Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**

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

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

ARSTRAT IO Newsletter Online

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

Table of Contents

Vol. 13, no. 05 (February-March 2013)

10th Annual Army Global Information Operations Conference Cancelled

Due to the current fiscal constraints, and the most recent Army guidance outlined in the SA and CSA Risk Mitigation Memo, we cancelled the 10th Annual Army Global Information Operations Conference this year. We will look at dates for the conference next year and announce those later.

More information will be provided later once we complete the approval process. Points of contact are Scott Janzen scott.c.janzen.civ@mail.mil, 719-554-8890; or Jose Carrington, jose.carrington.civ@mail.mil, 719-554-8880.

Table of Contents

North Korea propaganda taken off YouTube after Activision complaint

A propaganda video from the North Korean authorities has been removed from YouTube following a copyright claim by games maker Activision.

The clip showed a young man dreaming about a North Korean space shuttle destroying a city that resembles New York.

But the footage of burning buildings was taken from Activision's top selling game, Call of Duty.

North Korea insists its space programme is for peaceful purposes.

But the country's intent - particularly towards South Korea - has raised concerns leader Kim Jong-un has plans for a ballistic missile system.

The video was posted on Saturday by North Korea's official Pyongyang YouTube channel.

'Wickedness is ablaze'

It shows a futuristic space craft flying around the world and eventually over a city. The buildings are then seen crumbling amid fires and missile attacks.

However, the dramatic images were soon recognised as having been lifted from Call of Duty: Modern Warfare 3, a multi-million selling game released in 2011.

The video contained subtitles, in Korean, which read: "Somewhere in the United States, black clouds of smoke are billowing. It seems that the nest of wickedness is ablaze with the fire started by itself."

Footage of North Korea's own recent rocket launches is also shown in the clip.

Intriguingly, the anti-US footage is sound-tracked by an instrumental version of We Are The World, the 1985 charity single written by Michael Jackson and Lionel Richie.

By Tuesday, the video had been blocked, with a message notifying users of Activision's complaint shown in its place.

On Wednesday it appeared that the North Korean channel's administrators had removed the video completely.

Table of Contents

US Said To Be Target of Massive Cyber-Espionage Campaign

By Ellen Nakashima, Washington Post, 11 Feb 2013

A new intelligence assessment has concluded that the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country’s economic competitiveness, according to individuals familiar with the report.

The National Intelligence Estimate identifies China as the country most aggressively seeking to penetrate the computer systems of American businesses and institutions to gain access to data that could be used for economic gain.

The report, which represents the consensus view of the U.S. intelligence community, describes a wide range of sectors that have been the focus of hacking over the past five years, including energy, finance, information technology, aerospace and automotives, according to the individuals familiar with the report, who spoke on the condition of anonymity about the classified document. The assessment does not quantify the financial impact of the espionage, but outside experts have estimated it in the tens of billions of dollars.

Cyber-espionage, which was once viewed as a concern mainly by U.S. intelligence and the military, is increasingly seen as a direct threat to the nation's economic interests.

In a sign of such concerns, the Obama administration is seeking ways to counter the online theft of trade secrets, according to officials. Analysts have said that the administration's options include formal protests, the expulsion of diplomatic personnel, the imposition of travel and visa restrictions, and complaints to the World Trade Organization.

Cyber-espionage is "just so widespread that it's known to be a national issue at this point," said one administration official, who like other current and former officials interviewed spoke on the condition of anonymity to discuss internal deliberations.

The National Intelligence Estimate names three other countries — Russia, Israel and France — as having engaged in hacking for economic intelligence but makes clear that cyber-espionage by those countries pales in comparison with China's effort.

China has staunchly rejected such allegations, saying the Beijing government neither condones nor carries out computer hacking.

Dating to at least the early 1980s, China has made the acquisition of Western technology — through means licit and illicit — a centerpiece of its economic development planning. The explosion in computer use has greatly aided that transfer of technology.

China's intelligence services, as well as private companies, frequently seek to exploit Chinese citizens or people with family ties to China who can use their insider access to U.S. corporate networks to steal trade secrets using thumb drives or e-mail, according to a report by the Office of the National Counterintelligence Executive.

The National Intelligence Estimate comes at a time when the U.S. government is making a concerted effort to develop policies that address cyberthreats against the nation.

"We need the NIE on cyber for a systematic and comprehensive understanding of what the most dangerous technologies are, who are the most threatening actors and what are our greatest vulnerabilities," said former deputy defense secretary William J. Lynn III, who requested the report in 2011 but has not seen or been briefed on the contents.

Some officials have pressed for an unclassified summary to be released publicly. Michael Birmingham, a spokesman for the Office of the Director of National Intelligence, declined to comment on the report, except to say that "as a matter of policy, we do not discuss or acknowledge the existence of NIEs unless directed to do so."

A Range Of Sectors

Much of China's cyber-espionage is thought to be directed at commercial targets linked to military technology. In 2011, when Chinese hackers attacked network security company RSA Security, the technology stolen was used to penetrate military-industrial targets. Shortly after, the networks of defense contracting giant Lockheed Martin, which used RSA security tokens, were penetrated by Chinese hackers. The company said no data were taken.

Companies in other sectors also have been targeted, though the reasons for the espionage are not always related to economic interests. The New York Times, the Wall Street Journal and The Washington Post recently disclosed that they believe their networks were compromised in intrusions that originated in China.

Despite those disclosures and the growing prevalence of cyber-espionage, companies remain reluctant to report incidents.

"It's harder for companies to suggest that they haven't been attacked," the administration official said. "The question is, how do they respond when they are asked about it? Is it in their interest to work with other companies and with the government to alleviate some of the problem?"

A watershed moment came in January 2010, when the tech titan Google announced that its networks had been hacked and that the intrusions originated in China. The intruders made off with valuable source code and targeted the Gmail accounts of Chinese human rights activists and dissidents, the company announced.

In a new book, Google chief executive Eric Schmidt says China is the world's "most sophisticated and prolific" hacker, adding: "It's fair to say we're already living in an age of state-led cyberwar, even if most of us aren't aware of it."

Administration’s Response

In recognition of the growing problem, the State Department has elevated the issue to be part of its strategic security dialogue with China. Within the past year, the Justice Department has set up a program to train 100 prosecutors to bring cases related to cyber-intrusions sponsored by foreign governments.

In many ways, the moves are a response to what experts have described as the government’s earlier passivity in tackling the problem.

“The problem with foreign cyber-¬espionage is not that it is an existential threat, but that it is invisible, and invisibility promotes inaction,” a former government official said. The National Intelligence Estimate, he said, “would help remedy that” by detailing the scope of the threat.

Some experts have said that cyber-espionage’s cost to the U.S. economy might range from 0.1 percent to 0.5 percent of gross domestic product, or $25 billion to $100 billion. Other economists, while viewing the problem as significant, have pegged the losses lower.

The White House is set to soon release a trade-secrets report, compiled by U.S. Intellectual Property Enforcement Coordinator Victoria Espinel, that highlights the need for companies to work with the government to stop the pilfering, said officials familiar with the report.

The government cannot mount a case on its own. A company needs to think it was wronged, have enough evidence that can be made public and be willing to burn bridges with the country accused of the hacking, officials said.

The White House is also expected this week to issue an executive order on cybersecurity that calls for voluntary standards for critical private-sector computer systems and for enhanced sharing of threat information by the government with companies to help secure private-sector systems against cyber-intrusions.

Table of Contents

Electronic Warfare Will Be a Game-Changer in Modern Battle Zone

From The Hindu, 31 Jan 2013

In the modern battle zone, electronic warfare or EW, they say, will be a game-changer. On the sidelines of a four-day workshop in Bangalore, U.K. Revankar, top military scientist and former Director of the Defence Avionics Research Establishment (DARE), who is also president of the Association of Old Crows India Chapter, the 250-member national body of EW professionals, demystifies the world’s new weapon.

Q. Why do countries need electronic warfare?

A. It has become an essential component of military, its relevance in homeland security may be realised in the near future.

The prime job of EW is to sense the location and type of enemy radars, weapons, missiles, communication systems. Based on that information you take defensive and offensive counter measures, give it back to the enemy sensor, silence their radars or deceive their missiles and make them miss our systems.

EW, along with cyber warfare, will be an important part of future information warfare. The services are focussing on network centric warfare, where cyber radars and optical sensors will prevail.

Nowadays the IAF, for example, asks that EW systems be mounted as an essential component of its aircraft and almost all its platforms. The [ground] radar is becoming secondary.

What are these devices?

Radar warning receivers, missile warners, and communication jammers are the three main domains. Whoever responds first wins. [EW] is not an easy job.

What are the country’s strengths and gaps?

Today India is proud to have its own radars flying [on aircraft].

The BEL-made Tarang radar warner has been put on fighter planes and helicopters [for nearly a decade].

DARE is upgrading many things [for air platforms] and the Defence Electronics Research Lab for ship and ground systems. Now we are talking of having the warner and the jammer as an integrated system and trying to implement them on our LCA and Sukhoi-30 fighters.

However, we depend on the US for device technology, in fact, the whole world does. It may take us years to indigenise it totally. Which is why the thrust is on the systems side – to first [fit] the technology as a system and deliver it to the user and look into its indigenisation later.

We are excellent in design development and system engineering and in proving them on platforms. India is the EW market, people are looking this way to come and collaborate with us.

Where do we stand in manufacturing, funds support and people?

Electronic warfare is a domain where the systems and products are many, and the people are few.

For systems, we can only look at Bharat Electronics Ltd. Some private industries are coming up for sub-systems. The United States develops EW along with a ship or aircraft. We cannot afford to do it that way, but do the platform and the EW suite separately.

Funding has never been a problem. In terms of education EW is a specialised area and there is a dearth of skilled people — that is the reason for this workshop. We are 500 plus EW professionals [in the country] from the labs and services. It must grow to at least 1,000. It is essential to start [focussed] courses.

Apart from technology there is the [question of production] numbers. But we have not succeeded in the numbers game.

People in the EW area should learn that the numbers required are large; and miniaturisation. BEL and the private sector have to gear themselves up for this.

EW could form roughly 20 per cent of a defence system. It will be difficult to do without it.

There is the satellite domain also to work on. The future battle will be by and of EW experts.

Table of Contents

Army Is Gearing Up To Fight the PR War

By Walter Pincus, Washington Post, 7 Feb 2013

The U.S. Army has embraced what civilians would call public relations as a key part of military operations for the 21st-century battlefield.

"Combat power is the total means of destructive, constructive and information capabilities that a military unit or formation can apply at a given time," according to a new Army field manual released publicly last month.

Added to the traditional war elements - among them movement and maneuver, intelligence and firing against an enemy - is the new "Inform and Influence Activities" (IIA). As the manual states, IIA "is critical to understanding, visualizing, describing, directing, assessing, and leading operations toward attaining the desired end state."

I've written before about the military moving into PR. But this manual shows just how serious the Army has become about it. There's now a member of a commander's staff with a G-7 pay level whose job is for "planning, integration and synchronization of designated information-related capabilities," the manual says.

Listed on the Web site of the 2nd Infantry Division in Korea is its assistant chief of staff, G-7, who is "responsible for planning, coordinating and synchronizing Information Engagements activities of Public Affairs, Military Information Support Operations, Combat Camera and Defense Support to Public Diplomacy to amplify the strong Korean-American alliance during armistice, combat and stability operations."

The G-7 for the 3rd Infantry Division at Fort Stewart, Ga., "assesses how effectively the information themes and messages are reflected in operations . . . assesses the effectiveness of the media . . . [and] assesses how the information themes and messages impact various audiences of interest and populations in and outside the AO [area of operations]."

Two years ago, Lt. Gen. Robert L. Cashen Jr., commander of the Combined Arms Center at Fort Leavenworth in Kansas, wrote in Military Review magazine that Army doctrine would adopt words as a major war element, saying it "was validated in the crucible of operations in Iraq and Afghanistan."

In bureaucratese, he described IIA activities as employing "cooperative, persuasive and coercive means to assist and support joint, interagency, intergovernmental, and multinational partners to protect and reassure populations and isolate and defeat enemies."

Translated: Under the "inform" element, commanders will be responsible for keeping not only their own troops aware of what is going on and why, but also U.S. audiences "to the fullest extent possible," the manual states. Commanders abroad will be required to inform their foreign audiences, balancing disclosure with protecting operations.

The "influence" part is limited to foreign populations, where, according to the manual, the goal is to get them to "support U.S. objectives or to persuade those audiences to stop supporting the adversary or enemy."

The Army, like the other military services, has had PR operations for decades, but mostly they have been aimed at U.S. audiences. As the manual states, "Some people think of the information environment as a new phenomenon. In fact, it has been present throughout history and has always been an important military consideration."

When radio and then television arrived, the services used their own personnel for interviews for the public. During the Vietnam War, they offered stories that often contrasted with what reporters were providing commercial news outlets. As the war expanded, reporters who went to the front lines traveled primarily with military support.

In Desert Storm, the 1991 operation that forced Iraq out of Kuwait, reporters in the beginning had to cover the fighting far behind the lines by attending televised briefings by the U.S. commander, Gen. H. Norman Schwarzkopf. Near the end of the conflict, a few selected reporters rode with U.S. units.

As part of planning for the 2003 invasion of Iraq, the Pentagon under Defense Secretary Donald H. Rumsfeld decided to place reporters with military units. With "embedding," many reporters who had never been in the military service shared time with troops and essentially became part of the outfit they covered. It mostly worked to the Pentagon's benefit.

That lesson is key to the new manual's approach. The best way to keep Americans informed, it says, is "through the actions and words of individual soldiers." And the best way to do that is through army units that "embed media personnel into the lowest tactical levels, ensuring their safety and security."

There is to be "a culture of engagement in which soldiers and leaders confidently and comfortably engage the media as well as other audiences," the manual says.

Strategic communications came to the forefront over the past decade along with "information operations," propelled by the belief that the U.S. military has been losing the propaganda war in Afghanistan, thanks in good part to the Taliban's use of messaging. "Adversaries and enemies have proven adept at using information to gain a marked advantage over U.S. forces," the manual says.

"With the advent of the Internet and widespread availability of wireless communications and information technology, this environment has become an even more important consideration to military planning and operations than in years past," says the manual.

The Army has developed Military Information Support Operations units. These are troops trained as regional experts with language capabilities that are familiar with the religious, political, cultural and ethnic backgrounds of an area and so are prepared to shape messages to influence local perceptions and behavior.

"Victory depends on a commander's ability to shape, sway, and alter foreign audience perceptions, and ultimately behavior, especially in the area of operations," the manual says. Perhaps it's a step forward if we are using PR to win wars rather than more guns, bombs or missiles. But there needs to be more public explanation of what all this involves, who is doing it and the results so far.

The last step I remember Congress taking was to reduce Defense Department spending on strategic communications and ask for a more detailed explanation of such programs.

Table of Contents

Can Social Media Disarm Syria's Chemical Arsenal?

By Eli Lake, DailyBeast.com, 8 Feb 2013

When a bombing knocked out top Assad officials, Western intelligence agencies scrambled to find those left holding the deadly stash. Their tools: Facebook, Skype, Twitter, and more.

If you are a Syrian military officer in charge of some nasty chemical weapons, you've probably been friended or Skyped by the U.S. government. The message is simple: think twice before using or selling that mustard gas you are guarding.

On July 18, when a suicide bomber struck a meeting of Syria's security cabinet, killing the defense minister and President Bashar al-Assad's brother-in-law, it was a major victory for Syria's opposition. But it was also a cause for serious alarm at the Pentagon.

In public, Secretary of Defense Leon Panetta warned what was left of the regime's leadership to protect the state's large stockpile of chemical weapons. Privately, the U.S. intelligence community began to worry that the Syrian officials known to have the ability to authorize the use of that arsenal were now dead or gravely injured.

