Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**
US Army Space and Missile Defense Command
Army Forces Strategic Command
G39, Information Operations Division

ARSTRAT IO Newsletter Online

Table of Contents

Vol. 13, no. 08 (June 2013)

Clearing the Air on Cyber, Electronic Warfare

By Ben Iannotta, Deep Dive Intelligence, May 30, 2013

The Army's electronic warfare experts are feeling misunderstood, and they're worried that those misunderstandings could put them on the losing end in today's epic budget battles. The head worrier is Army Col. Jim Ekvall, a one-time artillery man who is now chief of the Electronic Warfare Division within the Army's G-3 operations staff at the Pentagon.

Ekvall wants to seal a place for the EW specialty in the Army's post Afghanistan future and hitch it to the growing field of cyberwarfare. That'll mean winning some internal battles and upgrading equipment, much of which was rushed into service in Iraq and Afghanistan to jam improvised explosive devices.

In a perfect world, Ekvall and his compatriots would give electronic warfare officers, known as EWOs or "29s" after their career field designation, a proposed software called the Electronic Warfare Planning and Management Tool. The EWOs would use it to receive intel about an adversary's comms frequencies and send updates to equipment in the field.

The field equipment could include a new Raytheon-built counter-IED and intel pod that Ekvall hopes will be sent forward, presumably to Afghanistan, for operational assessment on the Army's Gray Eagle unmanned planes. The pod is called NERO for the Networked Electronic Warfare Remotely Operated system. It can send spectrum info back to intel cells but its main purpose will be to jam frequencies used for triggering IEDs. NERO is just like the pods flown in Afghanistan on two traditionally piloted C-12 planes by Task Force CEASAR, short for Communications Electronic Attack with Surveillance and Reconnaissance.

NERO needs careful testing because the Gray Eagle is a radio controlled plane, and NERO will be jamming radio waves. "We gotta kinda make sure we don't make the thing crash," Ekvall tells Deep Dive.

A perfect world would also mean buying a new family of Multifunction Electronic Warfare electronics known as MFEW. A backpack version would let foot soldiers knock out an adversary's comms or jam a specific frequency, such as one used for triggering IEDs. MFEW might replace the jammers that were rushed onto vehicles in Iraq and Afghanistan, called CREW for Counter Radio-Controlled Improvised Explosive Device Electronic Warfare.

Then there's EW's bid for a role in cyberwarfare. EW advocates want a place in an Army cyber center of excellence, should one be created. You can't launch a cyber operation if you don't control the spectrum, Ekvall says. On top of that, troops in theory could use some of the EW equipment to jump the air gap and load malware into an adversary's network. "Could you plant a seed in that communication to cause a cyber attack? You absolutely could," Ekvall says.

When it comes to the relationship between cyberspace and EW, Ekvall wants a bit of history to be remembered. "The realities are the Army's interest in electronic warfare – and it's really a re-birth of electronic warfare inside the Army – preceded its now consuming worries and concerns about cyberspace and cyberspace operations. Whereas cyberspace is still trying to figure out what it all means, electronic warfare has already kind of done that."

Ekvall doesn't know which parts of this vision will come to pass, and he's not happy about that. Electronic warfare saw a resurgence in Iraq and Afghanistan, and that's led to a misperception that EW won't be important once the war in Afghanistan ends, Ekvall explains.

In his view, EW is not just about blocking IEDs, although he definitely sees the importance of that after riding around Iraq in vehicles equipped with jammers. "Electronic warfare is about gaining and maintaining an advantage in the electromagnetic spectrum. A piece of that would be counter IED. A piece of that would be counter comms. A piece of that is… protecting your own precision-guided munitions and your own ability to use, say, satellite communications."

In the world according to Ekvall, the fixation on jamming is the foundation for all the misunderstandings about EW from the Pentagon to Capitol Hill.

EW's confusing nomenclature hasn't helped either. A case in point: The Army manages EW acquisitions within its Intelligence Electronic Warfare & Sensors office, called IEW&S. The EW equipment managed there is collectively known as IEWS, for the Integrated Electronic Warfare System.

The potential for confusion matters at the decision-making levels.

"Things that are more well understood have greater chances of success in this very resource constrained environment that we're working in right now," Ekvall says.

Table of Contents

American Gets Targeted by Digital Spy Tool Sold to Foreign Governments

By Kim Zetter, Wired, 4 June 2013

The email appeared to come from a trusted colleague at a renowned academic institution and referenced a subject that was a hot-button issue for the recipient, including a link to a website where she could obtain more information about it.

But when the recipient looked closely at the sender's email address, a tell-tale misspelling gave the phishing attempt away — the email purported to come from a professor at Harvard University, but instead of harvard.edu, the email address read "hardward.edu".

Not exactly a professional con-job from nation-state hackers, but that's exactly who may have sent the email to an American woman, who believes she was targeted by forces in Turkey connected to or sympathetic to the powerful Gülen Movement, which has infiltrated parts of the Turkish government.

The email contained a link to a web site in Turkey, where a malicious downloader file was waiting to install on her computer — a downloader that has been connected in the past to a spy tool purportedly sold exclusively to law enforcement and intelligence agencies around the world.

The woman, who asked to remain anonymous because she's concerned about retaliation, sensed the email was a fraud and did not follow the link. Instead, the email was passed to researchers at digital forensics firm Arsenal Consulting, who set up a honeypot to visit the Turkish web site and obtained the downloader.

Though investigators didn't obtain the file that the downloader was supposed to install, analysis of it showed that it was the same downloader that has been used in the past to install Remote Control System (RCS), a spy tool made by the Italian company Hacking Team and sold to governments. A digital certificate used to sign the downloader has also been used in the past with Hacking Team's tool.

"It was the first hint that this was connected to Hacking Team and RCS," Mark. G. Spencer, president of Arsenal, told Wired.

Hacking Team asserts that it sells the RCS tool only to law enforcement and government security agencies for lawful intercept purposes, but it has reportedly been used against activists and political dissidents in Morocco and the United Arab Emirates and possibly elsewhere, an issue for which Hacking Team has been severely criticized.

The company touts in marketing literature that the tool evades encryption and bypasses antivirus and other security protections to operate completely invisibly on a target's machine.

The RCS tool, also known as DaVinci, records text and audio conversations from Skype, Yahoo Messenger, Google Talk and MSN Messenger, among other communication applications. It also steals Web browsing history and can turn on a computer's microphone and webcam to record conversations in a room and take photos. The tool relies on an extensive infrastructure to operate and therefore is not easily copied and passed to non-government actors outside that infrastructure to use for their own personal spy purposes, according to a Hacking Team spokesman.

Spencer says there's no definitive proof pointing to who is behind the attempted hack of the American woman, but notes there is circumstantial evidence that warrants further attention.

"We have an email, a purported sender, and a target all critical of the Gülen movement. We have professional malware launched from a server in Turkey. You can take it from there," Spencer said.

Turkey is a member of the North Atlantic Treaty Organization alliance. If authorities there were behind the hack attack, it would mean that a NATO ally had attempted to spy on a U.S. citizen on U.S. soil, presumably without the knowledge or approval of U.S. authorities, and for reasons that don't appear to be related to a criminal or counter-terrorism investigation.

Mustafa Kemal Sungur, a spokesman for the Turkish Embassy in Washington, DC, said he had no comment on the allegations.

Hacking Team spokesman Eric Rabe would not say if Turkey is a customer of its software, only that Hacking Team sells to "several dozen countries."

Speaking generally, he said the company will investigate cases where it believes clients may have used its software in an illegal manner or in a manner that violates the terms of service, and that if a customer is found to be using its software in an illegitimate manner, Hacking Team has ways to render the software useless by halting updates to it.

