporters Without Borders Syria's Internet is subject to aggressive surveillance, and its “ultra-centralized Internet architecture allows the government to cut off the country from the rest of the world.” There have been several instances of Internet blackouts in Syria during the course of the civil war that reports indicate may have been initiated by the regime.

“They have no idea what is going on”

Tucket says he was active in hacker circles about 10 years ago. Then he more or less “went clean” until two or three months ago, when news about the Middle East pushed him back into his old habits. He started poking around to see if he could gain control of the Syrian top level domain, thinking, “I could start my own .sy domain, and give it to the rebels.”

Before long, he says, he was inside some of the internal networks associated with the government-run telecommunications establishment. From that digital perch, he says, it was obvious “they're not taking [security] seriously” and “have no idea what is going on in their network.” He reports that much of the email traffic flowing around was not encrypted, and he was able to read messages – including one mentioning the administrative password for one server domain associated with the regime, syrgov.sy.

Tucket took administrative control of the syrgov.sy domain over the weekend. The website that once housed a login page for a Syrian government webmail pilot product started alternatively pointing towards The Drudge Report and an Israeli government web portal. The link to Israel is pure trolling—Tucket says he hoped it would be like “a slap in the face” to the Syrian regime. He also changed the mail server associated with the domain to mail.gov.il on Sunday. He later changed it to mail.navy.cn, a mail server of the Chinese navy.

It does not appear that either of these servers were configured to accept email for the domain syrgov.sy, but they may be able to collect IP addresses and the login information from failed attempts to access syrgov.sy mail accounts.

Kun, the Akamai security expert, reviewed technical information provided to the Post by Tucket and says that it's “likely he has compromised the server itself.” Three other security experts consulted by the Post shared his assessment. That suggests Tucket has access to data on the server, control over the websites hosted on it, and the ability to read the emails from and to the server. Tucket appears to have maintained his power over the server for days, although the Syrian government seems to have regained control as of Wednesday morning.

It remains unclear how important of a site syrgov.sy is, or if mailboxes related to it remained actively in use up until its compromise. But emails using that domain show up multiple times in the Wikileaks Syrian documents. An “Official SEA” twitter account responding to taunts from Tucket about the hack claimed “all Syrian government websites” were emptied of important data (presumably after Wikileaks collected and published so much of it).

Tucket provided the Post with two documents as evidence of the significance of activity on the domain and his access to internal networks. One document is an Arabic language review of vulnerabilities in web sites identified by the Syrian National Agency for Network Services’s Information Security Center in the first half of 2013, the other a map of an internal network for the Syrian telecommunications establishment including passwords. Two independent experts who reviewed the documents for The Post on background say they appear legitimate.

The new battlefield?

Tucket says few people know about his hacking hobby besides his mother and a few close friends, and he is “not worried at all about being traced or tracked” because his “footprint is pretty small.” While his current focus is on Syria, he also says he has successfully dug into a site associated with the Iranian Foreign Ministry within the past few months, as well as domains in China. He says that learning his way around the latter networks is “like learning the Internet all over again.”

He doesn’t claim an affiliation with Anonymous or have much to say about Edward Snowden’s National Security Agency leaks. But he does see himself as part of a larger movement toward cyber conflict, agreeing that the Internet is the “next battlefield.”

This form of cyber warfare has been drawing concern. Then-U.S. Defense Secretary Leon Panetta warned, perhaps hyperbolically, about the threat of a “cyber Pearl Harbor” last year. And lone wolves like Tucker, hacktivist collectives like SEA and Anonymous, and more organized actors like APT1 (which allegedly has ties to the Chinese government) have all made headlines for major hacking actions in recent months and years.

Kun notes that while Syria is a prime example, across cyberspace “different hackers who have allegiances to different nation states are hacking other ones.”

“Whenever you get people with strong opinions,” Kun says, “you get these sort of hacker wars going on where some sides are pushing to do one thing or the other, but they’re all trying to get their message out and get it noticed any way that they can.“

Still, it’s important to remember what hackers like Tucket cannot do by Internet. They can’t bomb enemy targets, capture and hold territory or repel invading forces.

Tucket himself notes the limitations of his hacking activities in an e-mail. “While this is pale and rather insignificant in comparison to what is happening on the ground in Syria,” he writes, “this is my very small contribution to their struggle.”

Table of Contents