A scramble then ensued: who were the midlevel officers in charge of the Syrian Air Force and Army units that controlled the stocks of sarin and mustard gas the Assad regime had been compiling for decades? And who was now running the Scud missiles and bombers that would be deployed to use these chemical weapons? According to current and retired U.S. and Western intelligence and defense officials, U.S. analysts began to hunt for email addresses, Twitter handles, Facebook accounts, phone numbers, and Skype contacts for those midlevel Syrian officers. The information was then used to deliver a pointed message: the U.S. government knows who you are, and there will be consequences if you use or transfer chemical weapons.

“The people who were killed and injured in that [July 18] suicide bombing were the people who we could try to persuade not to use this stuff,” says one congressional staffer who has been briefed extensively on the program. “When that happened, we needed to find another way to get to these guys.”

The project to reach out to Syria’s midlevel officers is an important part of the Obama administration’s planning for how to prevent the use and illicit transfer of Syria’s chemical arsenal. To date, President Obama has taken a cautious approach to the civil war inside the country, offering humanitarian aid, but choosing against arming the rebels. On Thursday, outgoing Secretary of Defense Leon Panetta and Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey told the Senate Armed Services Committee that they both favored a plan developed by the CIA to arm the rebels, a plan the White House rejected.

Obama has been publicly warning of grave consequences if the Syrians use chemical weapons or transfer them to groups like Hezbollah or al Qaeda. Israel, too, is establishing its own red lines. Last week, Israeli jets hit a convoy containing SA-17 rockets that was reportedly on the way to Hezbollah in Lebanon.

For now, it’s unlikely Obama would authorize airstrikes on the known weapons depots and chemical labs. Instead, the hope is that Syrian officers can be persuaded to safeguard the material if the regime collapses.

Charles Duelfer, a former CIA officer who served as the deputy chairman of the U.N. weapons-inspection team for Iraq and later as the head of the U.S. effort to find those weapons after the 2003 invasion, said there were two kinds of goals these types of operations can accomplish. “You want to transmit a message of deterrence,” he says. “It’s not just Bashar at the top that will be held responsible, it’s others down the food chain, too. You also want to know where the stuff is.”

The effort to reach out to midlevel officers is separate from other initiatives by the Syrian opposition to persuade officers to defect. The initiative to contact the Syrian officers, according to U.S. and Western officials, has been aided by Israel’s Unit 8200, the section of the Israel Defense Forces in charge of signal intelligence, or the monitoring of electronic communications.

Israel and the U.S. have utilized similar strategies in the past. Before the 1991 Gulf War and the 2003 invasion of Iraq, there was an intelligence operation to contact midlevel officers in charge of battalions and smaller units to persuade them to stand down—with the promise of better treatment later on. Israel sent text messages to the cellphones of Gazans in 2008 during Operation Cast Lead, warning of aerial bombardments.

For much of 2012, American diplomats also tried to work through Russia to secure Syria’s stash. During the Cold War, the Soviet Union trained Syria’s military and internal security services, and those relationships continued after the collapse of the U.S.S.R. Though high-level Russians have warned President Assad and other Syrians against using chemical weapons, U.S. officials say they don’t know how effective this approach might be.

For the West, part of the problem is that Syria’s chemical-weapons infrastructure is largely secret. It was not until July of last year that any Syrian official even acknowledged the nation had such weapons. On July 23, Jihad Maqdisi, a spokesman for the Syrian foreign ministry, warned that Syria would deploy its unconventional weapons only if the country is invaded and would not use the weapons against civilians.

“We’ve been watching Syria’s biological- and chemical-weapons programs for a lengthy period of time with concern,” says Paula DeSutter, the former assistant secretary of state for verification and compliance in the George W. Bush administration. “Anyone pursuing these types of programs will do what they can to hide as much information as possible about their program, locations, and use protocol.”

It remains unclear what Damascus is up to. In July, U.S. intelligence satellites began to detect Syrian units moving Scuds closer to the country’s Turkish border and the border with Israel, current and former U.S. intelligence officials says. But in the last three months, U.S. and Western intelligence agencies have watched Syrian forces moving chemical weapons into fewer locations than before, these officials say.

Table of Contents

Propaganda Programs Hard To Justify, Panetta Says

By Tom Vanden Brook, USA TODAY, February 2, 2013

WASHINGTON — Defense Secretary Leon Panetta said he is skeptical of the benefits the Pentagon's propaganda programs provide and added that the military struggles to gauge their effectiveness.

Propaganda can also be dangerous, he said in an interview with USA TODAY, referring to the smear attack against the newspaper by the owner of the military's top propaganda contractor.

"It's always been tough to quantify, frankly," Panetta said. "I've always been a little skeptical about how much good you can get out of that. There are instances where it can serve a purpose, and it can help as a way to defeat our enemies if it's used effectively. I think there are dangers associated with it, that you just have to continue to be very vigilant about, because it can be misused as we saw take place in your area. That's the kind of thing that we just have to be very careful about."

An investigation last year by USA TODAY found that the Pentagon has spent hundreds of millions of dollars on propaganda campaigns in Iraq and Afghanistan, much of it on poorly tracked marketing campaigns that the military refers to as "information operations."

The programs include leaflets and billboards encouraging Afghans to support their government. Millions are also spent on radio and television broadcasts and advertisements whose U.S. sponsorship is often hidden from Afghans because, military officials acknowledge, the information wouldn't be trusted if Afghans knew the source of funding. The Pentagon relies heavily on contractors to produce the propaganda, and has allowed the private firms to grade their own work.

Micah Zenko, a national security expert at the Council on Foreign Relations, a think tank, said the military must inform the public about its actions openly and honestly, not market them through contractors.

"The Pentagon has an obligation to the American people, and the world, to provide information and tell its story — if nothing else to counter myths and misinformation," Zenko said in an e-mail. "But it should only do so in an open and transparent way. Using third-party contractors to shape public opinion is dishonest and unethical."

USA TODAY found that the owners of the top propaganda contractor in Afghanistan, Leonie Industries, had failed to pay $4 million in federal taxes on time despite earning more than $200 million in contracts from the government. Their tax bills were paid after the story was published.

Shortly after USA TODAY made inquiries about the tax bills, fake Facebook and Twitter accounts, as well as phony fan club websites, were set up to disparage USA TODAY reporters. The co-owner of the company, Camille Chidiac, admitted to setting up some of the sites but said he did not use company resources in doing so. He had been suspended from receiving federal contracts because of the campaign, but the military lifted the suspension late last year.

The Pentagon's inspector general has launched a criminal investigation of Leonie and its owners. The company continues its work in Afghanistan.

The Pentagon, meantime, continues to struggle to understand what value its propaganda programs provide, Panetta said.

"Whatever we do, if we're using taxpayer money, I think we've got to be able to show the American taxpayer that we're getting something back for the dollars invested, which means that I've got to be able to quantify what is it we are getting back for the dollars that are spent," Panetta said. "I have to tell you in this area it's tough to quantify."

Table of Contents

Software That Tracks People On Social Media Created By Defence Firm

By Ryan Gallagher, the Guardian, 10 February 2013

Link to video: How Raytheon software tracks you online

A multinational security firm has secretly developed software capable of tracking people's movements and predicting future behaviour by mining data from social networking websites.

A video obtained by the Guardian reveals how an "extreme-scale analytics" system created by Raytheon, the world's fifth largest defence contractor, can gather vast amounts of information about people from websites including Facebook, Twitter and Foursquare.

Raytheon says it has not sold the software – named Riot, or Rapid Information Overlay Technology – to any clients.

But the Massachusetts-based company has acknowledged the technology was shared with US government and industry as part of a joint research and development effort, in 2010, to help build a national security system capable of analysing "trillions of entities" from cyberspace.

The power of Riot to harness popular websites for surveillance offers a rare insight into controversial techniques that have attracted interest from intelligence and national security agencies, at the same time prompting civil liberties and online privacy concerns.

The sophisticated technology demonstrates how the same social networks that helped propel the Arab Spring revolutions can be transformed into a "Google for spies" and tapped as a means of monitoring and control.

Using Riot it is possible to gain an entire snapshot of a person's life – their friends, the places they visit charted on a map – in little more than a few clicks of a button.

In the video obtained by the Guardian, it is explained by Raytheon's "principal investigator" Brian Urch that photographs users post on social networks sometimes contain latitude and longitude details – automatically embedded by smartphones within "exif header data."

Riot pulls out this information, showing not only the photographs posted onto social networks by individuals, but also the location at which the photographs were taken.

"We're going to track one of our own employees," Urch says in the video, before bringing up pictures of "Nick," a Raytheon staff member used as an example target. With information gathered from social networks, Riot quickly reveals Nick frequently visits Washington Nationals Park, where on one occasion he snapped a photograph of himself posing with a blonde haired woman.

"We know where Nick's going, we know what Nick looks like," Urch explains, "now we want to try to predict where he may be in the future."

Riot can display on a spider diagram the associations and relationships between individuals online by looking at who they have communicated with over Twitter. It can also mine data from Facebook and sift GPS location information from Foursquare, a mobile phone app used by more than 25 million people to alert friends of their whereabouts. The Foursquare data can be used to display, in graph form, the top 10 places visited by tracked individuals and the times at which they visited them.

The video shows that Nick, who posts his location regularly on Foursquare, visits a gym frequently at 6am early each week. Urch quips: "So if you ever did want to try to get hold of Nick, or maybe get hold of his laptop, you might want to visit the gym at 6am on a Monday."

Mining from public websites for law enforcement is considered legal in most countries. In February last year, for instance, the FBI requested help to develop a social-media mining application for monitoring "bad actors or groups".

However, Ginger McCall, an attorney at the Washington-based Electronic Privacy Information Centre, said the Raytheon technology raised concerns about how troves of user data could be covertly collected without oversight or regulation.

"Social networking sites are often not transparent about what information is shared and how it is shared," McCall said. "Users may be posting information that they believe will be viewed only by their friends, but instead, it is being viewed by government officials or pulled in by data collection services like the Riot search."

Raytheon, which made sales worth an estimated $25bn (£16bn) in 2012, did not want its Riot demonstration video to be revealed on the grounds that it says it shows a "proof of concept" product that has not been sold to any clients.

Jared Adams, a spokesman for Raytheon's intelligence and information systems department, said in an email: "Riot is a big data analytics system design we are working on with industry, national labs and commercial partners to help turn massive amounts of data into useable information to help meet our nation's rapidly changing security needs.

"Its innovative privacy features are the most robust that we're aware of, enabling the sharing and analysis of data without personally identifiable information [such as social security numbers, bank or other financial account information] being disclosed."

In December, Riot was featured in a newly published patent Raytheon is pursuing for a system designed to gather data on people from social networks, blogs and other sources to identify whether they should be judged a security risk.

In April, Riot was scheduled to be showcased at a US government and industry national security conference for secretive, classified innovations, where it was listed under the category "big data – analytics, algorithms."

According to records published by the US government's trade controls department, the technology has been designated an "EAR99" item under export regulations, which means it "can be shipped without a licence to most destinations under most circumstances".

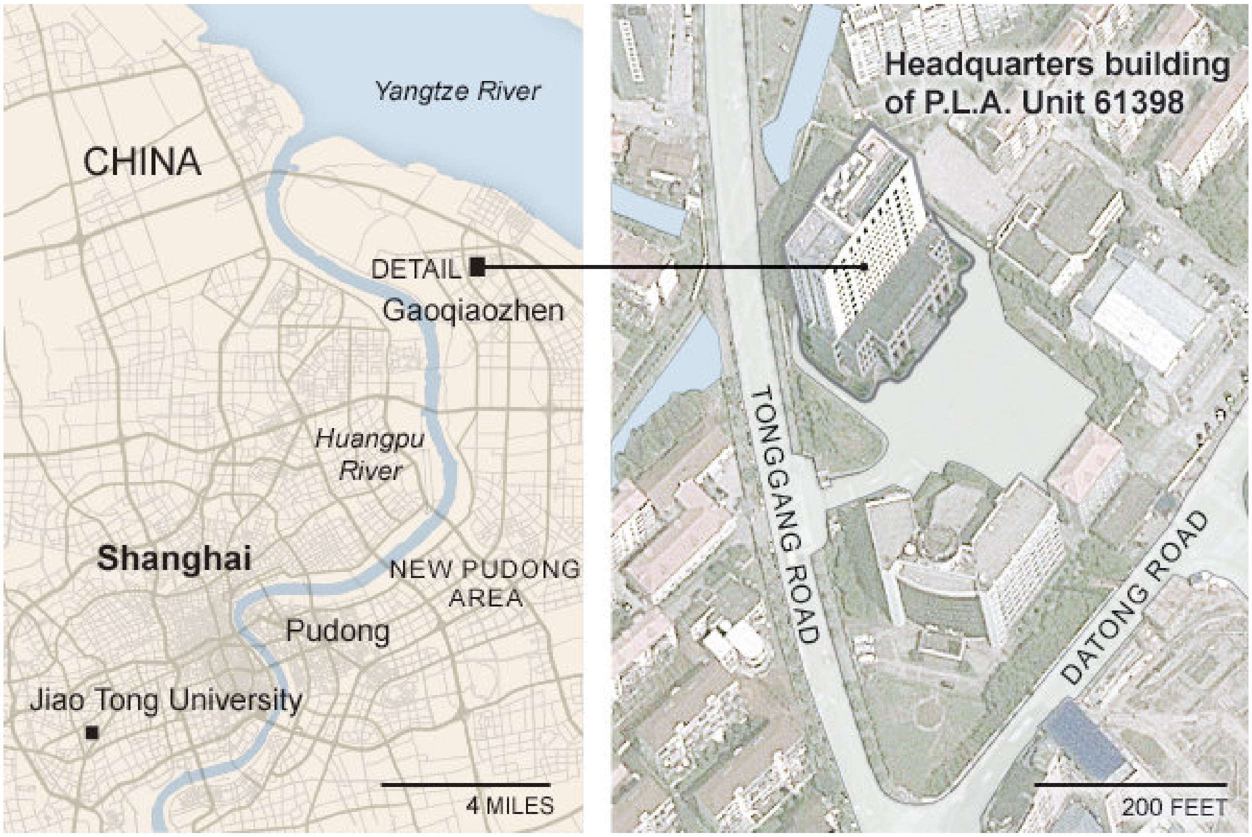
Table of Contents

Chinese Army Unit Is Seen As Tied To Hacking Against U.S.

By David E. Sanger, David Barboza and Nicole Perlroth, New York Times, 19 Feb 2013

On the outskirts of Shanghai, in a run-down neighborhood dominated by a 12-story white office tower, sits a People's Liberation Army base for China's growing corps of cyberwarriors.

The building off Datong Road, surrounded by restaurants, massage parlors and a wine importer, is the headquarters of P.L.A. Unit 61398. A growing body of digital forensic evidence — confirmed by American intelligence officials who say they have tapped into the activity of the army unit for years — leaves little doubt that an overwhelming percentage of the attacks on American corporations, organizations and government agencies originate in and around the white tower.



An unusually detailed 60-page study, to be released Tuesday by Mandiant, an American computer security firm, tracks for the first time individual members of the most sophisticated of the Chinese hacking groups — known to many of its victims in the United States as "Comment Crew" or "Shanghai Group" — to the doorstep of the military unit's headquarters. The firm was not able to place the hackers inside the 12-story building, but makes a case there is no other plausible explanation for why so many attacks come out of one comparatively small area.

"Either they are coming from inside Unit 61398," said Kevin Mandia, the founder and chief executive of Mandiant, in an interview last week, "or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood."

Other security firms that have tracked "Comment Crew" say they also believe the group is state-sponsored, and a recent classified National Intelligence Estimate, issued as a consensus document for all 16 of the United States intelligence agencies, makes a strong case that many of these hacking groups are either run by army officers or are contractors working for commands like Unit 61398, according to officials with knowledge of its classified content.