“If we don’t update the software pretty regularly, antivirus programs will detect the software and it will be useless to the agencies,” he said, referring to tweaks and obfuscations the company adds to the program to thwart detection.

The woman believes she was targeted because she’s an outspoken critic of Turkish charter schools in the U.S. that are run by supporters of the Gülen Movement, a secretive organization led by charismatic Turkish imam and scholar Fethullah Gülen, who resides in exile in Pennsylvania. She believes the email was sent to an anonymous email address she uses in an attempt to identify her and gain access to her private data and communications in order to try to discredit her.

The Gülen Movement has millions of supporters around the world and is behind a network of schools operated in more than 100 countries, including a string of charter schools in the U.S. But critics say that members of the movement have heavily infiltrated the Turkish judicial system and the police intelligence services with the aim of increasing Islamic influences in Turkey and pushing the country in a more conservative direction. Members of the movement are accused of using government and media connections to retaliate against and discredit opponents, including using trumped-up charges to get them jailed.

“We are troubled by the secretive nature of the Gülen movement, all the smoke and mirrors,” an anonymous U.S. official told the New York Times last year. “It is clear they want influence and power. We are concerned there is a hidden agenda to challenge secular Turkey and guide the country in a more Islamic direction.”

The woman who received the phishing attempt says she’s been warned against traveling to Turkey due to her outspoken criticism of the movement’s charter schools.

“I’ve been told by a U.S. official that I should never travel to Turkey, that it would be dangerous for me,” she told Wired.

The body of the email she received read, “Hi, There is a new site about Gülen movement. It is http://www.hizmetesorulanlar.org/homepage.html. Also you should read an essay which I sent. (passwprd:12345).”

The email was signed by a Harvard professor who has written and spoken publicly about the Gülen movement in the past, but the URL in the email actually went to a different web site than the one cited — a poorly designed GeoCities-type page in Turkey with the URL www.mypagex.com/fileshare/questions/main.html.

When Spencer’s team visited the latter web site with a test machine, a malicious Flash component called Anim.swf that appeared to be part of a multi-stage attack got installed on their machine.

“It’s really nice and impressive code,” Spencer told Wired.

This component gathered intelligence about the infected machine’s operating system and browser and was programmed to then download a second-stage Flash attack. Spencer’s team didn’t get a look at the second part, however, because the file was removed from the site before they could grab it. They were, however, able to grab half-a-dozen other components that were stored in folders on the site before being removed. These included the downloader file, an executable program that was designed to grab screenshots from targeted systems and send them to a command-and-control server in Turkey. It was also designed to download another tool, which Spencer believes may have been the main RCS spykit, though he can’t say for certain since the attack wasn’t completed.

The downloader file was digitally signed with a certificate issued to an individual named Kamel Abed. GlobalSign, the certificate authority that issued the certificate, told Wired that the company issued the certificate last November after receiving a legitimate application. The certificate was revoked February 12 after GlobalSign learned of its misuse, following a report by Kaspersky Lab that tied the certificate to Hacking Team’s spy tool.

“The certificate was revoked as soon as our community contacts made us aware of the usage of the key for reasons we do not permit,” GlobalSign CEO Steve Waite said in an email. “We conduct revocation investigations 24/7, and in this case the revocation happened quickly.”

He would not say whether Abed himself had misused the certificate or if someone had stolen it from him to sign the malicious downloader, but he said that GlobalSign revoked the certificate after trying to contact the subscriber to discuss it with him and was unable to reach him.

Asked if Hacking Team had ever been issued a certificate in the name of Kamel Abed or used such a certificate to sign its spy tools, spokesman Rabe said only, “Kamel Abed is a common Arab name, and I‘m not going to comment further than that.”

Arsenal contacted Nicolas Brulez, principal security researcher at Kaspersky Lab, to examine the downloader file and certificate. Kaspersky has written extensively about Hacking Team’s tools in the past, and Brulez found that the downloader code and Kamel Abed certificate were identical to another downloader known to

have been used with the RCS spykit in the past. He also found test code in the downloader file that matched exactly test code found in a component of the RCS spykit, and the two files used the same encryption algorithm to communicate with the command-and-control server. There were other similarities and exact matches as well, all of which led Brulez to conclude, “The guy who made the downloader that Arsenal found also made the RCS.”

Brulez believes the downloader is used by the attackers to first gather intelligence about a victim before determining if they want to send the entire RCS package to the machine. He also believes the RCS tool would have been installed on the U.S. victim’s machine through a zero-day Flash exploit that was used against other RCS victims around the same time she was targeted, before Adobe patched it.

Kaspersky has detected at least 50 incidents of RCS infections on computers in Italy, Mexico, Kazakhstan, Saudi Arabia, Turkey, Argentina, Algeria, Mali, Iran, India and Ethiopia.

Hacking Team came under fire last year after a number of security researchers linked the company’s spy kit to hacks that targeted political activists in Morocco and the United Arab Emirates for purposes of spying on and silencing dissenters.

In Morocco, an activist group known as Mamfakinch was reportedly a target of government spying in that country through use of Hacking Team’s software. And Ahmed Mansoor, an activist from the United Arab Emirate who was jailed for seven months in 2011 with four other activists on charges that they insulted the country’s vice president and threatened state security, was also reportedly targeted with the software.

Rabe called the claims “largely circumstantial,” but wouldn’t elaborate.

The company did investigate the claims, he said, but he wouldn’t disclose the outcome of the investigation.

“There are circumstances where we have refused to work with clients based on our examination of what they were doing or what we thought they were doing,” he said, but he would not say if Morocco and the UAE had been dropped as clients as a result of the allegations.

He said the company is careful about who it sells its software to, and won’t sell it to every country.

“We do our best to know who the agencies are and who the governments are who we’re selling to. There are certain governments we do not sell our software to,” he said, though he wouldn’t identify any countries that had been rejected.

Situations in which someone might abuse the software to spy on innocent people is something that “concerns” the company, he said, though he admits there is little Hacking Team can do to prevent it.

“We know how powerful is the tool that we’ve developed, so we’re doing our best to make sure it doesn’t get abused,” he said.”[B]ut there is a limit to how we can control what someone does with the software.”

Table of Contents

US Army Maps Future of the Electronic Battlefield

By Paul Mcleary, DefenseNews, Jun. 7, 2013

WASHINGTON — In a sense — and in one sense only — American and NATO forces have had it easy in Iraq and Afghanistan.

With uncontested control of the skies and with little to fear from electronic jamming or precision fires, virtually all of the defensive electronic warfare missions they have conducted involve roadside bombs.

But future battlefields will likely be more complex and not quite as permissive, analysts and Pentagon thinkers warn, citing the increasing proliferation of precision munitions and the more sophisticated communications and electronic jamming gear that states can now wield.

Permissive or not, the electronic jamming capabilities the US Army has developed in Iraq and Afghanistan are a far cry from the service’s Centra Spike program, which used commercial airplanes packed with electronics to find and track the location of Colombian drug kingpin Pablo Escobar in the early 1990s.

Since 2011, Army units rotating into Afghanistan have used the Communications Electronic Attack with Surveillance and Reconnaissance (CEASAR) system, a beyond-line-of-sight electronic jammer mounted on a Beechcraft King airplane that can both intercept phone communications on the ground as well as jam enemy cellphones.

The jammer is a repackaged version of the communications jammer found on the EA-18G Growler and was initially sent to Afghanistan in 2011 as a forward operational assessment program.

But the system "did so well in its forward operational assessment, the war fighter said, 'Hey, why don't you leave it here?' " instead of shipping it back to the states, Col. Jim Ekvall, chief of the Army's electronic warfare office, told Defense News on May 20.