Mandiant provided an advance copy of its report to The New York Times, saying it hoped to "bring visibility to the issues addressed in the report." Times reporters then tested the conclusions with other experts, both inside and outside government, who have examined links between the hacking groups and the army (Mandiant was hired by The New York Times Company to investigate a sophisticated Chinese-origin attack on its news operations, but concluded it was not the work of Comment Crew, but another Chinese group. The firm is not currently working for the Times Company but it is in discussions about a business relationship.)

While Comment Crew has drained terabytes of data from companies like Coca-Cola, increasingly its focus is on companies involved in the critical infrastructure of the United States — its electrical power grid, gas lines and waterworks. According to the security researchers, one target was a company with remote access to more than 60 percent of oil and gas pipelines in North America. The unit was also among those that attacked the computer security firm RSA, whose computer codes protect confidential corporate and government databases.

Contacted Monday, officials at the Chinese embassy in Washington again insisted that their government does not engage in computer hacking, and that such activity is illegal. They describe China itself as a victim of computer hacking, and point out, accurately, that there are many hacking groups inside the United States. But in recent years the Chinese attacks have grown significantly, security researchers say. Mandiant has detected more than 140 Comment Crew intrusions since 2006. American intelligence agencies and private security firms that track many of the 20 or so other Chinese groups every day say those groups appear to be contractors with links to the unit.

While the unit's existence and operations are considered a Chinese state secret, Representative Mike Rogers of Michigan, the Republican chairman of the House Intelligence Committee, said in an interview that the Mandiant report was "completely consistent with the type of activity the Intelligence Committee has been seeing for some time."

The White House said it was "aware" of the Mandiant report, and Tommy Vietor, the spokesman for the National Security Council, said, "We have repeatedly raised our concerns at the highest levels about cybertheft with senior Chinese officials, including in the military, and we will continue to do so."

The United States government is planning to begin a more aggressive defense against Chinese hacking groups, starting on Tuesday. Under a directive signed by President Obama last week, the government plans to share with American Internet providers information it has gathered about the unique digital signatures of the largest of the groups, including Comment Crew and others emanating from near where Unit 61398 is based.

But the government warnings will not explicitly link those groups, or the giant computer servers they use, to the Chinese army. The question of whether to publicly name the unit and accuse it of widespread theft is the subject of ongoing debate.

"There are huge diplomatic sensitivities here," said one intelligence official, with frustration in his voice.

But Obama administration officials say they are planning to tell China's new leaders in coming weeks that the volume and sophistication of the attacks have become so intense that they threaten the fundamental relationship between Washington and Beijing.

The United States government also has cyberwarriors. Working with Israel, the United States has used malicious software called Stuxnet to disrupt Iran's uranium enrichment program. But government officials insist they operate under strict, if classified, rules that bar using offensive weapons for nonmilitary purposes or stealing corporate data.

The United States finds itself in something of an asymmetrical digital war with China. "In the cold war, we were focused every day on the nuclear command centers around Moscow," one senior defense official said recently. "Today, it's fair to say that we worry as much about the computer servers in Shanghai."

A Shadowy Unit

Unit 61398 — formally, the 2nd Bureau of the People's Liberation Army's General Staff Department's 3rd Department — exists almost nowhere in official Chinese military descriptions. Yet intelligence analysts who have studied the group say it is the central element of Chinese computer espionage. The unit was described in 2011 as the "premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence" by the Project 2049 Institute, a nongovernmental organization in Virginia that studies security and policy issues in Asia.

While the Obama administration has never publicly discussed the Chinese unit's activities, a secret State Department cable written the day before Barack Obama was elected president in November 2008 described at length American concerns about the group's attacks on government sites. (At the time American intelligence agencies called the unit "Byzantine Candor," a code word dropped after the cable was published by WikiLeaks.)

The Defense Department and the State Department were particular targets, the cable said, describing how the group's intruders send e-mails, called "spearphishing" attacks, that placed malware on target computers once the recipient clicked on them. From there, they were inside the systems.

American officials say that a combination of diplomatic concerns and the desire to follow the unit's activities have kept the government from going public. But Mandiant's report is forcing the issue into public view.

For more than six years, Mandiant tracked the actions of Comment Crew, so named for the attackers' penchant for embedding hidden code or comments into Web pages. Based on the digital crumbs the group left behind — its attackers have been known to use the same malware, Web domains, Internet protocol addresses, hacking tools and techniques across attacks — Mandiant followed 141 attacks by the group, which it called "A.P.T. 1" for Advanced Persistent Threat 1.

"But those are only the ones we could easily identify," said Mr. Mandia. Other security experts estimate that the group is responsible for thousands of attacks.

As Mandiant mapped the Internet protocol addresses and other bits of digital evidence, it all led back to the edges of Pudong district of Shanghai, right around the Unit 61398 headquarters. The group's report, along with 3,000 addresses and other indicators that can be used to identify the source of attacks, concludes "the totality of the evidence" leads to the conclusion that "A.P.T. 1 is Unit 61398."

Mandiant discovered that two sets of I.P. addresses used in the attacks were registered in the same neighborhood as Unit 61398's building.

"It's where more than 90 percent of the attacks we followed come from," said Mr. Mandia.

The only other possibility, the report concludes with a touch of sarcasm, is that "a secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multiyear enterprise-scale computer espionage campaign right outside of Unit 61398's gates."

The most fascinating elements of the Mandiant report follow the keystroke-by-keystroke actions of several of the hackers who the firm believes work for the P.L.A. Mandiant tracked their activities from inside the computer systems of American companies they were invading. The companies had given Mandiant investigators full access to rid them of the Chinese spies.

One of the most visible hackers it followed is UglyGorilla, who first appeared on a Chinese military forum in January 2004, asking whether China has a "similar force" to the "cyber army" being set up by the American military.

By 2007 UglyGorilla was turning out a suite of malware with what the report called a "clearly identifiable signature." Another hacker, called "DOTA" by Mandiant, created e-mail accounts that were used to plant malware. That hacker was tracked frequently using a password that appeared to be based on his military unit's designation. DOTA and UglyGorilla both used the same I.P. addresses linked back to Unit 61398's neighborhood.

Mandiant discovered several cases in which attackers logged into their Facebook and Twitter accounts to get around China's firewall that blocks ordinary citizen's access, making it easier to track down their real identities.

Mandiant also discovered an internal China Telecom memo discussing the state-owned telecom company's decision to install high-speed fiber-optic lines for Unit 61398's headquarters.

China's defense ministry has denied that it is responsible for initiating attacks. "It is unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence," it said last month, one of the statements that prompted Mandiant to make public its evidence.

Escalating Attacks

Mandiant believes Unit 61398 conducted sporadic attacks on American corporate and government computer networks; the earliest it found was in 2006. Two years ago the numbers spiked. Mandiant discovered some of the intrusions were long-running. On average the group would stay inside a network, stealing data and passwords, for a year; in one case it had access for four years and 10 months.

Mandiant has watched the group as it has stolen technology blueprints, manufacturing processes, clinical trial results, pricing documents, negotiation strategies and other proprietary information from more than 100 of its clients, mostly in the United States. Mandiant identified attacks on 20 industries, from military contractors to chemical plants, mining companies and satellite and telecommunications corporations.

Mandiant's report does not name the victims, who usually insist on anonymity. A 2009 attack on Coca-Cola coincided with the beverage giant's failed attempt to acquire the China Huiyuan Juice Group for $2.4 billion, according to people with knowledge of the results of the company's investigation.

As Coca-Cola executives were negotiating what would have been the largest foreign purchase of a Chinese company, Comment Crew was busy rummaging through their computers in an apparent effort to learn more about Coca-Cola's negotiation strategy.

The attack on Coca-Cola began, like hundreds before it, with a seemingly innocuous e-mail to an executive that was, in fact, a spearphishing attack. When the executive clicked on a malicious link in the e-mail, it gave the attackers a foothold inside Coca-Cola's network. From inside, they sent confidential company files through a maze of computers back to Shanghai, on a weekly basis, unnoticed.

Two years later, Comment Crew was one of at least three Chinese-based groups to mount a similar attack on RSA, the computer security company owned by EMC, a large technology company. It is best known for its SecurID token, carried by employees at United States intelligence agencies, military contractors and many major companies. (The New York Times also uses the firm's tokens to allow access to its e-mail and production systems remotely.) RSA has offered to replace SecurID tokens for customers and said it had added new layers of security to its products.

As in the Coca-Cola case, the attack began with a targeted, cleverly fashioned poisoned e-mail to an RSA employee. Two months later, hackers breached Lockheed Martin, the nation's largest defense contractor, partly by using the information they gleaned from the RSA attack.

Mandiant is not the only private firm tracking Comment Crew. In 2011, Joe Stewart, a Dell SecureWorks researcher, was analyzing malware used in the RSA attack when he discovered that the attackers had used a hacker tool to mask their true location.

When he reverse-engineered the tool, he found that the vast majority of stolen data had been transferred to the same range of I.P. addresses that Mandiant later identified in Shanghai.

Dell SecureWorks says it believed Comment Crew includes the same group of attackers behind Operation Shady RAT, an extensive computer espionage campaign uncovered in 2011 in which more than 70 organizations over a five-year period, including the United Nations, government agencies in the United States, Canada, South Korea, Taiwan and Vietnam were targeted.

Infrastructure at Risk

What most worries American investigators is that the latest set of attacks believed coming from Unit 61398 focus not just on stealing information, but obtaining the ability to manipulate American critical infrastructure: the power grids and other utilities.

Staff at Digital Bond, a small security firm that specializes in those industrial-control computers, said that last June Comment Crew unsuccessfully attacked it. A part-time employee at Digital Bond received an e-mail that appeared to come from his boss, Dale Peterson. The e-mail, in perfect English, discussed security weaknesses in critical infrastructure systems, and asked the employee to click a link to a document for more information. Mr. Peterson caught the e-mail and shared it with other researchers, who found the link contained a remote-access tool that would have given the attackers control over the employee's computer and potentially given them a front-row seat to confidential information about Digital Bond's clients, which include a major water project, a power plant and a mining company.

Jaime Blasco, a security researcher at AlienVault, analyzed the computer servers used in the attack, which led him to other victims, including the Chertoff Group. That firm, headed by the former secretary of the Department of Homeland Security, Michael Chertoff, has run simulations of an extensive digital attack on the United States. Other attacks were made on a contractor for the National Geospatial-Intelligence Agency, and the National Electrical Manufacturers Association, a lobbying group that represents companies that make components for power grids. Those organizations confirmed they were attacked but have said they prevented attackers from gaining access to their network.

Mr. Blasco said that, based on the forensics, all the victims had been hit by Comment Crew. But the most troubling attack to date, security experts say, was a successful invasion of the Canadian arm of Telvent. The company, now owned by Schneider Electric, designs software that gives oil and gas pipeline companies and power grid operators remote access to valves, switches and security systems.

Telvent keeps detailed blueprints on more than half of all the oil and gas pipelines in North and South America, and has access to their systems. In September, Telvent Canada told customers that attackers had broken into its systems and taken project files. That access was immediately cut, so that the intruders could not take command of the systems.

Martin Hanna, a Schneider Electric spokesman, did not return requests for comment, but security researchers who studied the malware used in the attack, including Mr. Stewart at Dell SecureWorks and Mr. Blasco at AlienVault, confirmed that the perpetrators were the Comment Crew.

"This is terrifying because — forget about the country — if someone hired me and told me they wanted to have the offensive capability to take out as many critical systems as possible, I would be going after the vendors and do things like what happened to Telvent," Mr. Peterson of Digital Bond said. "It's the holy grail."

Mr. Obama alluded to this concern in the State of the Union speech, without mentioning China or any other nation. "We know foreign countries and companies swipe our corporate secrets," he said. "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems. We cannot look back years from now and wonder why we did nothing."

Mr. Obama faces a vexing choice: In a sprawling, vital relationship with China, is it worth a major confrontation between the world's largest and second largest economy over computer hacking?

A few years ago, administration officials say, the theft of intellectual property was an annoyance, resulting in the loss of billions of dollars of revenue. But clearly something has changed. The mounting evidence of state sponsorship, the increasing boldness of Unit 61398, and the growing threat to American infrastructure are leading officials to conclude that a far stronger response is necessary.

"Right now there is no incentive for the Chinese to stop doing this," said Mr. Rogers, the House intelligence chairman. "If we don't create a high price, it's only going to keep accelerating."

Table of Contents

Report Ties Cyberattacks on U.S. Computers to Chinese Military

By William Wan and Ellen Nakashima, Washington Post, February 19, 10:01 AM

BEIJING — A U.S. security firm has linked China's military to cyberattacks on more than 140 U.S. and other foreign corporations and entities, according to a report released Tuesday.

The 60-page study by investigators at the Alexandria-based Mandiant security firm presents one of the most comprehensive and detailed analyses to date tracing corporate cyber-espionage to the doorstep of Chinese military facilities. And it calls into question China's repeated denials that its military is engaged in such activities.

The document, first reported by the New York Times, draws on data Mandiant collected from what the company said were "intrusions against nearly 150 victims over seven years." Mandiant traced the attacks back to a single group it designated "Advanced Persistent Threat 1," or "APT1," and now has identified the group as a Chinese military unit within the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department, going by the designation "Unit 61398."

Analysts have long linked the unit to the Chinese military's 3rd Department, and to extensive cyber-espionage. But what Mandiant has done is connect the dots and add new ones by locating the Internet protocol addresses used in commercial cyberattacks, placing them on a map and linking that information to open-source data about people associated with the unit.

"Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries," the firm said in its report. Of those victims, 87 percent "are headquartered in countries where English is the native language," it said.

Mandiant did not name the victims but said 115 of them are located in the United States, two in Canada and five in Britain. Of the 19 others, all but two operate in English. The report lists three victims each in Israel and India, two each in Taiwan, Singapore and Switzerland, and one each in Norway, Belgium, France, Luxembourg, Japan, South Africa and the United Arab Emirates.

These targeted entities include "international cooperation and development agencies, foreign governments in which English is one of multiple official languages, and multinational conglomerates that primarily conduct their business in English," the report said.

The top sectors targeted by the APT1 cyber-espionage campaign, Mandiant said, are information technology, aerospace, public administration, satellites and telecommunications and scientific research and consulting.

"We have figured things out in an unclassified way that the government has known through classified means," said Richard Bejtlich, Mandiant chief security officer, adding that the company shared the study with U.S. intelligence agencies before it was released.

The unit is just one of dozens working for the Chinese military in cyber-espionage all over the country, analysts say. There are other units within the General Staff Department's 2nd Department, which conducts military intelligence, and within the Ministry of State Security, which conducts internal counterintelligence and external espionage, according to analysts.

APT1, also dubbed “Comment Crew” by security companies that have studied its tactics, focuses on commercial targets overseas, which makes its work more visible to the security firms tracking the intrusions. Chinese units that focus on military and intelligence targets are less visible to the cyber-security companies.

“Once APT1 has compromised a network, they repeatedly monitor and steal proprietary data and communications from the victim for months or even years,” Mandiant said. It said the activity it has uncovered appears to represent “only a small fraction of the cyber espionage that APT1 has committed.”

The Chinese military has repeatedly denounced accusations that it is engaging in cyber-espionage, and did so again Tuesday.

“Similar to other countries, China faces serious threats from cyberattack and is one of the main victims of cyberattacks in the world,” the Ministry of Defense said. “The Chinese army never supported any hacking activities. The accusation that the Chinese military engaged in cyberattacks is neither professional nor in accordance with facts. “

Chinese Foreign Ministry spokesman Hong Lei on Tuesday also challenged the report’s findings. “Hacking attacks are transnational and anonymous,” and determining their origins is extremely difficult, he said. “We don’t know how the evidence in this so-called report can be tenable.”

Mandiant investigators said they based their conclusion in part by tracing an overwhelming number of cyberattacks by the APT1 group to networks serving a small area on the edges of Shanghai — the same area where Unit 61398 is believed to be operating in a 12-story building. It also found evidence that China Telecom had provided special high-speed fiber optic lines for those headquarters in the name of national defense.

The only alternative explanation to military involvement, Mandiant argues in the report, is that “a secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398’s gates.”

The Mandiant report coincides with the completion of a classified National Intelligence Estimate by the U.S. intelligence community that concluded that China was the most aggressive perpetrator of a massive campaign of cyber-espionage against commercial targets in the United States.

It also comes days after President Obama issued an executive order aimed at better securing the computer networks run by critical U.S. industries, such as transportation and energy.

“We know foreign countries and companies swipe our corporate secrets,” Obama said in his State of the Union address. “We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.”

On Tuesday, White House spokeswoman Caitlin Hayden said the administration was aware of the Mandiant report. She reiterated that the United States “has substantial and growing concerns about the threats to U.S. economic and national security posed by cyber intrusions, including the theft of commercial information.”

Before she left office this month, Secretary of State Hillary Rodham Clinton said the United States has elevated the cyber-espionage issue to the strategic dialogue level with China. “We have to begin making it clear to the Chinese that the United States is going to have to take action to protect not only our government, but our private sector, from this kind of illegal intrusions,” Clinton said.

Other security experts have also traced cyberattacks to China in the past. In one instance, documented by Bloomberg News reporters last week, a malware expert at Dell SecureWorks and other security experts traced cyberattacks to a man named Zhang Changhe teaching at a Chinese military academy, PLA Information Engineering University.

Along with Tuesday’s report, Mandiant included lengthy descriptions of the group’s past methods and more than 3,000 indicators to help others bolster their defenses against the unit’s tactics.

The company explained its rationale, saying its leaders decided that the benefits of exposing the military unit’s activity and pinning responsibility squarely on China now outweighed the usefulness of keeping silent.

“It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively,” the report said. “Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns.”

Company officials, however, acknowledged that the report would likely lead to negative consequences, such as prompting Unit 61398 and other military operations to change their methods, making them harder to detect and stop. They also concluded the report by saying that Mandiant as a company was ready to face “reprisals from China as well as an onslaught of criticism.”

Details included in the new report suggest a massive operation behind the cyberattack carried out by the unit singled out by Mandiant. According to Mandiant, the unit is one of the most prolific and likely includes hundreds or even thousands of employees.

The group’s attack infrastructure uses more than 1,000 servers. In the past two years alone, the report noted, hackers logged into the same attack infrastructures 1,905 times from 832 different Internet protocol (IP) addresses. And in 97 percent of the cases, according to the report, the hacking group used IP addresses registered in Shanghai and computer systems set to Simplified Chinese language — a written form of Chinese that is unique to mainland China and not used in Taiwan and Hong Kong.

An operation of such a size, the report argues, would require a sizable dedicated IT staff as well as linguists, open source researchers, malware authors and other support staff.

The scale of the unit’s intrusions is also surprising. While Mandiant was careful not to name any targeted corporations, the report counts 147 targeted companies, spanning 20 major industries, including several sectors publicly identified by China’s government as emerging ones central to China’s strategic interests.

On average, the attackers stayed in companies’ systems almost a year, but in one case investigated by Mandiant, a company was infiltrated for almost five years. In many cases terabyte-size portions of intellectual property were siphoned off.

In an effort to illuminate the hackers behind such attacks, the report also included personal details of three operators believed to be part of the unit, tracking them using accounts associated with attacks.

In a video addendum published online with the report, the security firm showed one of the hackers using details such as a Shanghai cellphone to create a Google mail account that is later used in cyberattacks to target the e-mail accounts of Southeast Asian military organizations in Malaysia and the Philippines.

Table of Contents

Hackers Attack European Governments Using 'Miniduke' Malware

By Josh Halliday, the Guardian, 27 February 2013

Cyber criminals have targeted government officials in more than 20 countries, including Ireland and Romania, in a complex online assault seen rarely since the turn of the millennium.

The attack, dubbed "MiniDuke" by researchers, has infected government computers as recently as this week in an attempt to steal geopolitical intelligence, according to security experts.

MiniDuke is the latest in a string of cyber attacks aimed at governments and other high-profile institutions, following revelations about the suspected Chinese hacking of western defence and media organisations.

Unusually, security researchers said there was no clear indication of who was behind the latest online attack.

The cybersecurity firm Kaspersky Lab, which discovered MiniDuke, said the attackers had servers based in Panama and Turkey – but an examination of the code revealed no further clues about its origin.

Goverments targeted include those of Ireland, Romania, Portugal, Belgium and the Czech Republic. The malware also compromised the computers of a prominent research foundation in Hungary, two thinktanks, and an unnamed healthcare provider in the US.

Victims' computers were infected when they opened a cleverly disguised Adobe PDF attachment to an email. The document would be tailored specifically to its target, according to the researchers, as unsuspecting government victims are more likely to open an attachment that mentioned foreign policy, a human rights seminar, or Nato membership plans.

Once it was opened, the MiniDuke malware would install itself on a victim's computer. It is not known what information the attackers are targeting. "It's currently unclear what the attackers were after. But the interest in these high-profile victims is quite obvious," said Vitali Kamluk, chief malware expert at Kaspersky Lab.

Eugene Kaspersky, founder and chief executive of Kaspersky Lab, said MiniDuke had the potential to be "extremely dangerous" because it was an "elite, old-school" attack that used some 21st century tricks.

"This is a very unusual cyber attack," he said. "I remember this style of malicious programming from the end of the 1990s and the beginning of the 2000s. I wonder if these types of malware writers, who have been in hibernation for more than a decade, have suddenly awoken and joined the sophisticated group of threat actors active in the cyber world."

Table of Contents

Top US General in Afghanistan: Taliban Succeeding With Its Messaging

By Chris Carroll, Stars and Stripes, March 11, 2013

KABUL — The top U.S. commander in Afghanistan said that while the Taliban appear to be facing organizational breakdown and resource shortages, they are succeeding in the important battle for the minds of the Afghan people.

In a wide-ranging discussion with reporters Sunday, Gen. Joseph Dunford, who took command in February, outlined his vision of the final phases of a war in which U.S. troops are rapidly shifting to an advisory and training role while Afghans take over most of the fighting.

He spoke in Kabul on the same day that visiting U.S. Defense Secretary Chuck Hagel was forced to cancel a joint press conference with President Hamid Karzai and rearrange other meetings because of an unspecified security threat.

Hagel was returning to the United States on Monday after two days in Afghanistan punctuated by series of security issues as well as anti-U.S. statements by Karzai.

On Saturday, a suicide bomber killed 10 people outside the Afghan Defense Ministry, a "message" to Hagel, a Taliban spokesman said.

"There is one place where the Taliban are still successful, and that is the messaging," said Dunford, who called the primary challenge of the remaining months of the war a "psychological" one.

Two powerful though contradictory Taliban messages are resonating with the Afghan public, which fears instability and uncertainty after the NATO combat mission ends next year more than it fears the Taliban, he said.

"One (message) is the coalition as occupiers, and the other is that the coalition will abandon Afghanistan at the end of 2014," he said.

But Dunford said that several processes in motion could counteract those ideas, ultimately persuading the Afghan public to throw its support behind a democratic government allied with the United States.

First, the capability of the nation's security forces is developing rapidly, he said, putting an increasingly Afghan face on the fight against the Taliban. With U.S. and NATO forces in the background, he predicted, ANSF would handle the Taliban in the 2013 fighting season and be able to secure the Afghan national elections in 2014.

The ANSF are doing most of the fighting and nearly all the dying now, Dunford said. Since he assumed command, he said, over 200 Afghan troops had been killed in battle, compared to one American servicemember, as of Sunday. Two U.S. soldiers were killed Monday in Wardak province.

"This is evidence the ANSF is truly in the lead and bearing the brunt," he said, adding that U.S. commanders are working with Afghan counterparts on tactics to reduce Afghan casualties.

Secondly, Dunford said, the fear of abandonment and instability will be calmed in the coming months as a series of security pacts are signed, including a U.S.-Afghan bilateral security agreement and a NATO status-of-forces agreement.

Those will set the stage for solid commitments of aid and troop levels for training and counterterrorist activities after 2014, he said.

"I think we address that message of abandonment, and that's with the bilateral security agreement and commitments post-2014," he said. "[W]ith Afghans in the lead this summer and Afghans providing security across the country, I think we then address that challenge of us as an occupying force."

On Sunday, Karzai charged that the United States and the Taliban were essentially working together to destabilize Afghanistan. In a nationally televised speech, he said the Defense Ministry attack and another suicide bombing in Khost on Sunday benefits the United States, which he portrayed as trying to stir up fear about the impending end of the war.

Though Karzai has publicly lashed out at the United States over issues including coalition airstrikes and custody of prisoners in recent weeks, Dunford said that he has an effective working relationship with Karzai in private.

Afghanistan is an embattled country trying to rise from the ashes of nearly constant war, and diplomatic flare-ups should be kept in perspective, Dunford said.

“These issues… are a natural tension as Afghanistan increasingly asserts it sovereignty,” Dunford said. “We do not have a broken relationship, we do not have a lack of trust. We have a relationship that actually can absorb this tension as we work through difficult issues.”

Upon his return to Washington from his first trip to Afghanistan as defense secretary, Hagel will “seek ways of deepening and our engagement with Afghan leaders, some of whom clearly have issues they want resolved,” according to a written statement from a senior defense official.

“The top priority for Secretary Hagel will be the Bilateral Security Agreement, which he sees as the lynchpin of U.S.-Afghan relations in the years ahead.”

Table of Contents

The Great Cyberscare

By Thomas Rid, Foreign Policy, March 13, 2013

The White House likes a bit of threat. In his State of the Union address, Barack Obama wanted to nudge Congress yet again into passing meaningful legislation. The president emphasized that America's enemies are "seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems." After two failed attempts to pass a cybersecurity act in the past two years, he added swiftly: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." Fair enough. A bit of threat to prompt needed action is one thing. Fear-mongering is something else: counterproductive. Yet too many a participant in the cybersecurity debate reckons that puffery pays off.

The Pentagon, no doubt, is the master of razzmatazz. Leon Panetta set the tone by warning again and again of an impending "cyber Pearl Harbor." Just before he left the Pentagon, the Defense Science Board delivered a remarkable report, Resilient Military Systems and the Advanced Cyber Threat. The paper seemed obsessed with making yet more drastic historical comparisons: "The cyber threat is serious," the task force wrote, "with potential consequences similar to the nuclear threat of the Cold War." The manifestations of an all-out nuclear war would be different from cyberattack, the Pentagon scientists helpfully acknowledged. But then they added, gravely, that "in the end, the existential impact on the United States is the same."

A reminder is in order: The world has yet to witness a single casualty, let alone fatality, as a result of a computer attack. Such statements are a plain insult to survivors of Hiroshima. Some sections of the Pentagon document offer such eye-wateringly shoddy analysis that they would not have passed as an MA dissertation in a self-respecting political science department. But in the current debate it seemed to make sense. After all a bit of fear helps to claim -- or keep -- scarce resources when austerity and cutting seems out-of-control. The report recommended allocating the stout sum of $2.5 billion for its top two priorities alone, protecting nuclear weapons against cyberattacks and determining the mix of weapons necessary to punish all-out cyber-aggressors.

Then there are private computer security companies. Such firms, naturally, are keen to pocket some of the government's money earmarked for cybersecurity. And hype is the means to that end. Mandiant's much-noted report linking a coordinated and coherent campaign of espionage attacks dubbed Advanced Persistent Threat 1, or "APT1," to a unit of the Chinese military is a case in point: The firm offered far more details on attributing attacks to the Chinese than the intelligence community has ever done, and the company should be commended for making the report public. But instead of using cocky and over-confident language, Mandiant's analysts should have used Words of Estimative Probability, as professional intelligence analysts would have done.

An example is the report's conclusion, which describes APT1's work: "Although they control systems in dozens of countries, their attacks originate from four large networks in Shanghai -- two of which are allocated directly to the Pudong New Area," the report found. Unit 61398 of the People's Liberation Army is also in Pudong. Therefore, Mandiant's computer security specialists concluded, the two were identical: "Given the mission, resourcing, and location of PLA Unit 61398, we conclude that PLA Unit 61398 is APT1." But the report conspicuously does not mention that Pudong is not a small neighborhood ("right outside of Unit 61398's gates") but in fact a vast city landscape twice the size of Chicago. Mandiant's report was useful and many attacks indeed originate in China. But the company should have been more careful in its overall assessment of the available evidence, as the computer security expert Jeffrey Carr and others have pointed out. The firm made it too easy for Beijing to dismiss the report. My class in cybersecurity at King's College London started poking holes into the report after 15 minutes of red-teaming it -- the New York Times didn't.

Which leads to the next point: The media want to sell copy through threat inflation. "In Cyberspace, New Cold War," the headline writers at the Times intoned in late February. "The U.S. is not ready for a cyberwar," shrieked the Washington Post earlier this week. Instead of calling out the above-mentioned Pentagon report, the paper actually published two supportive articles on it and pointed out that a major offensive cyber capability now seemed essential "in a world awash in cyber-espionage, theft and disruption." The Post should have reminded its readers that the only military-style cyberattack that has actually created physical damage -- Stuxnet -- was actually executed by the United States government. The Times, likewise, should have asked tough questions and pointed to some of the evidential problems in the Mandiant report; instead, it published what appeared like an elegant press release for the firm. On issues of cybersecurity, the nation's fiercest watchdogs too often look like hand-tame puppies eager to lap up stories from private firms as well as anonymous sources in the security establishment.

Finally, the intelligence community tags along with the hype because the NSA and CIA are still traumatized by missing 9/11. Missing a "cyber 9/11" would be truly catastrophic for America's spies, so erring on the side of caution seems the rational choice. Yes, Director of National Intelligence James Clapper's recent testimony was more nuanced than reported and toned down the threat of a very serious cyberattack. But at the same time America's top spies are not as forthcoming with more detailed information as they could be. We know that the intelligence community, especially in the United States, has far better information, better sources, better expertise, and better analysts than private companies like Symantec, McAfee, and Kaspersky Lab. But for a number of reasons they keep their findings and their analysis classified. This means that the quality of the public debate suffers, as experts as well as journalists have no choice but to rely on industry reports of sometimes questionable quality or anonymous informants whose veracity is hard to assess.

The tragedy is that Obama actually has it right: Something needs to be done, urgently. But Washington's high-octane mix of profiteering, protectiveness, and politics is sadly counterproductive for four reasons:

First, the hype actually makes it harder to focus on crucial engineering details. Security standards in industrial control systems and SCADA networks -- the networks that control stuff that physically moves around, from trains to gas to elevators -- are shockingly low. The so-called Programmable Logic Controllers widely used in critical infrastructure are designed to be safe and reliable in tough factory-floor conditions and harsh weather, not secure against outside attack. This year's S4-conference in Miami Beach, organized by the small and specialized security outfit Digital Bond, again showcased how vulnerable these systems are. But Washington is too busy screaming havoc and too ill-informed to do something meaningful about concrete engineering issues. Just sharing information, as the inspector general of the Department of Homeland Security recommended in a report last month, is useful but it will not deliver security. Connecting critical infrastructure that was never designed to be linked to the Internet is also not the root of the problem -- the built-in security flaws and fragility of these systems needs to be fixed, as Digital Bond's Dale Peterson pointed out last week in response to the timid DHS report. The political dynamic behind this logic is clear: The more is declared critical, the harder it becomes to act on the really critical.