While the program has been highly successful in eavesdropping on Taliban cellphone communications and has given dismounted troops a better sense of what they're facing over the next ridgeline, Ekvall is well aware of the issues US forces will likely face in controlling the electromagnetic spectrum in coming years.

"We can't afford to build something that only works in a permissive environment, or it only works in a [counterinsurgency] environment," he said, "but if you take on a sophisticated enemy it's not going to work." Anything the Army builds has to be able to fight across the spectrum. "It's gotta be versatile, it's gotta be flexible, it's gotta be programmable."

Given the success of CEASAR on manned aircraft, the Army is working to attach the jamming pod on its MQ-1C Gray Eagle UAV, dubbing it the Networked Electronic Warfare, Remotely Operated (NERO). Ekvall said the Roman theme is by design: He decided that all of the Army's airborne electronic warfare technologies will use this naming convention.

The move to NERO is indicative of how the Army has changed some of its procurement processes to meet urgent wartime needs over the past decade.

After commanders in Afghanistan started asking about an unmanned version of CEASAR, Ekvall approached the Joint Improvised Explosive Device Defeat Organization to see if it could fund installing a CEASAR on a Gray Eagle. The office funded an assessment program that fit in nicely with the Gray Eagle evaluations the Army was already conducting.

NERO is set to deploy to Afghanistan in 2014 for operational assessments. Both CEASAR and NERO are produced by Raytheon.

Continuing the trend, in January the Army issued a request for information for an even smaller version of the jammer that can be fitted on UAVs — as small as the hand-launched Wasp or Puma.

The service "is looking at some testing where companies can prove out the airborne electronic attack capability that we're calling NERVA," Ekvall said. "Industry has come back and said, 'Hey, we know what CEASAR did; we think we can make it smaller.' "

NERVA — in addition to being a Roman emperor for two years before dying of natural causes — also stands for Networked Electronic Warfare Remote Vehicle-Aerial.

Budgets being what they are, there is some worry that all of these programs — which are being funded completely by supplemental war budgets — might be in trouble once war funding shrinks.

"We're going to continue to rely on [supplemental] funds, but at some point it's going to have to go into the base budget," Ekvall said, acknowledging that competition for resources in coming years will be tight.

Still, given that the Army relies more than ever on a safe, secure electromagnetic spectrum to enable its communications and its growing arsenal of GPS-enabled precision munitions, Ekvall said his job is "all about creating freedom of maneuver in the electromagnetic spectrum" while also defeating the enemy's ability to use the spectrum.

Table of Contents

Silent War

By Michael Joseph Gross, Vanity Fair, July 2013

On the hidden battlefields of history's first known cyber-war, the casualties are piling up. In the U.S., many banks have been hit, and the telecommunications industry seriously damaged, likely in retaliation for several major attacks on Iran. Washington and Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar, enmeshing such high-tech giants as Microsoft, Google, and Apple. With the help of highly placed government and private-sector sources, Michael Joseph Gross describes the outbreak of the conflict, its escalation, and its startling paradox: that America's bid to stop nuclear proliferation may have unleashed a greater threat.

I. Battlespace

Their eyeballs felt it first. A wall of 104-degree air hit the cyber-security analysts as they descended from the jets that had fetched them, on a few hours' notice, from Europe and the United States. They were in Dhahran, in eastern Saudi Arabia, a small, isolated city that is the headquarters of the world's largest oil company, Saudi aramco. The group included representatives of Oracle, IBM, CrowdStrike, Red Hat, McAfee, Microsoft, and several smaller private firms—a SWAT dream team for the virtual realm. They came to investigate a

computer-network attack that had occurred on August 15, 2012, on the eve of a Muslim holy day called Lailat al Qadr, “the Night of Power.” Technically the attack was crude, but its geopolitical implications would soon become alarming.

The data on three-quarters of the machines on the main computer network of Saudi aramco had been destroyed. Hackers who identified themselves as Islamic and called themselves the Cutting Sword of Justice executed a full wipe of the hard drives of 30,000 aramco personal computers. For good measure, as a kind of calling card, the hackers lit up the screen of each machine they wiped with a single image, of an American flag on fire.

A few technical details of the attack eventually emerged into the press. Aboard the U.S.S. Intrepid, in New York Harbor, Defense Secretary Leon Panetta told a group of C.E.O.’s that the aramco hack was “probably the most destructive attack that the private sector has seen to date.” Technical experts conceded the attack’s effectiveness but scorned its primitive technique. “It wrote over memory five, six times,” one hacker told me. “O.K., it works, but it’s not sophisticated.” Even so, many current and former government officials took account of the brute force on display and shuddered to think what might have happened if the target had been different: the Port of Los Angeles, say, or the Social Security Administration, or O’Hare International Airport. Holy shit, one former national-security official recalls thinking—pick any network you want, and they could do this to it. Just wipe it clean.

In the immediate aftermath of the attack, as forensic analysts began work in Dhahran, U.S. officials half a world away gathered in the White House Situation Room, where heads of agencies speculated about who had attacked aramco and why, and what the attackers might do next. Cutting Sword claimed that it acted in revenge for the Saudi government’s support of “crimes and atrocities” in countries such as Bahrain and Syria. But officials gathered at the White House could not help wondering if the attack was payback from Iran, using America’s Saudi ally as a proxy, for the ongoing program of cyber-warfare waged by the U.S. and Israel, and probably other Western governments, against the Iranian nuclear program.

When the history of cyber-warfare comes to be written, its first sentence may go something like this: “Israel gave the United States an ultimatum.” For a number of years, intelligence reports intermittently indicated that Iran was getting closer to building a nuclear bomb, which the Israeli leadership views as an existential threat. In 2004, Israel gave Washington a wish list of weapons and other capabilities it wanted to acquire. The list—for various kinds of hardware but also for items such as aerial transmission codes, so that Israeli jets could overfly Iraq without having to worry about being shot down by U.S. warplanes—left little doubt that Israel was planning a military attack to stop Iran’s nuclear progress. President George W. Bush regarded such action as unacceptable, while acknowledging that diplomacy and economic sanctions had failed to change Iran’s mind.

Intelligence and defense officials offered him a possible third way—a program of cyber-operations, mounted with the help of Israel and perhaps other allies, that would attack Iran’s nuclear program surreptitiously and at the very least buy some time. As with the drone program, the Obama administration inherited this plan, embraced it, and has followed through in a major way. Significant cyber-operations have been launched against Iran, and the Iranians have certainly noticed. It may be that these operations will eventually change minds in Tehran. But the aramco attack suggests that, for the moment, the target may be more interested in shooting back, and with weapons of a similar kind.

Cyberspace is now a battlespace. But it’s a battlespace you cannot see, and whose engagements are rarely deduced or described publicly until long after the fact, like events in distant galaxies. Knowledge of cyber-warfare is intensely restricted: almost all information about these events becomes classified as soon as it is discovered. The commanding generals of the war have little to say. Michael Hayden, who was director of the C.I.A. when some of the U.S. cyber-attacks on Iran reportedly occurred, declined an interview request with a one-line e-mail: “Don’t know what I would have to say beyond what I read in the papers.” But with the help of highly placed hackers in the private sector, and of current and former officials in the military and intelligence establishments and the White House, it is possible to describe the outbreak of the world’s first known cyber-war and some of the key battles fought so far.