Second, the hype clouds badly needed visibility. A fascinating project at Free University Berlin has produced a vulnerability map. The map uses publicly available data from Shodan, the Google for control system hackers, and adds a layer of information crawled from the web to geo-locate the systems that often should not be connected to the Internet in the first place. Red dots on the map show those systems. The United States looks as if it has the measles. But note that the map is incomplete: It is biased towards German products, the project's founder told me. If that flaw can be fixed, the United States and other countries would look as bloody red as Germany does already. The U.S. government's attention-absorbing emphasis on offensive capabilities means it has very little visibility into what this vulnerability map would actually look like.

Third, sabotage and espionage are rather different things -- technically as well as politically. SCADA systems are highly specific kit, often old and patched together over years, if not decades. That means these systems are highly specific targets, not generic ones. Affecting critical operations requires reprogramming these systems, not just disrupting them; the goal is modifying output parameters in a subtle way that serves the saboteur's purpose. With Stuxnet, the U.S. government provided the -- so far -- most extreme and best-documented case study. The operation showed that successful sabotage that goes beyond just deleting data is far more difficult than successful espionage: It requires testing and fine-tuning an attack over many iterations in a lab environment, as well as acquiring highly specific and hard-to-get target intelligence. Stealing large volumes of intellectual property from a commercial competitor, by contrast, is a technically rather different operation -- there is little to no valuable IP hidden inside control systems. To put it bluntly: China and others have a high commercial incentive to steal stuff, but they have no commercial incentive to break stuff. All threats are not created equal. What's needed is nuance, surgical precision, differentiation, and sober analysis -- not funk, flap, and fluster.

Finally, hype favors the offense over the defense. The offense is already sexier than the defense. Many software engineers who consider a career in public administration want to head north to the dark cubicle at Fort Meade, not bore themselves in the Department of Homeland Security -- if they are not working happily in the Googleplex on bouncing rubber balls already. If the NSA sucks up most of the available talent and skill and puts it to work on the offense, the defense will continue to suffer. By overstating the threat, and by lumping separate issues into one big bad problem, the administration also inadvertently increases the resistance of powerful business interests against a regulatory over-reaction.

As President Obama mentioned in his State of the Union address, if we look back years from now and wonder why we did nothing in the face of real threats, the answer may be straightforward: too much bark, not enough bite.

Table of Contents

Wanted: Ph.D.s Who Can Win a Bar Fight

By Fernando M. Luján, Foreign Policy, March 8, 2013

Looming budget cuts, ground forces worn down by years of repeated deployments, and a range of ever evolving security challenges from Mali to Libya and Yemen are quickly making "light footprint" military interventions a central part of American strategy. Instead of "nation building" with large, traditional military formations, civilian policymakers are increasingly opting for a discrete combination of air power, special operators, intelligence agents, indigenous armed groups, and contractors, often leveraging relationships with allies and enabling partner militaries to take more active roles.

Despite the relative appeal of these less costly forms of military intervention, the light footprint is no panacea. Like any policy option, the strategy has risks, costs and benefits that make it ideally suited for certain security challenges and disastrous for others. Moreover, recent media coverage of drone strikes and SEAL raids may also distort public perceptions, creating a bin Laden effect -- the notion of military action as sterile, instantaneous, and pinprick accurate. Yet nighttime raids are only the proverbial tip of the iceberg: the most visible part of a deeper, longer-term strategy that takes many years to develop, cannot be grown after a crisis, and relies heavily on human intelligence networks, the training of local security forces, and close collaboration with diplomats and development workers. For these smaller-scale interventions to be an effective instrument of national policy, civilian and military leaders at all levels should make a concerted effort to understand not only their strategic uses and limitations, but also the ways the current defense bureaucracy can undermine their success.

The most critical resource requirement in smaller interventions is human capital: talented, adaptable professionals who are not only fluent in language, culture, politics, and interpersonal relationships, but also willing to deploy for long periods and operate with little guidance. Smaller-scale missions mean less redundancy, less room for error, and more responsibility for every person in the field. In the words of Lt. Gen. Charlie Cleveland, the commander of U.S. Army Special Operations Command: "To succeed in these missions, we need people who can wade into uncertainty, learn the key players, and figure out the best way to influence outcomes." This means that in the face of looming budget cuts, the Pentagon's biggest national security challenge may not be dealing with a rival power or preserving force structure, but instead solving an intractable human resources problem -- how to retool outdated institutions to select, train, assign, and retain the most talented people to address today's security problems overseas.

Two of my own operational assignments may help illustrate how light-footprint missions can succeed or fail depending on the people who are assigned to accomplish them. I served in the 7th Special Forces Group and the Department of Defense AFPAK Hands program -- organizations with very different missions but built for the same fundamental task of influencing foreign partners and building security capacity with a handful of U.S. personnel. These contrasting vignettes should serve as a vivid example of two different organizational philosophies and the institutional challenges that must be overcome if the United States is to master a smaller, more indirect, lower-profile approach to warfare.

The 7th Special Forces Group

The ethic that defines Special Forces training is probably best described as "select hard, manage easy." Operators enjoy tremendous autonomy in the field, but they must earn it first. Before reporting to an operational unit, every Special Forces officer and soldier is required to undergo a rigorous screening and selection process, followed by a two-year qualification course that includes instruction on infantry tactics, specialized technical skills such as weapons or communications, guerrilla warfare, survival, and foreign language training.

Undertaking these intense experiences just after the 9/11 terrorist attacks, I was surprised by two things. First, there was a strong connection between our training and real-world Special Forces missions -- operators who had just fought on horseback with the Northern Alliance would return to speak to the class, and their feedback would be immediately incorporated into realistic, immersive exercises. Second, a large portion of the course was focused on the intellectual and social attributes of the students -- creativity, oral and written communication, judgment, cultural respect, and interpersonal skills -- rather than sheer athletic prowess. Peers who aced every physical challenge would suddenly be dropped when the instructors observed them unable to plan a mission alone without further guidance or incapable of building rapport with role players during a cross-cultural scenario. Sensing our confusion after a particularly tough cut sent a dozen students home, one instructor quoted a line from our World War II predecessors, the Office of Strategic Services: "The OSS, when selecting officers to parachute into occupied France, described the ideal candidate as a Ph.D. that can win a bar fight. We don't just want an officer that can carry a hundred-pound rucksack on his back. We need someone who can think and improvise."

Upon graduation, I was assigned to the 7th Special Forces Group, a unit that has long specialized in Latin America. Every Army Special Forces unit is permanently aligned with a region of the world, and as the Spanish-speaking son of Mexican immigrants, I saw 7th Group as the natural choice. From the first day I arrived, I was struck by the sense of continuity and shared culture I encountered; it showed in the soccer posters hanging in the team rooms and the salsa music playing in the hallway. Like me, many of the operators were native or advanced Spanish speakers with families from Mexico, Puerto Rico, the Dominican Republic, or Panama, and those who were not had gradually improved upon their few months of formal language instruction by working with foreign militaries across the region. This was a unit full of very talented people, focused on conducting tough training and advisory missions. At any given time, 12-man detachments were scattered across a half-dozen countries, from Peru to Bolivia to Chile, or attending privately run tactical schools for off-road driving, mountaineering, or whatever the mission required. Moreover, the teams prized their independence when deployed, and they were accustomed to frequently operating as the only military presence in a country. A longtime unit veteran pulled me aside and explained: "In 7th Group, you can maybe get away with calling back to the United States and asking your boss for guidance once. But do it twice, and you'll be out of a job. Fix problems at your level. You're in charge."

On my first deployment, to conduct a State Department-funded infrastructure security mission in the Colombian jungle, I had the good fortune of being mentored by a senior warrant officer and sergeant major with nearly 35 years of experience and seven or eight trips to Colombia between them. While I was impressed by their ease working with civilian embassy officials and their tactical knowledge in the field, the most valuable lesson they taught me was the power of relationships. I watched these experienced American soldiers walk into high-level meetings to give the Colombian generals a bear hug and immediately start joking about past exploits. They'd known most of the top officers for more than a decade. More importantly, this level of rapport and trust allowed them to have a deeper influence than any first-time adviser with a standard training plan; they could discuss topics that mattered, such as corruption, professionalism, or ethics -- not just tactics and marksmanship. I saw the power of relationships repeated again and again in many countries, even in Iraq, where I served as an adviser to a battalion from El Salvador. In the middle of an Arabic-speaking country, we conducted missions together in Spanish and learned that even though specific personalities had changed, the Salvadorans knew the history of our unit and the names of the U.S. advisers who had been killed, and they felt honored to repay the sacrifices that our 7th Group predecessors made for their homeland more than 30 years ago.

The Pentagon's AFPAK Hands Program

In late 2009, as the military was ramping up for a surge in Afghanistan, the Pentagon announced the creation of the AFPAK Hands program. Chairman of the Joint Chiefs of Staff Mike Mullen wrote a memo calling it his "number one" manpower priority and asked the services to search for the "best and brightest" candidates. The concept was innovative: A small contingent of several hundred military personnel from all branches of service would be carefully selected, given intensive instruction in Dari, Pashto, or Urdu, and then would spend years rotating between critical assignments in theater and Afghanistan-Pakistan staff positions in Washington or at Central Command. The in-theater jobs would be totally immersive, requiring advisers to embed within Afghan ministries, military units, district centers, and other key places where they could help serve as a cultural bridge and build long-term relationships that could endure after most U.S. troops had withdrawn. According to the concept briefing, the goal was to create a deep bench of knowledgeable, talented regional experts who would add much-needed continuity to the campaign. It was billed as a strategic game changer and basically sought to apply special operations methodologies, as I had seen in 7th Group, to the broader military effort in Afghanistan. I jumped at the chance to participate.

But a few days after reporting to Washington for the initial AFPAK Hands training, it quickly became apparent that something was amiss. First, there was no mechanism to turn unsuitable candidates away, and half of the cohort had not even volunteered for the assignment. As such, the class included far too many students who lacked either the aptitude or desire to participate in the challenging, unstructured advisory missions for which the program was designed. The overarching problem was incentives. I distinctly remember one of the best students -- an exceptionally talented F-16 pilot named Lt. Col. "Bruiser" Bryant, who was later tragically killed in Afghanistan -- explaining the situation during a coffee break: "Some of the most talented people in the Air Force are the fighter pilots. Now, you try asking one of them if he wants to stop flying, learn to speak Pashto, and spend the next three to five years away from his family in a high-risk mission, after which he won't be promoted because he's off his career track? Not many volunteer for that. So sometimes you end up with people that just didn't have any better options." Yet beyond the selection and screening problems, the program did little to prepare even the most qualified volunteers for their future roles. The AFPAK Hands training basically consisted of four months of abbreviated language courses, a few days of PowerPoint presentations, and a week of basic combat skills. There was no practical instruction in the tasks most important to embedded advisers, such as rapport building, negotiation, force protection, or anti-terrorism measures, meaning that those volunteers who came from non-combat occupations or had no previous adviser experience were left with few resources to help prepare.

Rather than "select hard, manage easy," the program had essentially "selected easy," had skipped vital training, and was now left to "manage hard." When the first mixed bag of AFPAK Hands graduates arrived in theater, conditions were set for disappointment all around. Receiving commanders in Afghanistan had been promised a strategic game changer but all too often encountered a mediocre staff officer with a smattering of language skills and no desire or training to embed with Afghan counterparts. Conversely, the best AFPAK Hands, eager to immerse with their counterparts and full of good ideas, were frequently placed into jobs that involved little interaction with Afghans or placed under rules that severely restricted access. This became a vicious cycle, with the program developing a stigma, commanders tightening rules to prevent untrained personnel from getting into situations beyond their training or abilities, and AFPAK Hands often resigning themselves to jobs that did nothing to influence U.S.-Afghan relationships. Even today, as I prepare for my second AFPAK Hands deployment, half of the original cohort of students is now gone -- departed because career progression demanded it or because the frustrating experience of their first tour gave them little desire to return.

Right People, Right Training, Right Assignments

Every new initiative suffers setbacks and implementation problems, and the experiences I have described with AFPAK Hands should not overshadow the sincere efforts by various managers and staff to improve the program since its inception. Fundamentally, the concept has great promise, but a clear-eyed discussion of the bureaucratic and structural factors that drove these early difficulties is vitally important to the future of preventive, light-footprint missions. If light-footprint missions are to become central to U.S. strategy, where dozens, not thousands, of troops work under the lead of civilian embassy authorities, then the fundamental assumptions that have determined personnel policies for much of the past decade may need to be re-examined or rewritten to get the right people, with the right training, into the right assignments.

Right People: Not Everyone Can Do Light-Footprint Missions

The selection course attended by candidates en route to the 7th Special Forces Group is just one version of a process used by nearly every organization in the broader special operations and intelligence community. Working to influence foreign partners, collect intelligence, and, on occasion, surgically apply violence requires a unique mix of maturity, cross-cultural competence, and creativity, and it is a mission better conducted by seasoned veterans than by 19-year-olds spoiling for their first firefight. The philosophy behind the rigorous screening is simple: "The wrong man can do more harm than the right man can do good." In light-footprint missions, amid today's hyper-globalized media environment, a single person in the wrong job can uproot entire campaigns and undo years of progress, and it is often better to leave a position empty than to send an untrained or unqualified person in to fail. Unfortunately, this concept is the polar opposite of the assignment methodology that has been used to fill many critical adviser and staff positions in the broader military for the past decade.

Adviser positions are generally stigmatized and relegated to subpar performers, and the centralized mechanisms to fill billets are talent-blind and based only on rank and specialty. The bureaucracy sees "major, combat arms," and not "bottom 20 percent performer" or "has never deployed" or "lacks relevant experience for the job." Moreover, even if a candidate has performed well in conventional assignments, qualities like the ability to learn a foreign language, work across cultures, operate with minimal guidance, or build rapport are all impossible to gauge without specifically screening for them. All too often, the mission is left to the mercy of a personnel assignment lottery, and progress only happens when chance places the right person in the right place.

The timing has never been better to reform selection mechanisms. After 12 years of continuous war in and among foreign populations, the U.S. military has never before possessed so many people in its ranks with the experience and aptitude working as foreign advisers, human intelligence professionals, linguists, development workers, and other critical skills. Yet the window of opportunity is closing: As the Army and Marines begin to cut 100,000 personnel during the next few years, policymakers and senior military leaders have announced plans to retain an expansible, experienced force that can be reconstituted rapidly in the event of a major war. The rationale is that under emergency conditions, entry-level soldiers can be trained in a matter of weeks, but midlevel leaders take years to develop. This leaves the military with a pressing need to retain a top-heavy rank structure and keep more majors, colonels, and senior noncommissioned officers than there are operational units to command. If these extra personnel are sent to administrative or institutional positions while they wait for a major contingency to break out, many will simply depart the service. As former Defense Secretary Robert Gates said in his farewell speech: "Men and women in the prime of their professional lives, who may have been responsible for the lives of scores or hundreds of troops, or millions of dollars in assistance, or engaging or reconciling warring tribes, may find themselves in a cube all day re-formatting PowerPoint slides, preparing quarterly training briefs, or assigned an ever-expanding array of clerical duties... the consequences of this terrify me." Instead, the most effective way to keep the most experienced leaders from leaving the military may not be by awarding bonus pay or special incentives, but by selecting the best and keeping those with the right aptitude and skills engaged in light-footprint missions overseas.

Right Training: The Limits of Modularity

Achieving the level of training required to thrive in complex environments among foreign populations demands a willingness to specialize not only in the mission, but also in the specific geographic region where it will be conducted; it requires a major cultural shift in the unit's mindset. The process takes years, not weeks, and goes far beyond what can be taught in a classroom at a pre-deployment training center. Advisers need to learn firsthand how to navigate the delicate politics of a U.S. embassy country team, not just be given a briefing on the State Department. They must be able to leverage the military professional culture of the partner nation, not just memorize lists of cultural dos and don'ts. They should know how to communicate in the same language as their foreign counterparts, not just recite the words for "hello" and "goodbye."

Unfortunately, this need to train specifically for light-footprint missions lies at odds with the military's overarching drive for modularity. Since the 1990s, ground forces have been designed to be interchangeable, rapidly deployable organizations that can "plug and play" anywhere in the world, and even the Army's recently unveiled "regionally aligned forces" concept reflects a deep hesitation to specialize. A 4,000-man test brigade has already been aligned with Africa and will conduct various decentralized, small-scale advisory missions there in the coming months. But regional alignment is temporary and still constrained by the limits of a system that reconstitutes and realigns units every three years. In other words, soldiers might conduct missions in Africa, but after three years, they will rotate and never return. Also, like all conventional forces, the brigades consist of a large number of very junior soldiers led by a small number of midlevel officers and sergeants. This arrangement might be effective for more centralized, large-scale combat operations, but when piecemeal teams of five, 10, or 20 soldiers are sent to various countries across the African continent, seasoned leaders run out quickly and the resulting lack of maturity or experience becomes a liability on the ground -- nothing will shut down a military engagement program faster than an international incident.

Instead, the demands of light-footprint missions suggest the need for some proportion of the military, beyond just the special operations community, to break away from modularity and truly specialize. Rather than "plug and play" building blocks that can go anywhere in the world, policymakers may also need a continuum of smaller-scale, regionally aligned capabilities -- a range of specialized tools instead of dozens of gigantic "Swiss Army knives." One possible institutional solution might be developing a stratified or tiered system of units that specialize in light-footprint missions. The conventional military lacks any standing adviser units, and very few small-scale "quick reaction force"-type teams (such as the Marine Fleet Antiterrorism Security Team) can easily support light-footprint missions. Yet even a cursory glance at today's security environment suggests that the special operations community cannot handle the full range of small-scale missions alone.

Right Assignments: You Can't Surge Trust

For all its faults, the AFPAK Hands program made an earnest attempt to address the paralyzing criticism that Afghanistan was "not a ten year war, but a one year war fought ten times." By deploying language-capable advisers repeatedly into the country and encouraging them to build long-term relationships, the program aimed to make a disproportionately large impact on the campaign with a very small number of people. As Admiral William McRaven warned at the recent Aspen Security Forum, "You can't surge trust," and real influence with foreign counterparts, in Afghanistan or elsewhere, can only be developed over many years and repeat assignments. Unfortunately, while service as a foreign adviser is certainly not career-enhancing for most military volunteers, returning to do a second tour with the same counterparts is regarded as even worse, and the institutional pull to maintain competitiveness for promotion proved too strong for many AFPAK Hands.

To address the issue, the military may need to re-evaluate the incentives for advisory work, foreign languages, and overseas duty in support of small-scale missions. For instance, assignment opportunities may in some cases need to be mission- or country-based instead of installation- or unit-based. Rather than changing duty stations to Fort Bragg or Fort Hood, an officer might be assigned to a specific task force or embassy overseas, learning the language, then spending three or four years overseas or supporting policymakers in Washington. To facilitate these assignments, the rules regarding families and accompanied tours may need to be relaxed to fall more in step with other U.S. government agencies or even the civilian sector, or rotation cycles may need to be changed (e.g., three months deployed, three months home). These steps may seem drastic, but with the proper incentives and selection mechanisms, the number of volunteers may be surprisingly high. As the U.S. troop presence in Afghanistan winds down and the opportunities to deploy decrease dramatically, even those officers who are selected to fill positions within standard combat units may find themselves essentially serving rear detachment duty -- preparing for simulated wars at national training centers while dozens of small-scale, real-world missions are being conducted in countries overseas.

Conclusion: System Reboot?

Despite the best intentions of senior officials, some worry that the frustrations of waging counterinsurgency in Iraq and Afghanistan may drive the military bureaucracy to repeat the post-Vietnam years, returning to the status quo of preparing for large conventional wars rather than retooling for smaller ones. Shawn Brimley and Vikram Singh call this a system reboot, or a tendency to "purge those military innovations most associated with a campaign that is considered a failure." While it is too early to tell which direction the Defense Department is headed, if the revised curriculum of the Army's Command and General Staff College offers any hint, future war will look conspicuously like it did before September 11, 2001. Officers from a recent class discovered that the school's final culmination exercise was focused not on irregular threats, but on planning a deliberate defense against a fictitious tank division attacking with old Soviet tactics.

The looming defense budget cuts only complicate matters, as they are likely to greatly intensify the Pentagon's natural institutional tendency to protect large, high-tech, expensive programs, while "squishy," esoteric programs such as language lessons, culture immersion, broadening experiences, advanced education, advisory units, and other human capital investments -- all invaluable to smaller missions -- have little hope of being prioritized. Without a concerted, sustained effort by military and civilian leaders at all levels, the state of affairs within the defense establishment may come to resemble the parable of the blind men and the elephant, with doctrine writers, strategists, operators, and budget analysts all drawing different lessons from the past decade of war and telling a different story about how the institution should change to remain relevant. Unless speeches and policy documents are backed up by culture, processes, doctrine, and strategic clarity, the light footprint will likely remain a niche capability confined to a few fringe military units, not an effective instrument of national policy.

PDF Report at: http://www.cnas.org/lightfootprints

Table of Contents

Talking Past Each Other? How Views of U.S. Power Vary between U.S. and International Military Personnel

Authored by Colonel Richard H. M. Outzen, Strategic Studies Institute, US Army War College, Jan 31, 2013

Brief Synopsis

The 21st century U.S. military seldom operates alone. Except for initial entry and organizational training, it works almost always with and through foreign partners. Yet over the past decade, anecdotal evidence suggests that U.S. military organizations and personnel have trouble understanding, influencing, and cooperating with international partners. This evidence includes high-profile incidents from Iraq and Afghanistan: civilian deaths, Koran burnings, blue-on-blue or green-on-blue lethal attacks. It also includes more numerous, lower profile bits of friction that follow U.S. service members around the globe in the form of protests, lawsuits, criminal cases, and difficult military-to-military relations from Iraq and Afghanistan to Turkey and Pakistan. In some instances, the U.S. military may be entirely without fault, suffering friction driven by problematic local attitudes or political dynamics. On the other hand, it is possible that certain characteristics of thought or behavior within the U.S. military culture increase the likelihood of severe friction. Against this backdrop, the gap between the U.S. military’s self-image and its image in the eyes of an international military audience is examined. When considering U.S. power, do response patterns indicate great difference between how U.S. military officers view themselves, and how they are viewed by their international peers? If so, is there anything that the United States can do about it, or does a fundamental and pathological anti-Americanism predetermine outcomes? Based on a survey administered at the National Defense University, this study offers observations and recommendations about the increasingly central question of how U.S. forces can form better and stronger ties with partners.

Download full paper at http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1140

Table of Contents

Army Electronic Warfare Evolutionary Path Presented At EW Summit

By Adrienne Moudy, Inside the Army News, March 20, 2013

ALEXANDRIA, Va. (March 20, 2013) -- Army electronic warfare is an evolving capability for the Army. Col. Jim Ekvall, the Headquarters, Department of the Army G-39 Electronic Warfare Division chief, had the opportunity to speak at the Institute for Defense and Government Advancement Electronic Warfare Summit, March 19, which just so happened to be the tenth anniversary of the beginning of the War in Iraq.

After deploying twice to Iraq himself, Ekvall can tell you first-hand how electronic warfare saves lives and is a much needed capability for the Army.

Thousands of miles from the streets of Baghdad or Fallujah, industry, military and scholars gathered at the Crowne Plaza in historic Old Town Alexandria, near the Pentagon, for the Institute for Defense and Government Advancement Electronic Warfare, or IDGA EW, Summit. Ekvall's presentation focused on the evolution of Electronic Warfare, known as EW, within the Army, specifically during the past several years of warfare as well as where the Army plans to take electronic warfare in the future.

Ekvall began his presentation with an overview of the key players within Army EW.

Army EW has a broad base of players; Ekvall is the division chief of G-39 Army EW Division in the Pentagon, which provides Headquarters, Department of the Army, or HQDA, staff the oversight for the entire Army EW enterprise. Fort Leavenworth's Mission Command Center of Excellence provides the oversight to the EW proponent office whereas the Program Executive Office in Aberdeen, Md., provides the oversight for the program manager of electronic warfare.

EW has its own MOS -- the 29 series. Soldiers who choose this career path are trained at the Fires Center of Excellence at Fort Sill, Okla.

"Fort Sill has created a range which has the ability to train Soldiers how to operate within the electromagnetic spectrum and in a realistic battle scenario," said Ekvall.

Communications systems for electronic warfare are supported at both the Intelligence Center of Excellence at Fort Huachuca, Ariz., as well as the Signal Center of Excellence in Fort Gordon, Ga.

Cyber electromagnetic activities were a large piece of Ekvall's presentation. Ekvall highlighted that Army doctrine for, cyber electromagnetic activities, or CEMA, is comprised of three areas -- electromagnetic spectrum operations, cyber operations and electronic warfare.

"These three areas are inextricably linked to one another. We are still evolving how cyber operations will work within the Army," said Ekvall. "All of these areas must be synchronized for the commander to maneuver."

On the battlefield, Ekvall emphasized that there was urgency for a material solution that would allow Soldiers to maneuver safely within the electromagnetic spectrum. Currently, the Army has several systems such as the Counter Radio-Controlled Improvised Explosive Device Electronic Warfare, or CREW, systems, and the communications electronic attack surveillance and reconnaissance, or CEASAR, among others. Ekvall explained that while all of these systems are important to protect the war fighter, more advanced systems are being planned.

"It is important for our senior leaders to know that EW is more than just a CREW system," said Ekvall.

Aside from the CREW systems that are currently in use on the ground, the CEASAR program is an airborne electronic attack capability.

Future material solutions for the Army include the Integrated Electronic Warfare System, or IEWS. IEWS is a system of systems which will include the Electronic Warfare Planning and Management Tool, also known as EWPMT, Multi Function Electronic Warfare, or MFEW, and Defensive Electronic Attack, or DEA.

"In the long run we need an electronic warfare of tomorrow, and that is IEWS," said Ekvall.

Ekvall emphasized that it was important for senior leaders within the Army and the Department of Defense continue to learn more about the need for EW not only during the current war, but to continue growing Army electronic warfare when the war concludes.

"I was happy to speak at the IDGA EW Summit," said Ekvall. "Organizations such as IDGA are an excellent way which allows us to get our message out to the defense community. Educating senior leaders in industry, academia, and the in the military about what electronic warfare does for the Army will help grow the field and EW will continue down its evolutionary path."

Table of Contents

Nazi and Soviet Propaganda's Shared Aesthetic

Published 20 March 2013 – Radio Free Europe/Radio Liberty

With their emphasis on totalitarianism, rigid ideology, and personality cults, it's safe to say that Nazi Germany and the Soviet Union had many common characteristics. Both regimes also had great faith in propaganda to promote their political ideas. This comparative collection of Nazi and Soviet posters compiled by the website gulag.ipvnews.org appears to indicate that the two authoritarian systems also had an uncannily similar aesthetic and approach to graphic design.

http://www.rferl.org/media/photogallery/24934238.html

Table of Contents

NATO: U.S.-Israeli Cyberattack On Iran Was 'Act Of Force'

By Shaun Waterman, Washington Times, March 24, 2013

The 2009 cyberattack by the U.S. and Israel that crippled Iran's nuclear program by sabotaging industrial equipment constituted "an act of force" and was likely illegal under international law, according to a manual commissioned by NATO's cyberwarfare center in Estonia.

"Acts that kill or injure persons or destroy or damage objects are unambiguously uses of force," according to "The Tallinn Manual on the International Law Applicable to Cyber Warfare."

Michael N. Schmitt, the manual's lead author, told The Washington Times that "according to the U.N. charter, the use of force is prohibited, except in self-defense."

Under the charter, states may use force in self-defense — and that, some argue, includes "anticipatory self-defense" against an incipient or imminent attack.

The international group of researchers who wrote the manual were unanimous that Stuxnet — the self-replicating cyberweapon that destroyed Iranian centrifuges that were enriching uranium — was an act of force, said Mr. Schmitt, professor of international law at the U.S. Naval War College in Newport, R.I.

But they were divided on whether its effects were severe enough to constitute an "armed attack," he said.

Under the U.N. charter, an armed attack by one state against another triggers international hostilities, entitling the attacked state to use force in self-defense, and marks the start of a conflict to which the laws of war, such as the Geneva Conventions, apply.

Neither Israel nor the United States has publicly acknowledged being behind Stuxnet, but anonymous U.S. national security officials have told news outlets that the two countries worked together to launch the attack, which set the Iranian nuclear program back as much as two years, according to some estimates.

A group of 20 researchers wrote the manual at the invitation of NATO's Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia.

It is not a statement of official policy by NATO or any of its member governments, but it reflects a consensus view of a large group of legal scholars and practitioners, including several senior military lawyers from NATO countries who took part in producing the manual.

The authors, advised by a group of technical analysts in cybersecurity, took three years to write the 300-page manual, which was published earlier this month in London, Mr. Schmitt said.

"We wrote it as an aid to legal advisers to governments and militaries almost a textbook," he said, noting that many of the authors are or have been legal advisers.

He said the manual also was intended to be a starting point for discussions about the law.

NATO, the International Committee of the Red Cross and U.S. Cyber Command had sent personnel to observe the writing process, Mr. Schmitt said.

"States make law, not scholars," he said. "We wanted to create a product that would be useful to states to help them decide what their position is" in regard to the manual's interpretation of the law.

"We were not making recommendations, we did not define best practice we did not want to get into policy," he said.

Instead, the authors had tried to write the definitive account of "how does existing law apply in cyberspace," he said.

The threshold questions of what constitutes an act of force and what triggers international hostilities are far from merely hypothetical questions, Mr. Schmitt said.

In August 2008, Georgia and Russia went to war in the disputed border province of South Ossetia. The shooting war was accompanied by cyberattacks that knocked offline many Georgian news sites and much of the country's government, including the foreign ministry.

Mr. Schmitt said that if a cyberattack occurs before the shooting starts, "It's a crime." If it occurs after the shooting begins, then the hackers behind the cyberattack effectively have joined the hostilities as combatants and can be targeted with lethal force, he said.

Some researchers in cybersecurity and international law believe that judgment, like many others in the manual, is contentious.

"That's is why you don't let lawyers go off on their own," said James A. Lewis, a scholar at the Center for Strategic and International Studies.

Mr. Lewis said there has not yet been enough conflict in cyberspace to allow states to develop the norms and rules needed to interpret international law. The manual's authors "are writing way ahead of practice," he said.

"A cyberattack is generally not going to be an act of force," Mr. Lewis said. "That is why Estonia did not trigger Article 5 in 2007."

Article 5 of the NATO treaty obliges member states to come to the aid of a fellow member state that has been attacked.

In 2007, Estonia was locked in a civil and political conflict with its ethnic Russian population and with Russia over the removal of a war memorial to the Russian soldiers killed fighting Nazism in World War II. The country was beset by massive cyberattacks that crippled computer networks belonging to the government, news organizations and banks.

The attacks were traced to hackers in Russia, and most Western observers believe they were encouraged or even orchestrated by the Kremlin.

But the murky circumstances of the attacks against Georgia and Estonia illustrate an important truth that severely complicates international law when it comes to cyber, Mr. Schmitt said.

"The facts of a cyberincident are generally not well known, difficult to ascertain in detail and unclear even years in retrospect," he said.