II. Flame, Mahdi, Gauss

‘I needed to come up with something cool for self-promotion at conferences,” Wes Brown recalls. The year was 2005, and Brown, a hacker who is deaf and has cerebral palsy, started a business called Ephemeral Security with a colleague named Scott Dunlop. Banks and other corporations hired Ephemeral to hack their networks and steal information, then tell them how to keep bad guys from doing the same thing. So Brown and Dunlop spent a lot of time dreaming up ingenious break-ins. Sometimes they used those ideas to boost their street cred and advertise their business by making presentations at elite hacker conferences—elaborate festivals of one-upmanship involving some of the greatest technical minds in the world.

At a Dunkin' Donuts coffee shop in Maine, Brown and Dunlop started brainstorming, and what they produced was a tool for attacking networks and gathering information in penetration tests—which also amounted to a revolutionary model for espionage. By July of that year, the two men completed writing a program called Mosquito. Not only did Mosquito hide the fact that it was stealing information, but its spy methods could be updated, switched out, and re-programmed remotely through an encrypted connection back to a command-and-control server—"the equivalent of in-flight drone repair," Brown explains. In 2005 the unveiling of Mosquito was one of the most popular presentations at the prestigious hacker conference known as Def Con, in Las Vegas.

Many U.S. military and intelligence officials attend Def Con and have been doing so for years. As early as the 1990s, the U.S. government was openly discussing cyber-war. Reportedly, in 2003, during the second Gulf War, the Pentagon proposed freezing Saddam Hussein's bank accounts, but the Treasury secretary, John W. Snow, vetoed the cyber-strike, arguing that it would set a dangerous precedent that could result in similar attacks on the U.S. and de-stabilize the world economy. (To this day, the Treasury Department participates in decisions concerning offensive cyber-warfare operations that could have an impact on U.S. financial institutions or the broader economy.) After 9/11, when counterterrorism efforts and intelligence became increasingly reliant on cyber-operations, the pressure to militarize those capabilities, and to keep them secret, increased. As Iran seemed to move closer to building a nuclear weapon, the pressure increased even more.

As Wes Brown recalls, none of the government types in the audience said a word to him after his Mosquito presentation at Def Con. "None that I could identify as government types, at least," he adds, with a chuckle. But about two years later, probably in 2007, malware now known as Flame appeared in Europe and eventually spread to thousands of machines in the Middle East, mostly in Iran. Like Mosquito, Flame included modules that could, through an encrypted connection to a command-and-control server, be updated, switched out, and re-programmed remotely—just like in-flight drone repair. The Flame software offered a very full bag of tricks. One module secretly turned on the victim's microphone and recorded everything it could hear. Another collected architectural plans and design schematics, looking for the inner workings of industrial installations. Still other Flame modules took screenshots of victims' computers; logged keyboard activity, including passwords; recorded Skype conversations; and forced infected computers to connect via Bluetooth to any nearby Bluetooth-enabled devices, such as cell phones, and then vacuumed up their data as well.

During that same period, a virus that would be named Duqu—which targeted fewer than 50 machines, mostly in Iran and Sudan—began collecting information about the computer systems controlling industrial machinery, and to diagram the commercial relationships of various Iranian organizations. Duqu, like many other significant pieces of malware, was named for a feature of the code, in this case derived from the names the malware gave to files it created. In time, researchers found that Duqu bore several resemblances to an even more virulent cyber-attack.

As early as 2007, the first versions of a computer worm, designed not for espionage but for the physical sabotage of machinery, began to infect computers in several countries but primarily in Iran. As reported in these pages ("A Declaration of Cyber-War," April 2011), it was one of the most resilient, sophisticated, and noxious pieces of malware ever seen. The following year, after the worm got loose on the Internet, analysis by private experts swiftly produced a detailed conjecture regarding its source, aims, and target. Named Stuxnet, the worm appeared to have come from the U.S. or Israel (or both), and it seemed to have destroyed uranium-enrichment centrifuges at Iran's nuclear facility in Natanz. If the suppositions about Stuxnet are correct, then it was the first known cyber-weapon to cause significant physical damage to its target. Once released into the wild, Stuxnet performed a complex mission of seeking out and destroying its target. Jason Healey, a former White House official who now runs the Cyber Statecraft Initiative for the Atlantic Council, argues that Stuxnet was "the first autonomous weapon with an algorithm, not a human hand, pulling the trigger."

For the U.S., Stuxnet was both a victory and a defeat. The operation displayed a chillingly effective capability, but the fact that Stuxnet escaped and became public was a problem. Last June, David E. Sanger confirmed and expanded on the basic elements of the Stuxnet conjecture in a New York Times story, the week before publication of his book Confront and Conceal. The White House refused to confirm or deny Sanger's account but condemned its disclosure of classified information, and the F.B.I. and Justice Department opened a criminal investigation of the leak, which is still ongoing. Sanger, for his part, said that when he reviewed his story with Obama-administration officials, they did not ask him to keep silent. According to a former White House official, in the aftermath of the Stuxnet revelations "there must have been a U.S.-government review process that said, This wasn't supposed to happen. Why did this happen? What mistakes were made, and should we really be doing this cyber-warfare stuff? And if we're going to do the cyber-warfare stuff again, how do we make sure (a) that the entire world doesn't find out about it, and (b) that the whole world does not fucking collect our source code?"

In September 2011, another piece of malware took to the Web: later named Gauss, it stole information and login credentials from banks in Lebanon, an Iranian ally and surrogate. (The program is called Gauss, as in Johann Carl Friedrich Gauss, because, as investigators later discovered, some internal modules had been given the names of mathematicians.) Three months later, in December, yet another piece of malware began spying on more than 800 computers, primarily in Iran but also in Israel, Afghanistan, the United Arab Emirates, and South Africa. This one would eventually be named Mahdi, after a reference in the software code to a messianic figure whose mission, according to the Koran, is to cleanse the world of tyranny before the Day of Judgment. Mahdi was e-mailed to individuals who worked in government agencies, embassies, engineering firms, and financial-services companies. In some cases, the Mahdi e-mails bore a Microsoft Word file attachment containing a news article about a secret Israeli-government plan to cripple Iran's electrical grid and telecommunications in the event of an Israeli military strike. Other Mahdi e-mails came with PowerPoint files containing slides bearing religious images and text. Anyone who received these e-mails and clicked on the attachment became vulnerable to infection that could result in their e-mails, instant messages, and other data being monitored.

Time started running out for all this malware in 2012, when a man from Mali met with a man from Russia on a spring day in Geneva. The man from Mali was Hamadoun Touré, secretary-general of the International Telecommunication Union, a U.N. agency. He invited Eugene Kaspersky, the Russian C.E.O. of the cyber-security firm Kaspersky Lab, to discuss a partnership to perform forensic analysis on major cyber-attacks—"like a Stuxnet," as Kaspersky recalls. Kaspersky says that Touré made no explicit mention of Iran, even though Stuxnet was an impetus for the collaboration.

The partnership sprang into action within a month of that Geneva meeting, in response to a cyber-attack on Iran that had wiped data from the memory of an unknown number of computers at the country's oil-and-gas ministry. Iranian officials said the cyber-attack, by malware that came to be called Wiper, did not affect oil production or exports, but the ministry reportedly cut Internet access to the national oil company as well as to oil facilities and oil rigs, and to the main sea terminal for oil exports on Kharg Island, for two days.

While investigating the Wiper attack, Kaspersky analysts also discovered Flame, which they announced on May 28, 2012. Kaspersky researchers wrote that Flame appeared to have been state-sponsored and contained elements of Stuxnet's code, suggesting that the makers of both pieces of malware had collaborated in some way. Further evidence that Flame may have been state-sponsored appeared almost immediately after it was made public. At that point, Flame's operators pushed a self-destruction module to the malware, and its command-and-control infrastructure went down. Criminal malware does not delete itself so neatly and so quickly, but intelligence operations generally include "fail-safe" plans to abort if discovered.