A central issue for international law, such as who carried out an attack, for instance, is generally regarded as extremely difficult to ascertain — the so-called attribution problem.

Mr. Schmitt opined that, for "a [nation] state with highly advanced technical capabilities, attribution is not as hard as the public believes."

As Mr. Lewis noted, "The standards of proof on the battlefield are lower than they are in court."

Table of Contents

PACOM Promotes Regional Cyber Capabilities, Defenses

By Donna Miles, American Forces Press Service, 3/11/2013

3/11/2013 - WASHINGTON (AFNS) -- Two years ago, U.S. Pacific Command set out on a big experiment during its Terminal Fury exercise, subjecting participants for the first time to simulated cyber intrusions and network access denials, among other unexpected curve balls the exercise planners threw their way.

PACOM's cyber cell, serving as a testbed for the newly established U.S. Cyber Command, grappled with scenarios that shot holes through their cyber defenses, compromising their command-and-control systems and, by extension, their ability to control their forces.

The exercise underscored what already had become abundantly clear throughout PACOM and the entire Defense Department: the cyber domain is the new military "high ground" -- an advantage to those to use it effectively, and the downfall of those who don't.

So in officially standing up its Joint Cyber Center last year at the direction of then-Defense Secretary Leon E. Panetta, PACOM officials set out to capitalize on cyber capabilities and make them integral to the entire command structure.

"The intent is to be a fusion center to integrate cyber in all its versions in the entire cyber portfolio into the command's daily and warfighting battle rhythm," Brig. Gen. John "Mark" Hicks, PACOM's director of command, control, communications and cyber, told American Forces Press Service during a telephone interview from Camp Smith, Hawaii.

PACOM's vast area of responsibility -- more than half the globe -- makes it particularly reliant on its secure and unsecure networks to operate, Hicks explained.

"Nothing happens out here -- we don't have visibility on anything, we can't command and control anything, my boss, (Navy) Adm. (Samuel J.) Locklear (III) can't do his mission -- without assured and secure communications," Hicks said. "That means communications, not just with his own forces, but also between our allies and partners, because that is a very big part of our job here."

Collaborating closely with Cyber Command, the Defense Information Systems Agency and the services, the CyberPac team helps to ensure the command's networks provide a reliable command-and-control platform. In addition, they coordinate with other U.S. government agencies to promote the global debate on the future of cyberspace.

"We view cyber as a global common, much like sea, air and space," Hicks said. "So we are advocates for unfettered, free and secure use of the Internet and other telecommunications."

Unfortunately, not everyone sees it that way. Cyberthreats come in many forms, Hicks said. They range from hackers intent on stealing intellectual property to well-organized campaigns by state and nonstate actors to exploit national secrets, deny service or bring down vital military networks.

Recognizing that cyber threats have no respect for national borders, CyberPac increasingly is reaching out to regional allies and partners to encourage closer cooperation across the cyber domain.

"As I like to put it, communications interoperability is both an agent of and a necessary condition for improved relationships," Hicks said. "So by helping partner nations build their military communications and cyber capacity and capability, we are building partner capacity, improving our relationships with them in a non-threatening way. That potentially opens the door and allows greater access for other U.S. military activities."

So in addition to its other activities, CyberPac is leveraging PACOM's exercise program and hosting workshops and other bilateral and multilateral forums that promote closer military-to-military cyber engagement.

"There is a very palpable sense of concern with respect to cyber vulnerability in the Asia-Pacific," Hicks said, citing the frequency of software pirating and intellectual property theft through cyber intrusions. "This is a very needed capability in the Asia-Pacific."

Vietnam participated for the first time in the Cyber Endeavor workshop that ran concurrently with the Pacific Endeavor exercise. And despite widespread criticism of China's suspected role in cyber incursions, PACOM officials hope it will agree to join other regional countries at future cyber venues.

"We are continuing to reach out and hope to include the People's Republic of China in that list in the new future," Hicks said. "This is something about which everyone in the Asia-Pacific can agree. It provides a nonthreatening opportunity for us to work together toward a common goal, with the collateral benefit of building relationships."

Table of Contents

Information Warfare on the Korean Peninsula

By Michael Raska, the Strategist, 13 Mar 2013

Over the last decade, security dilemmas on the Korean peninsula have become progressively more 'hybrid' and multi-faceted. Traditional conventional threats, scenarios and contingencies linked to high intensity conventional wars, have been converging with a range of asymmetric and non-linear security challenges, including nuclear threats, ballistic missiles, and increasingly information and cyber warfare. According to General James Thurman, commander of US forces in South Korea, North Korea has acquired 'significant' IW-related military capabilities. This is an attempt to explore the idea of asymmetric negation, probing any vulnerabilities of the US–ROK alliance. Now, that means more than just nuclear weapons. In addition to its nuclear and ballistic missile programs, these also include hacking, encryption, and virus insertion capabilities.

In this context, information and cyber warfare is becoming a part of the ongoing conflict on the Korean Peninsula, and its threats and risks are continuously challenging traditional defence strategies and operational concepts of the US–ROK alliance.

I argue that we really are in a new regime of information warfare in Korea, where both North and South Korea are engaged at three levels of information conflict simultaneously: (1) a war for information to obtain information and intelligence about each other's means, capabilities, and strategies; (2) a war against information aimed at protecting their information systems, while disrupting or destroying the other side's information infrastructure; and (3) a war through information reflected in the misinformation and deception operations to shape their broader internal and external strategic narratives.

In the first category of war for information, for example, one of the most sophisticated attacks occurred in November 2009, when South Korean National Intelligence Service and the Defence Security Command reported that a suspected North Korean hacker unit operating under the North Korean Army General Staff's Reconnaissance Bureau intercepted confidential defence strategy plans, including plans detailing US–ROK responses to potential North Korean provocations. The incident happened as an officer with the ROK–US Combined Forces Command used an unsecured USB memory stick plugged into his PC while switching from a highly secure private intranet to the public Internet. While the plan is currently under review with the ROK military planning to take over the war time operational control from the United States Forces Korea in 2015, its compromise raises questions to what extent North Korea could access and potentially disrupt selected US–ROK operational plans in times of war or crisis.

In the same year, North Korean hackers reportedly stole information from the South Korean Chemical Accidents Response Information System (CARIS) after infiltrating the ROK Third Army headquarters' computer network and using a password to access CARIS's Center for Chemical Safety Management. North Korea's overseas-intelligence gathering unit under the State Security Agency (SSA) is also believed to increasingly rely on information warfare techniques for cyber-espionage to access information, steal sensitive data, and monitor foreign communications.

In the category of war against information, North Korea has attempted to disrupt South Korea's highly developed digital information infrastructure using cyber attacks to shut down major websites, disrupt online services of major banks, and probe South Korea's readiness to mitigate cyber-attacks. Most cited cases in this tier include the 2009 distributed denial-of-service (DDoS) attacks against four dozen targets in South Korea and the United States, and the 'Ten Days of Rain'; the 2011 DDoS attacks on South Korean government websites and the network of the US Forces Korea (USFK).

Interestingly, they seem to have been 'testing the fence.' According to analysis by McAfee Labs (PDF), the combination of clearly defined targets, highly destructive malware code, multiple encryption algorithms, and multi-tiered botnet architecture preconfigured for specific duration, has led to a conclusion that the attack was set up by North Korea to test and observe how rapidly the attack would be discovered, reverse engineered, and mitigated. At the end of the 'Ten Days of Rain' DDoS attacks, the botnets were configured to self-destruct.

Finally, in the category of war through information, North Korea has relied on information warfare to alter the perceptions of its strategic plans. For example, prior to the rocket launch in December 2012, the DPRK announced several days before the launch that there were technical problems, and were observed byUS satellites taking apart the three-stage rocket, and removing the parts from the launch pad. North Korea, however, launched the rocket without any delay, catching US–ROK military and intelligence agencies off-guard. Subsequent reports indicate that North Korea manipulated the launch so that US intelligence satellites would not be overhead.

At the same time, however, US–ROK forces have also engaged in a war through information—particularly focusing on psychological operations. Following the sinking of the Cheonan warship and subsequent shelling of Yeonpyeong Island in 2010, the South Korean military established a new psyops unit to diffuse news and information into North Korea—whether through radio transmissions, balloon leaflets, DVDs, and possibly USB memory sticks. Since then, it has sent thousands of leaflets and transmitted broadcast into North Korea using mobile broadcast vehicles and six relay stations. While its effects on North Korean society are difficult to ascertain, North Korea has previously threatened to fire across the heavily fortified border to stop such campaigns.

With changing strategic realities on the Korean Peninsula, information warfare has important ramifications for the US–ROK defence strategy. While we don't really know how disruptive a well-orchestrated North Korean IW campaign could be against the US–ROK alliance forces, we saw in 2007 and 2008 how effective Russian efforts were against targets in Estonia and Georgia. In the intervening five years the world, and with it alliance forces and South Korean society more generally, have become even more dependent on networks and the data they carry. Conversely, the capability of the US and its allies are likely to be steadily increasing. You can bet that the topic of IW is being actively thought about on both sides of the 38th parallel.

Table of Contents

How Space and Cyberspace are Merging to Become the Primary Battlefield of the 21st Century

Posted on March 20, 2013 by Matthew Mather (Originally appearing in Space Quarterly Magazine, Mar.15th, 2013)

Cyberspace and outer space are merging to become the primary battlefield for global power in the 21st century. Both space and cyberspace systems are critical in enabling modern warfare—for strike precision, navigation, communication, information gathering—and it therefore makes sense to speak of a new, combined space-cyberspace military high-ground. This article will discuss the similarities, key differences, and potential consequences of this.

From the moment Sputnik was launched in 1957, and everyone's head turned skyward, space has occupied the military high-ground, defining much of the next fifty years of global geopolitics. Space-based systems, for the first time, broke the link between a nation's physical territory and its global ability to gather information, communicate, navigate, and project power.

In the 1980's, the rise of advanced ICT—information and communications technology—enabled the creation of the internet and what we've come to call cyberspace, a loosely-defined term that encompasses the global patchwork collection of civilian, government and military computer systems and networks. For the same reasons that space came to occupy the military high-ground—information gathering, navigation, communication—cyberspace is now taking center stage.

From a terrestrial point of view, space-based systems operate in a distant realm, but from a cyber point of view, space systems are no different than terrestrial ones. In the last decade, there has been a seamless integration of the internet into space systems, and communications satellites are increasingly internet-based. One can make the case that that space systems are now a part of cyberspace, and thus that space doctrine in the future will be heavily dependent upon cyber doctrine.

The argument can also be made, however, that cyberspace, in part, exists and rests upon space-based systems. Cyberspace is still based in the physical world, in the data processing and communications systems that make it possible. In the military domain, cyberspace is heavily reliant on the physical infrastructure of space-based systems, and is therefore subject to some of the same threats.

Space and cyberspace have several similarities. Both are entirely technological domains that only exist due to advanced technology. They are new domains of human activity created by, and uniquely accessible through, sophisticated technology. Both are vigorous arenas for international competition, the outcomes of which will affect the global distribution of power. It is no coincidence that aspiring powers are building space programs at the same time as they are building advanced cyber programs.

Space and cyberspace are both seen as a global commons, domains that are shared between all nations. For most of human history, the ability of one group of humans to influence another was largely tied to control of physical territory. Space and cyberspace both break this constraint, and while there is a general common interest to work cooperatively in peace, there has inevitably been a militarization in both domains. As with any commons, over time they will become congested, and new rules will have to be implemented to deal with this.

Congestion and disruption are problems in both space and cyberspace. Ninety percent of email is spam, and a large proportion of traffic over any network is from malware, which clogs up and endangers cyberspace. Cyberattacks are now moving from email as the primary vector, to using customized web applications using tools such as the Blackhole automated attack toolkit. Cyberattack by nation-states is now joining the criminal use of spam, viruses, Trojans and worms as deliberate attempts to attack and disrupt cyberspace.

The congestion analogy in space is that entire orbital regions can become clogged with debris. Tens of thousands of objects, from satellites and booster rockets to smaller items as nuts and bolts, now clog the orbital space around Earth. The danger of this was dramatically illustrated when an Iridium satellite was destroyed when it was hit by a discarded Russian booster in February of 2009. The situation can be made dramatically worse by purposely creating debris fields, as the Chinese did when they conducted an anti-satellite test in 2007 using a kinetic kill. Over time, entire orbital regions could become unusable.

Another similarity is that while traditional the air-sea-land domains are covered under the UN—Law of the Sea, Arctic, Climate Change, Biodiversity—outer space and cyberspace still operate under ad-hoc agreements mostly outside of UN frameworks. They both expand the range of human activity far in advance of laws and rules to cover the new areas being used and explored. Because space can be viewed as a sub-domain of cyberspace, any new rules brought into effect to govern cyberspace, will also affect outer space.

If there are many similarities between space and cyberspace, there are some critical differences, the most important being that space-based systems require massive capital outlays, while in comparison, cyberspace requires very little. As James Oberg points out in his book Space Power Theory, the most obvious limitation on the exercise of space power is cost, with the astronomical cost of launch first among these.

Cyberspace, on the other hand, has a low threshold for entry, giving rise to the reality that governance of an extremely high-cost domain, space systems, will be dictated by rules derived from the comparatively low-cost domain of cyberspace. Space power resides on assumption of exceptionalism, that it is difficult to achieve, giving nations possessing it a privileged role in determining the balance of global power. In contrast, cyberspace, and the ability to conduct cyberwar, is accessible to any nation, or even private organizations or individuals, which have the intent.

Another important defining characteristic of cyberwarfare is the difficulty with attribution. Deterrence is only effective as a military strategy if you can know, with certainty, who it was that attacked you, but in a cyberattack, there is purposeful obfuscation that makes attribution very difficult.

To most people, the term cyberwar still has a metaphorical quality, like the War on Obesity, probably because there hasn't yet been a cyberattack that directly resulted in a large loss of life. In many analysts' opinions, this is just a matter of time, especially given internet-centric reliance of a modern nations' critical infrastructure. Cyberwar has already started, and is beginning to gain in frequency and intensity.

The first cyberattack can be traced back to the alleged 1982 sabotage of the Soviet Urengoy–Surgut–Chelyabinsk natural gas pipeline by the CIA—as a part of a policy to counter Soviet theft of Canadian technology—that resulted in a three-kiloton explosion, comparable to a small nuclear device. Titan Rain is the name the US government gave a series of coordinated cyberattacks against it over a three-year period from 2003 to 2006, and in 2007 Estonia was subject to an intense cyberattack that swamped the information systems of its parliament, banks, ministries, newspapers and broadcasters.

In 2011, the McAfee security company revealed a series of cyberattacks, that it dubbed Night Dragon, against Western critical infrastructure companies, most specifically against the energy grid. This is significant because of the Aurora Test conducted by Idaho National Laboratory in conjunction with the Department of Energy in early 2007. In this test, a 21-line package of software code, delivered remotely, caused a large commercial electrical generator to self-destruct by rapidly recycling its circuit breakers, demonstrating that cyberattack can destroy physical infrastructure.

A new breed of sophisticated cyberweapon was revealed when the Stuxnet worm attacked Iran's Natanz uranium enrichment facilities in June of 2010. It was not the first time that hackers targeted industrial systems, but it was the first discovered malware that subverted industrial systems. A recent game-changer was the August, 2012 Shamoon virus that knocked out 50,000 computers at Saudi Aramco, forcing that company to spend a week restoring global services. Shamoon was significant because it was specifically design to inflict damage, and was one of the first examples of a military cyberweapon being used against a civilian target. It is only a matter of time before a cyberweapon targeting space-based systems is unleashed, if it already hasn't happened.