For the next few months, Kaspersky's team was off to the races. It announced Gauss in June and Mahdi in July. In October, it found a much smaller, more targeted version of Flame, called MiniFlame, which had been used to spy on a few dozen computers in Western Asia and Iran, as early as 2007. Traces of some of these pieces of malware were found inside one another. MiniFlame was not only a freestanding program, for instance, but also a module used by both Gauss and Flame, which itself spawned elements of Stuxnet, which was built on the same software platform as Duqu.

Beyond Kaspersky's discoveries, the Iranian press occasionally published news of other cyber-attacks on the country's nuclear program, though none have been independently verified. One person claiming to be an Iranian nuclear scientist e-mailed a prominent researcher in Finland to say that hackers had caused music to play on workstations at full blast in the middle of the night. "I believe it was playing 'Thunderstruck' by AC/DC," the e-mail said.

A small but dedicated group devoured all this news and teased out the possibilities. Wes Brown, who now works as chief architect at ThreatGrid, was struck by Flame's many similarities to his groundbreaking Mosquito program. His first thought upon seeing Flame's code was "It's about time"—it had been two years since he and his buddy brought Mosquito into the world, so he figured that by now, "it was a certainty that a state organization could do what we did."

The man whose company discovered most of this malware, Eugene Kaspersky, became an object of increasing curiosity. One night in January of this year, I arrived for a conversation at his suite in Manhattan's Dream Downtown hotel, where his company was hosting a product launch. Kaspersky answered the door and welcomed me in a way that conveyed two of the qualities—gregarious wonderment and fantastical suspicion—that make him a leading thinker on the topic of cyber-warfare. Still getting dressed, he ducked into his bedroom to button and tuck in his shirt, then summoned me to see a creepy painting on the wall: an extreme close-up of a young woman's face, topped by a Girl Scout cap. The young woman wore big Lolita-style sunglasses. "Terrible," Kaspersky said, shaking his shaggy gray hair. Pointing to the dark sunglasses, he said

in broken English that he feared that behind them there were only black holes where the girl's eyes ought to be.

Kaspersky's early education took place at a school supported by the K.G.B., and he and his company have a variety of relationships, both personal and professional, with various Russian-government leaders and agencies. (After one journalist wrote in detail about those connections, Kaspersky accused the journalist of indulging "cold-war paranoia" and responded that, far from being a "spy and Kremlin team member … the reality however is much more mundane—I'm just a man who's 'here to save the world.' ") But some have wondered if his company's 2012 streak of disclosures was in part politically motivated—all of the spyware Kaspersky made public seems to have advanced U.S. interests and undermined Iranian interests, and many suspect that Iran receives support for its cyber-operations from Russia. Kaspersky denies this, pointing to the company's disclosure of the "Red October" cyber-espionage operation—aimed at governments worldwide—which appears to have been Russian in origin. When it comes to cyber-attacks on Iran, Kaspersky's analysts stop short of explicitly pointing fingers at Washington, but it would seem that sometimes their innuendo obviates the need to name names.

One of the most innovative features of all this malware—and, to many, the most disturbing—was found in Flame, the Stuxnet precursor. Flame spread, among other ways, and in some computer networks, by disguising itself as Windows Update. Flame tricked its victim computers into accepting software that appeared to come from Microsoft but actually did not. Windows Update had never previously been used as camouflage in this malicious way. By using Windows Update as cover for malware infection, Flame's creators set an insidious precedent. If speculation that the U.S. government did deploy Flame is accurate, then the U.S. also damaged the reliability and integrity of a system that lies at the core of the Internet and therefore of the global economy.

Asked whether he sees this development as crossing a Rubicon, Kaspersky raised his hand as if to make a point, brought it back down to his chest, then put his fingers to his mouth and cast his eyes to the side, collecting his thoughts. In an hour-long interview, it was the only question that made him fidget. The response he settled on evoked the moral ambiguity—or, maybe, incoherence—of a cyber-warfare operation such as Flame, which surreptitiously did wrong for the sake of doing right. "It's like gangsters in a police uniform," he finally said. Pressed about whether governments should be held to a higher standard than criminals, Kaspersky replied, "There is no rules for this game at the moment."

III. Boomerang

In June of 2011, someone broke into the computer networks of a Dutch company called DigiNotar. Inside the networks the hacker generated and stole hundreds of digital certificates—electronic credentials that Internet browsers must receive from network servers as proof of a Web site's identity before encrypted data can flow back and forth between a computer and the site. Digital certificates had been stolen before but never in such quantity. Whoever was behind the DigiNotar hack could have broken into other networks and used the stolen certificates to intercept Web traffic anywhere and to conduct surveillance on anyone. They could have stolen information worth millions of dollars or unearthed the secrets of some of the world's most powerful people. But instead, for two months, the hackers who controlled DigiNotar's certificates, apparently in Iran, conducted "man in the middle" attacks on Iranian connections to and from sites including Google, Microsoft, Facebook, Skype, Twitter, and—notably—Tor, which provides anonymizing software that many dissidents in Iran have used to elude state surveillance. The hackers were intent on intercepting the e-mails, passwords, and files of ordinary Iranians.

A 21-year-old in Tehran who goes by the name of Comodohacker took responsibility for the DigiNotar breach. In an online posting, he claimed the hack was revenge for an episode in the Balkan wars when Dutch soldiers surrendered Muslims to Serb militias; the Muslims were summarily executed. But the scale and focus of this event—in one month alone, 300,000 people in Iran who connected to Google were vulnerable to hacking via stolen DigiNotar certificates—led many to believe that the Iranian government had engineered the DigiNotar breach itself, using Comodohacker as camouflage. One analyst who spent months investigating the event scoffs at the young man's claim of responsibility. "Twenty-one-year-old hackers are the new stealth," he says—meaning that militaries use hackers to hide their operations the same way they use advanced design to hide bombers. (After details of the DigiNotar hack were made public, the company went bankrupt.)

The U.S. began cultivating cyber-capabilities as an adjunct to its diplomatic, intelligence, and military operations. Iran's initial impetus was to suppress domestic dissent, especially in the wake of the 2009 Green Revolution protests, when citizens took to the streets to dispute the re-election of President Mahmoud Ahmadinejad. But ever since the Stuxnet attack, Iran has been enhancing its cyber-warfare capability. Public remarks by government leaders in March 2011 indicated that the Iranian Revolutionary Guard had created a cyber unit to coordinate offensive attacks on "enemy sites." In March 2012, Ayatollah Ali Khamenei

established the High Council of Cyberspace; reportedly, Iran is spending $1 billion on building cyber-capabilities.

A symmetric warfare—unconventional, guerrilla-style attacks on more powerful adversaries, such as the U.S.—is a cornerstone of Iranian military doctrine. The Revolutionary Guard has ties to terrorist organizations and to prominent hacker groups both in Iran and around the world. Iran may be receiving support for its cyber-operations not only from Russia but also from China and the terrorist network Hezbollah. A top hacker with many well-placed friends in the U.S. government says, "I hear Iran pays Russian guys millions to do the attacks, and the guys are living high, flying in prostitutes from all over." Who told him this? "Nobody who would talk to you," he says. Other dramatic but plausible speculation abounds. One high-level Lebanese political operative believes that the Revolutionary Guard runs its cyber-operations from a six-story underground bunker in a Hezbollah-controlled neighborhood of Beirut called Haret Hreik. Lebanon's absence of any laws against cyber-crime or hacking would make it an appealing launching pad for operations. "Consider how Iran uses Hezbollah as a platform for many critical activities," the Lebanese operative notes. "We say, 'Lebanon is the lungs through which Iran breathes.' Iran wouldn't breathe these attacks with its own lungs. They need a way to answer Stuxnet without having to answer for what they are doing. Hezbollah is the way."

As recently as February of 2012, U.S. defense officials privately dismissed Iran's cyber-warfare efforts as trifling. By August, many had come to believe that the aramco hack showed that Iran was learning fast. In essence, the aramco attack was a mirror image of what had happened when Wiper shut down Kharg Island. Before aramco, Kharg had been the only major cyber-attack on record whose goal was to annihilate data rather than to steal or alter it. The worm that struck aramco, named Shamoon (a word found in the program, the Arabic version of the proper name Simon), adopted this same tactic. Kaspersky believes that Shamoon was a copycat, inspired by the Kharg Island hack. In its attack technique, if not in its actual code, Shamoon anticipates the well-known boomerang effect in weaponry: adaptation and re-deployment of a weapon against the country that first launched it.

Two weeks after the aramco attack, Qatar's state-owned natural-gas company, RasGas, was also hit by malware. Unconfirmed reports say that the cyber-weapon used was also Shamoon. Qatar, home to three U.S. military bases, is among America's closest allies in the Middle East and, therefore, another convenient proxy target.

During the second week of September 2012, a new spate of cyber-attacks against American interests began. This time, the targets were on American soil: U.S. banks. A previously unknown group calling itself the Izz ad-Din al-Qassam Cyber Fighters and presenting itself as an organization of Sunni jihadists made an online posting written in broken English, referring to an anti-Islamic video on YouTube called "Innocence of Muslims" that had sparked riots in the Muslim world the week before. The posting stated that "Muslims must do whatever is necessary to stop spreading this movie All the Muslim youths who are active in the Cyber world will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult."

If Qassam really were a Sunni jihadist group, then Iran, a predominantly Shiite nation, would hardly have been involved. But the jihadist flavoring appears to be a false flag. As one U.S. intelligence analyst points out, none of the language used in Qassam's public communication bears any resemblance to the standard language of jihadist groups. There was no trace of Qassam's formation in any Sunni, jihadist, or al-Qaeda online forums. And the name Qassam itself refers to a Muslim cleric who has significance for Palestinians and Hamas but not for jihadists. "Everything is wrong," this analyst says. "It looks manufactured."

Qassam announced that it would inundate Bank of America and the New York Stock Exchange with distributed-denial-of-service (DDoS) attacks. Such attacks seek to crash a Web site or induce the failure of a computer network by making an overwhelming number of requests for connections. Qassam proceeded to expand its targets to include many more banks, including SunTrust, Regions Financial, Webster Financial Corporation, JPMorgan Chase, CitiGroup, Wells Fargo, U.S. Bancorp, Capital One, PNC, Fifth Third Bank, HSBC, and BB&T. Qassam knocked at least five of these banks' Web sites off-line, though most of the banks have said that no money or information was stolen. In October, PNC bank C.E.O. James Rohr stated that "we had the longest attack of all the banks" and warned that "cyber-attacks are a very real, living thing, and if we think we are safe that way, we're just kidding ourselves." Shortly afterward, the attacks on PNC escalated, causing further problems. Neither Rohr nor any other high-level executive of any victim bank has since made any such conspicuous and pointed statement. "The lesson from Rohr's statement was, don't talk," says one former national-security official.

As an attack technique, DDoS is primitive, and the impact is usually evanescent. But the difference between Qassam's DDoS and previous attacks was like the difference between a crowded parking lot at the mall and a full-on, road-rage-inducing L.A. traffic jam on Memorial Day weekend. Qassam's DDoS was especially

effective—and, for its victims, especially damaging—because it hijacked entire data centers full of servers to do its work, generating 10 times more traffic than the largest hacktivist DDoS previously recorded. (That was Operation Avenge Assange, launched by Anonymous in defense of Wikileaks, in December 2010.)

To absorb the gargantuan volume of traffic coming their way, banks had to buy more bandwidth, which telecommunication companies had to create and provide. Telecoms have borne the brunt of these battles, just as the banks have, spending large sums to expand their networks, and to strengthen or replace hardware associated with their "scrubber" services, which absorb DDoS traffic. Qassam's first wave of attacks was so intense that it reportedly broke the scrubbers of one of this country's largest and best-known telecom companies. In December, AT&T executive director of technology security Michael Singer reportedly stated that the attacks posed a growing threat to the telecommunications infrastructure, and that the company's chief security officer, Ed Amoroso, had reached out to government and peer companies to collaborate in defending against the attacks. Neither Amoroso nor any of his peers have provided specific information about the damage done or the exact cost to telecom companies. (Amoroso declined to comment.)

Qassam Cyber Fighters, like Comodohacker and the Cutting Sword of Justice, launched attacks that were technically unsophisticated enough that they could have been executed by any talented hacktivist or criminal group. But the context, timing, techniques, and targets of Qassam's DDoS all but implicate Iran or its allies. The unpublished research of one cyber-security analyst provides some concrete though circumstantial evidence connecting the bank attacks to Iran. A few weeks prior to the start of the attacks, in September, several individual hackers in Tehran and an Iranian hacker living in New York bragged of having created the same kind of attack tools that Qassam would use. The hackers made postings online offering those tools for sale or rent. The postings were then mysteriously deleted. A hacker in Iran who appeared to be the prime mover in this group goes by the name of Mormoroth. Some of the information concerning these attack tools was posted to his blog; the blog has since disappeared. His Facebook page includes pictures of himself and his hacker friends in swaggering poses reminiscent of Reservoir Dogs. Also on Facebook, his hacking group's page bears the slogan "Security is like sex, once you're penetrated, you're fucked."

Communications from Qassam have been traced to a server in Russia that had only once previously been used for illicit activity. This might indicate that Qassam's attacks were planned with greater care and deliberateness than is typical of hacktivist or criminal intrusions, which usually come from servers where illicit activity is common. This I.P. address, however, like almost all tracebacks of Web traffic, could easily have been faked. Whoever they are, the Qassam Cyber Fighters have a sense of humor. Some of the computers they leveraged for use in the bank attacks were located inside the U.S. Department of Homeland Security.

Critically, two other things distinguish Qassam, according to an analyst who works for several victim banks. First, each time the banks and Internet-service providers figure out how to block the attacks, the attackers find a way around the shields. "Adaptation is atypical," he says, and it may indicate that Qassam has the resources and support more often associated with state-sponsored hackers than with hacktivists. Second, the attacks appear to have no criminal motive, such as fraud or robbery, suggesting that Qassam may be interested more in making headlines than in causing truly meaningful harm. The researcher points out that, for all the hassle and financial damage Qassam has caused its victims, its main accomplishment has been to make news pointing up American weakness in the cyber realm at a time when the U.S. wants to demonstrate strength.

The U.S. banking leadership is said to be extremely unhappy at being stuck with the cost of remediation—which in the case of one specific bank amounts to well over $10 million. The banks view such costs as, effectively, an unlegislated tax in support of U.S. covert activities against Iran. The banks "want help turning [the DDoS] off, and the U.S. government is really struggling with how to do that. It's all brand-new ground," says a former national-security official. And banks are not the only organizations that are paying the price. As its waves of attacks continue, Qassam has targeted more banks (not only in the U.S., but also in Europe and Asia) as well as brokerages, credit-card companies, and D.N.S. servers that are part of the Internet's physical backbone.

For a major bank, $10 million is a drop in the bucket. But bank executives, and current and former government officials, see the recent attacks as shots across the bow: demonstrations of power and a portent of what might come next. One former C.I.A. officer says of the conflict thus far, "It's like the fingernail full of coke, to show that you're dealing with the real thing." Of the bank attacks in particular, a former national-security official says, "If you're sitting in the White House and you can't see that as a message, I think you're deaf, dumb, and blind."