It is worth it to back up and explore the core issues surrounding internet security. The internet was originally designed as a redundant, self-healing network, the sort of thing that is purposely hard to centrally control. In the late 80's it evolved into an information-sharing tool for universities and researchers, and in the 90's it morphed into America's shopping mall. Now it has become something that is hard, even impossible, to define—so we just call it cyberspace, and leave it at that.

First and foremost, there is the issue that while everyone runs the internet, nobody is really in charge of it. ICANN— The Internet Corporation for Assigned Names and Numbers—exerts some control, but the World Summit on the Information Society (WSIS), convened by UN in 2001, was created because nations around world have become increasingly uneasy that their critical infrastructures, and economies, are dependent on the internet, a medium that they had little control over and no governance oversight. The issue has still not been resolved. To the libertarian-minded creators of the internet, decentralized control is a feature, but to governments trying to secure nuclear power stations and space-based assets, it is a serious flaw.

A large part of the problem is that we are trying to use the same internet-based technology for social networking and digital scrap-booking, and use this same technology to control power stations and satellites. Not that long ago, critical systems—space systems, power grid, water systems, nuclear power plants, dams—had their own proprietary technologies that were used to control them, but many of these have been replaced these with internet-based technologies as a cost-savings measure. The consequence is that as a result, now nearly everything can be attacked via the internet.

Another problem is that a truly secure internet is not in the common interest of freedom, nor in the interest of software producers—a curious statement, but one that is true. As more of our lives move into the cyber realm, for everything from banking to dating, a truly secure internet would be the same as installing CCTV cameras on every street and inside every home. Privacy is one of the cornerstones of freedom and civil liberty, and a truly secure internet would bring about an end to privacy, and thus an end to freedom—at least in the sense that we understand it today.

When it comes to software producers, while they would like their products to be secure from hackers, they have a competing interest in wanting to able to access their software installed on customers' machines. They want to be able to collect as much information as possible, to sell to third parties or use in their own marketing, and also to want to update new features into their software remotely. Often, this is to install patches to discovered security vulnerabilities, precisely because code is poorly written to begin with, because they realize they can update it later. This backdoor into software is a huge security flaw—one that companies purposely build into their products—and is one that has been regularly exploited by hackers.

There are many consequences to all this.

The first is that, because we use the same internet-based technology to support both the private lives of individuals and operate critical infrastructure, there will be a perpetual balancing act between these two competing interests when it comes to security. Another is that until the general public really sees cybersecurity as a threat, many of the fixable problems will not be addressed, such as setting international prohibitions on cyberespionage—making them comparable in severity to physical incursions into the physical sovereign space of a nation-state—or forcing software companies to get serious about secure coding practices and eliminating backdoors into their products.

Because of the extremely high value of space-based assets, and because they are already a seamless part of cyberspace, when a major cyber conflict does emerge, space systems will be primary targets for cyberattack. Even if space systems are not directly attacked, they may be affected. There can be no known blast radius to a cyberweapon when it is unleashed. Even the Stuxnet worm, which was highly targeted in several ways, still infected other industrial control systems around the world, causing untold collateral damage.

A more difficult threat to consider than simply denying access or service to a space system through cyberattack is the problem of integrity. In the cybersecurity world, the three things to protect are confidentiality (keeping something secret, and being able to verify this), availability, and integrity of data. Integrity is by far the hardest to protect and ensure. If a cyberattacker, for example, decided on a slow (over time) modification of data in a critical space junk database, they could influence moving satellites into harm's way.

Over the last fifty years, a comprehensive strategy based around deterrence was developed in conjunction with the idea of space power theory. In the future, a comparable framework and space-cyberspace power theory will need to be developed. Many questions need to be answered, most especially regarding how the international community will establish rules for cyberspace, the definition of rules for cyberwar, proportionality of response, and how to deal with the problem of attribution. Exactly how the developing cyberwar doctrine will affect the way outer space is governed remains to be seen.

Table of Contents

AQAP Releases 10th Copy Of Inspire; Features Adam Gadahn

By Bill Roggio, Long War Journal, March 1, 2013

Al Qaeda in the Arabian Peninsula has released the 10th edition of Inspire, its English language propaganda magazine that is marketed to Westerners. The magazine features an article by Adam Gadahn, the American traitor who works with al Qaeda's core leadership cadre in Pakistan.

AQAP released the current addition of Inspire "nine months after the release of the eighth and ninth issues" of the magazine, the SITE Intelligence Group noted. SITE obtained a copy of Inspire, which was released yesterday on Jihadist Internet forums.

The latest edition of Inspire focused on al Qaeda's view of the so-called Arab Spring. Inspire promoted two articles on the topic that are written by Gadahn and Yahya Ibrahim, a cleric who has been featured in the magazine in the past.

Both Gadahn and Ibrahim focus on al Qaeda's ability to capitalize on the Arab Spring. Gadahn calls for the US to end all involvement in the upheavals in the Middle East, and says a failure to do so "will result in a backlash which will make you regret the day you put your hands where they don't belong."

Gadahn also advises jihadists in the West to continue "direct engagement [attacks] at home and abroad with America and its NATO parents, particularly France and Britain."

"The enemies' economic and military hemorrhage must not stop until the day comes when the people of the West are forced to make a choice: either the continuation of the Crusade against the Muslims and the continuation of their backing Israel, or the continuation of viable governments and basic public services," Gadahn writes.

Ibrahim focuses on the assaults on the US Consulate in Benghazi and the US embassies in Egypt, Tunisia, and Yemen in September 2012. Jihadists raised al Qaeda's flag at the US installations, and killed the US's ambassador to Libya and three personnel in Benghazi. Ibrahim notes that the so-called protesters chanted "Obama! Obama! we are all Osama!" He also claims that despite bin Laden's death at the hands of US special operations forces in May 2011, bin Laden continues to inspire old and new jihadists alike.

The release of the latest edition of Inspire shows that al Qaeda's core in Pakistan is not cut off from its affiliates, and that AQAP retains the ability to produce the magazine despite the loss of two Americans who were thought to be important to its continuation.

AQAP touted Gadahn's article as an "exclusive," which means the group was either able to contact Gadahn to solicit and receive it, or that Gadahn contacted the publishers of Inspire to offer the article. Gadahn is believed to be based in Pakistan and is known to work with As Sahab, al Qaeda's primary propaganda production outfit. He also releases propaganda via As Sahab on occasion.

The Obama administration has claimed that al Qaeda's "core" leadership cadre in Pakistan is cut off and disconnected and isolated from its affiliates, and that the terror group is on the verge of defeat. But as Gadahn's latest article and numerous propaganda tapes and communiques by al Qaeda emir Ayman al Zawahiri and other top leaders show, the terror group is intact and capable of producing propaganda and communicating with its affiliates worldwide.

Additionally, it was unclear if AQAP would continue to produce Inspire after the deaths of American jihadists Samir Khan and Anwar al Awlaki, both of whom are thought to have greatly influenced the magazine's publication. Al Awlaki and Khan were killed in a US drone strike in Yemen in September 2011. As the release of the 10th edition of Inspire shows, AQAP clearly maintains the capacity to produce the magazine, and still remains committed to attacking the West.

Table of Contents

Assessing Inspire Magazine's 10th Edition

By Scott Stewart, Stratfor, March 21, 2013

Al Qaeda in the Arabian Peninsula released the 10th edition of its English-language magazine, Inspire, on March 1. After discussing its contents with our analytical team, initially I decided not to write about it. I concluded that Inspire 10 conformed closely to the previous nine editions and that our analysis of the magazine, from its inception to its re-emergence after the death of editor Samir Khan, was more than adequate.

Since making that decision, however, I have been very surprised at how the media and other analysts have received the magazine. Some have overhyped the magazine even as others have downplayed -- even ridiculed -- its content. I have heard others say the magazine revealed nothing about al Qaeda in the Arabian Peninsula. All these reactions are misguided. So in response, I've endeavored to provide a more balanced assessment that can be placed in a more appropriate perspective.

A Balanced Assessment

I am certainly not among those who want to sensationalize the threat the magazine poses. Inspire 10 is not going to launch the grassroots jihadist apocalypse al Qaeda in the Arabian Peninsula seeks to foment any more successfully than the magazine's previous nine editions. The fact that a photograph of Austin, Texas, appears in the magazine does not mean that the city is somehow being secretly targeted for attack by jihadist sleeper cells.

But laughing at the magazine or dismissing it as irrelevant would be imprudent. The magazine has in fact inspired several terrorist plots. In some cases, the connections to the magazine have been obvious, as in cases where plotters have attempted to assemble improvised explosive devices using instructions provided in Inspire magazine's first edition. This happened in July 2011, when U.S. Army Pfc. Naser Jason Abdo was arrested as he attempted to assemble explosive devices he planned to use in an attack against a restaurant in Killeen, Texas, that was popular with soldiers from nearby Fort Hood.

In November 2011, the New York Police Department arrested Jose Pimentel, also known as Muhammad Yusuf, a 27-year-old Dominican-American. Pimentel was arrested at an apartment in Manhattan as he was allegedly constructing homemade improvised explosive devices, again following the instructions provided in Inspire.

Other cases have not been as blatant as those involving Abdo and Pimentel. However, they have involved individuals who were radicalized or motivated by Inspire. As recently as March 15, three men in the United Kingdom pleaded guilty to terrorism charges related to attending terrorism training camps in Pakistan. The men allegedly were motivated by Inspire. They had discussed attack ideas from the magazine, and the wife of one of the men was convicted in December 2012 on charges of possessing two digital copies of the magazine on a memory card.

There are several other recent and notable cases connected to Inspire magazine.

- On Nov. 29, 2012, two brothers from Florida, Raees Alam Qazi and Sheheryar Alam Qazi, were arrested and charged with plotting attacks in New York. Prosecutors noted that the pair had been motivated by Inspire magazine.
- On Oct. 17, 2012, Bangladeshi national Quazi Nafis was arrested as part of an FBI sting operation after he attempted to detonate a vehicle bomb outside New York's Federal Reserve Bank. Nafis reportedly was an avid reader of Inspire magazine.
- On Sept. 15, 2012, Adel Daoud, another avid Inspire reader, was arrested after he parked a Jeep Cherokee outside a Chicago bar and attempted to detonate the bomb he thought it contained. His was also an FBI sting operation.
- On April 25, 2012, four men were arrested in the British town of Luton and charged with plotting attacks against a British army base. The four were also charged with downloading and possessing six editions of Inspire magazine. They pleaded guilty March 1, 2013.

Target Audience

Some commentators have noted that most of the suspects arrested in connection with these plots were fairly hapless and clueless -- the type of individuals we have long referred to as "Kramer jihadists." Though partly incompetent, these grassroots operatives are exactly the demographic al Qaeda in the Arabian Peninsula is targeting for radicalization and mobilization.

Inspire seeks to reach amateur terrorists living in the West; professional terrorists already know how to create pipe bombs. For this reason, the magazine urges amateurs to undertake simple attacks rather than the complex attacks. Too often they find assistance from an FBI informant.

It is a grave error to dismiss Kramer jihadists and assume they pose no threat. They can indeed kill people if they heed the advice of al Qaeda in the Arabian Peninsula and conduct simple attacks that are within their capability. That is what Maj. Nidal Hasan did in Fort Hood in November 2009 and what Abdulhakim Mujahid Muhammad, also known as Carlos Bledsoe, did in June 2009. Both men were inspired to action by al Qaeda in the Arabian Peninsula.

Kramer jihadists can also be deadly if they actually find a real terrorist, rather than a government informant, to assist or equip them. It is very important to remember that amateur, committed jihadists such as shoe bomber Richard Reid and underwear bomber Umar Farouk Abdulmutallab nearly succeeded in destroying an airliner.

Twenty years ago last month, I witnessed firsthand the dangers of discounting Kramer jihadists when I peered into a massive crater in the floor of the World Trade Center parking garage. The FBI had deemed those responsible for the attack too hapless to do much more than assassinate the leader of the Jewish Defense League in a midtown Manhattan hotel. And they were -- until a trained terrorist operative traveled to New York and organized their efforts, enabling them to construct, deliver and detonate a massive 590-kilogram (1,300-pound) truck bomb.

I also take umbrage at those who snicker at the thought of grassroots jihadists lighting fires. As noted last month, I believe that fire is an underappreciated threat. Many people simply do not realize how deadly a weapon it can be, even though starting fires does not require sophisticated terrorist tradecraft.

Some Revelations

Despite claims to the contrary, Inspire 10 reveals much about al Qaeda in the Arabian Peninsula. Like all propaganda and political rhetoric, its assertions must not be taken at face value. But to claim that the magazine tells us nothing about al Qaeda in the Arabian Peninsula is simply lazy analysis.

Clearly, the concept of reaching out and attempting to radicalize and equip English-speaking jihadists was not something promoted only by Anwar al-Awlaki and Khan. English-speaking outreach has continued after their deaths. The group maintains that traveling to places such as Yemen for training is too dangerous.

That al Qaeda in the Arabian Peninsula continues to publish Inspire, which takes time and resources to produce, is also revelatory. The group has been under increased pressure over the past 18 months. The jihadists have been pushed back to their desert hideouts from much of the territory they conquered in southern Yemen. Yet despite these setbacks, they continue to devote resources to publishing Inspire, they have people with access to computers and the Internet, and they remain in contact with jihadists in other parts of the world, such as Pakistan and Mali.

The copyediting in Inspire 10 was also cleaner than the previous edition, which had a major typo on the front cover. The new editor, who uses the nom de guerre Yahya Ibrahim, has worked with Khan since the first edition of the magazine. He is a native English speaker who is familiar with Western culture and idioms. Ibrahim was clearly influenced by Khan and has attempted to continue Khan's work, but he lacks Khan's acerbic wit and irreverence. In Inspire 10, for example, Ibrahim attempts to replicate the insulting one-page "advertisements" that Khan included in earlier editions of the magazine -- one in particular racially derided U.S. President Barack Obama -- but they lack the bite and general snark of Khan. Inspire seems to be more serious and less edgy than when Khan was in charge. This may dull its appeal to its targeted audience.

Another thing we can ascertain from Inspire 10 is that, despite al Qaeda in the Arabian Peninsula's continued commitment to foment grassroots terrorism in the West, the group is clearly disappointed by the response it has gotten. The magazine has mobilized some jihadists but probably not as many as the group would like. Those who have been inspired have not been very successful in their attacks.

The Open Source Jihad section also continues to show the low view that al Qaeda in the Arabian Peninsula's professional terrorist cadre has for grassroots operatives. They see them as not-so-exceptional individuals incapable of much more than simple attacks. Yet, since al Qaeda in the Arabian Peninsula lacks the ability to attack the West, the group must depend on these less than ideal individuals to do so for them.

In addition to what it reveals about al Qaeda in the Arabian Peninsula, Inspire 10 can also tell us some important things about what tactics we can expect the group to use and what locations we can expect it to target. Clearly the magazine continues to focus on targets in the West that have insulted the Prophet

Mohammed. It revives the "the dust has not settled" theme from the first edition of the magazine and provides an updated hit list of individuals who have insulted Mohammed, including Terry Jones, the controversial Koran-burning pastor; Morris Sadek, who made a controversial film that disparaged Islam; and Stephane Charbonnier of the French magazine Charlie Hebdo.

We have seen several attacks and thwarted plots directed against these individuals in the past. In fact, in November 2011, Charlie Hebdo's office was completely destroyed by fire, which was started by the very type of accelerant and match attack promoted in Inspire 10. We believe we will continue to see grassroots plots against these targets.

Despite the weakening of the al Qaeda core group and the serious blows that regional franchises such as al Qaeda in the Arabian Peninsula, al Qaeda in the Islamic Maghreb and al Shabaab have suffered in recent months, jihadism continues to attract new adherents. And Inspire hopes to motivate and equip them to conduct attacks in the West.

"Assessing Inspire Magazine’s 10th Edition is republished with permission of Stratfor."

Table of Contents