Another hack, which occurred even as the bank attacks continued through the spring, delivered a still more dramatic financial threat, although its ultimate source was difficult to discern. On April 23, the Twitter account of the Associated Press sent this message: "Breaking: Two Explosions in the White House and Barack Obama

Is Injured." Faced with this news, the Dow Jones Industrial Average dropped 150 points—the equivalent of $136 billion in value—within a matter of minutes. Upon learning that the information was false—and that the A.P.'s Twitter account had simply been hacked—the markets rebounded. A group calling itself the Syrian Electronic Army (S.E.A.) claimed credit for the disruption.

But did the S.E.A. act alone? Previously, the S.E.A. had hacked the Twitter accounts of several other news organizations, including the BBC, Al Jazeera, NPR, and CBS. But none of its hacks had taken aim at, or caused any collateral damage to, the U.S. financial system. That distinction had previously belonged only to the Qassam Cyber Fighters, who, as noted, likely have Iranian ties.

One Middle Eastern cyber-analyst in London has said that "there are strong indications that members of [S.E.A.] are trained by Iranian experts." And an American analyst pointed out that the A.P. hack—which used information warfare to cause financial damage—not only resembles Qassam's technique but also mirrors Iran's own perception of what the U.S. has done to the Islamic Republic. (Last year, before Qassam began its attacks on the banks, state-run Iranian media asserted that the U.S. had driven Iran's currency to the brink of collapse by telling lies about Iran.) At this point, there's no solid evidence that Iran was party to the A.P. hack, but among the list of plausible scenarios, none is comforting. Perhaps, with Iran's help or urging, the S.E.A. continued Qassam's experimentation with threats on the U.S. financial system. Perhaps the S.E.A. learned from Qassam's bank attacks and launched an independent operation on the same model. Or perhaps whoever hacked the A.P. had no financial outcome in mind at all—it was just a $136 billion aftershock.

IV. The Cyber-Arms Bazaar

Throughout the fall and winter of 2012, U.S. officials began to speak more frequently than usual about cyber-war. During the same period, Iranian officials offered unusually detailed accusations regarding Western sabotage. On September 17, an Iranian official claimed that power lines to its nuclear facility at Fordow had been damaged, perhaps by Western "terrorists and saboteurs." The next day, the bank attacks commenced, and State Department chief counsel Harold Koh stated for the record that the Obama administration believes the law of war applies to cyber-operations. He emphasized that "civilian objects … under international law are generally protected from attack." The following week, Iran claimed that the German manufacturer Siemens had planted tiny explosives inside some of the hardware used for its nuclear program. Siemens denied any involvement. Then Western intelligence sources let The Sunday Times of London know that another explosion had occurred at Fordow. This time, a spying device disguised as a rock blew up when Iranian soldiers tried to move it.

In the subsequent months, as the bank attacks continued, the U.S. and Iran appeared to engage in a kind of semi-public tit for tat. In November, a classified Presidential Policy Directive was leaked to The Washington Post; the directive allowed the military to take more aggressive steps to defend computer networks in the U.S. In December, Iran conducted a cyber-warfare drill during its naval exercises in the Strait of Hormuz, to demonstrate the resilience of its submarines and missiles to cyber-attack. In January 2013, Pentagon officials reportedly approved a fivefold increase in the number of U.S. Cyber Command personnel, from 900 to 4,900, over the next few years. An Iranian general, as if in response, noted publicly that the Revolutionary Guard controls "the fourth largest cyber army in the world."

In the midst of all this, the Pentagon's secretive research-and-development wing, the Defense Advanced Research Projects Agency (DARPA), invited hackers to propose "revolutionary technologies for understanding, managing, and planning cyberwarfare," for use in a new effort called "Plan X." Plan X aims to persuade some of the most talented hackers in the country to lend the Pentagon their skills. The best talents in cyber-security tend to work in the private sector, partly because corporations pay better and partly because many hackers lead unconventional lives that would clash with military discipline. Drug abuse, for instance, is so common in the hacking subculture that, as one hacker told me, he and many of his peers could never work for the government or the military, because "we could never get high again."

For at least a decade, Western governments—among them the U.S., France, and Israel—have been buying "bugs" (flaws in computer programs that make breaches possible) as well as exploits (programs that perform jobs such as espionage or theft) not only from defense contractors but also from individual hackers. The sellers in this market tell stories that suggest scenes from spy novels. One country's intelligence service creates cyber-security front companies, flies hackers in for fake job interviews, and buys their bugs and exploits to add to its stockpile. Software flaws now form the foundation of almost every government's cyber-operations, thanks in large part to the same black market—the cyber-arms bazaar—where hacktivists and criminals buy and sell them. Some of this trade is like a floating craps game, occurring at hacker conventions around the globe. At gatherings such as Def Con in Las Vegas, dealers in bugs and exploits reserve V.I.P. tables at the most exclusive clubs, order $1,000 bottles of vodka, and invite top hackers to hang out. "It's all about the relationships, all about the drinking," says one hacker. "This is why government needs the black

market: you can't just call up someone in the sober light of day and say, Can you write a bug for me?" The most talented hackers—smartest guys in the room, to a man—are egged on and beckoned to devise ever more ingenious intrusion capabilities, for which someone, somewhere, is always willing to pay.

In the U.S., the escalating bug-and-exploit trade has created a strange relationship between government and industry. The U.S. government now spends significant amounts of time and money developing or acquiring the ability to exploit weaknesses in the products of some of America's own leading technology companies, such as Apple, Google, and Microsoft. In other words: to sabotage American enemies, the U.S. is, in a sense, sabotaging its own companies. None of these companies would speak on the record about the specific issue of U.S.-government use of flaws in their products. Speaking more generally about the use of flaws in Microsoft products by many governments, Scott Charney, head of Microsoft's Trustworthy Computing Group, points out that nations have been conducting military espionage from time immemorial. "I don't expect it to stop," he says, "but governments should be candid that it is going on and have a discussion about what the rules should be." More openly defining what is legitimate for military espionage and what is not would be constructive. This would bring order to the mess of outdated laws and contradictory cultural precepts that aggravate the uncontrollable, unintended consequences of cyber-operations by nation-states. Brad Arkin, Adobe's chief security officer, says, "If you drop a bomb, you use it once and then it's done, but an offensive exploit in the digital realm, once it's used, it's out there Regardless of what [its initial intended] use was, it very quickly rolls downhill." First, he explains, it's "used by nation-states for espionage, and then you see it quickly go towards the financially motivated, and then to the hacktivists, whose motivations are hard to predict."

Meaningful discussion of U.S. cyber-warfare continues to take place behind veils of secrecy that make the drone program look transparent. President Obama, who has defended American use of drones, has never spoken about offensive cyber-warfare. The leak of information about Stuxnet has only driven that conversation further underground. "Our bureaucracy confirms what our elected officials are unwilling to acknowledge," says one former intelligence officer, regarding the F.B.I.'s leak investigation into Stuxnet, which no government entity has officially claimed as a U.S. project. "It's absurd."

Fundamentally, cyber-warfare is a story about proliferation. Iran's nuclear program crossed a line that Israel and the U.S. deemed unacceptable, so the U.S. and its allies used a secret new weapon to try to stop it. With Stuxnet becoming public, the U.S. effectively legitimized the use of cyber-attacks outside the context of overt military conflict. Stuxnet also appears to have emboldened Iran to mount attacks on targets of its choosing. One former government official says, "What did we anticipate that Iran's reaction [to Stuxnet] was going to be? I bet it wasn't going after Saudi aramco."

The paradox is that the nuclear weapons whose development the U.S. has sought to control are very difficult to make, and their use has been limited—for nearly seven decades—by obvious deterrents. In the years since August 1945, a nuclear weapon has never been used in war. Cyber-weapons, by contrast, are easy to make, and their potential use is limited by no obvious deterrents. In seeking to escape a known danger, the U.S. may have hastened the development of a greater one.

And unlike the case with nuclear weapons, anyone can play. Wes Brown, who has never sold a bug or exploit to a government but whose Mosquito program may have inspired part of the best-known cyber-warfare operation so far, puts it simply. "You don't have to be a nation-state to do this," he says. "You just have to be really smart."

Table of Contents

US Disrupts Al-Qaeda's Online Magazine

By Ellen Nakashima, Washington Post, 11 Jun 2013

U.S. intelligence operatives covertly sabotaged a prominent al-Qaeda online magazine last month in an apparent attempt to sow confusion among the group's followers, according to officials.

The operation succeeded, at least temporarily, in thwarting publication of the latest issue of Inspire, the English-language magazine distributed by al-Qaeda in the Arabian Peninsula. When it appeared online, the text on the second page was garbled and the following 20 pages were blank. The sabotaged version was quickly removed from the online forum that hosted it, said independent analysts who track Islamist militant Web sites.

It is unclear how the hacking occurred, although U.S. intelligence agencies, including the National Security Agency and the CIA, have invested heavily in cyber-capabilities in recent years. Security officials, speaking on the condition of anonymity, said the recent operation was only the latest U.S. attempt to disrupt al-Qaeda's online propaganda.

“You can make it hard for them to distribute it, or you can mess with the content. And you can mess with the content in a way that is obvious or in ways that are not obvious,” said one intelligence official, who, like others, spoke on the condition of anonymity in order to discuss sensitive internal debates.

Officials at the Office of the Director of National Intelligence, which oversees the government’s 16 intelligence agencies, declined to comment, as did the White House and the Pentagon.

The hacked version of Inspire magazine appeared May 14, said Evan Kohlmann, an analyst who tracks jihadist Web sites. His firm, Flashpoint Global Partners, captured an image of the issue, which featured a cover showing a fighter in a heavy coat, shouldering a rocket-propelled grenade launcher and a Kalashnikov rifle. The title was “How Did It Come to This?”

Within half an hour of its appearance, the magazine was removed, presumably in response to the hacking, Kohlmann said.

On May 30, a new version, Issue 11, appeared. That issue portrayed the Boston Marathon bombing as vindication of Inspire’s message that “a single lone jihad operation can force America to stand on one foot and live in a terrified state, full of fear.”

Inspire comprises first-person accounts of operations, exhortations to jihad and do-it-yourself advice for extremists. A second intelligence official said the publication is seen as a threat because it “has a specific readership — a following.

People will look for it, as opposed to something randomly posted. Two, it is very user-friendly. Inspire uses pictures and step-by-step diagrams, and that’s a problem.”

Does disruption work?

The decision to disrupt the magazine last month was part of a debate within the Obama administration over the response to online publications that promote radicalization.

The debate spiked after the April 15 Boston Marathon bombing. One of the suspects, Dzhokhar Tsarnaev, 19, told the FBI that he and his late brother, Tamerlan Tsarnaev, 26, learned from the magazine how to make the pressure-cooker bombs used in the attack. He also told them they had been inspired by sermons and other material from the Internet, said officials briefed on the disclosures.

“There’s a robust debate in the community about where do you draw the line on whether or not you should interfere with or take down certain sites,” the second intelligence official said.

Current and former government officials said the debate has been swayed by an argument that Inspire represents an incitement to imminent lawless action, which outweighs First Amendment protections. A 2011 Justice Department “white paper” invoked a similar concept in debates over the lethal targeting of U.S. citizens.

Incitement to violent action is an Inspire staple. A 2010 issue, for example, provided instructions for turning a pickup truck into “The Ultimate Mowing Machine” by welding steel blades onto the front at headlight level — about the height of a human torso — and then plowing into a crowd “to strike as many people as possible.”

The FBI later investigated a homegrown terrorist cell on the East Coast that discussed using the mowing-machine technique, said a consultant who worked on the investigation.

“I don’t think al-Qaeda has a First Amendment right to put out its propaganda, to encourage people to commit acts of terrorism,” said Rep. Adam B. Schiff (D-Calif.), a member of the House Intelligence Committee, who declined to comment on specific cases. “Unfortunately, I think Inspire magazine is a significant threat to the extent that it disseminates information about how to build a bomb or encourages people to get radicalized. It has shown a dangerous effectiveness. And one that’s difficult to address.”

Others contend that disruption is not the best long-run strategy. “The only way that you’re really going to be effective is to help amplify more mainstream moderate Muslim voices,” said Michael E. Leiter, former director of the National Counterterrorism Center. “That’s vastly more effective than trying to disrupt radical voices.”

In the case of Inspire, the debate stretches back three years. The first issue contained a recipe for making a bomb using common materials, such as nails and a pressure cooker like the ones used in Boston. The title of the article was “Make a Bomb in the Kitchen of Your Mom.”

There was also a threat to Molly Norris, a Seattle cartoonist who published a satirical cartoon about the prophet Muhammad. “She should be taken as a prime target of assassination,” wrote Anwar al-Awlaki, the American-born cleric who was later killed in a U.S. drone strike.

“It’s obvious if people are calling for crazies to murder a U.S. citizen, why wouldn’t you stop it?” said one former official, recalling the debate in which Gen. Keith B. Alexander, director of the National Security Agency, argued on behalf of disruption.

In that case, the administration decided against action, in part because the CIA preferred to use the site to gather intelligence. In subsequent debates, the danger of an imminent threat “really made the difference” in terms of whether to disrupt issues of the magazine, according to a former administration official.

Attacks on production

Although techniques are carefully guarded, officials said U.S. intelligence operatives have monitored the magazine during its production process through overseas computer networks.

Each time an issue is about to hit the Internet, officials from the NSA, the CIA, the Pentagon, the State Department and the Justice Department debate whether to sabotage it.

In cases where threats appear imminent, steps might be taken to disrupt publication. In some cases, cyberspies sabotage files so that they come up blank when a user clicks on them, according to the former official. In one case, the official said, the sabotage was not corrected for months.

Sometimes, the disruption occurs when the magazine is being put together, intelligence officials said. An U.S. operator might alter a technical point in a set of bomb-making instructions so the device will not work. The sabotage could go unnoticed for a long time, an official said.

Still, the disruptions are temporary, and the content usually makes its way online.

The quality of Inspire’s writing diminished after Awlaki and Samir Khan, the American-born editor of the magazine, were killed in a drone strike in Yemen in September 2011. Despite intelligence assessments that Inspire might disappear after the deaths, it has continued to publish.

Table of Contents

Marines Focused At the Tactical Edge of Cyber, Says Commander

By Defense Systems Staff, Jun 11, 2013

Today there are 300 Marines and civilians handling cyber operations as part of the Marine Corps Forces Cyberspace Command (MARFORCYBER), and what differentiates them from personnel at the other military cyber commands is their focus on forward-deployed warfighters.

"Where we differ is that we look more at tactical-level cyber operations and how we will be able to provide our forward-deployed Marine air-ground task force commanders with the capability to reach back into the cyber world (at home) to have their deployed units supported," said MARFORCYBER commander Lt. Gen. Richard Mills, who was interviewed for an article written by American Forces Press Service. “We're more focused at the tactical level, the tactical edge of cyber operations, in supporting our forward-deployed commanders, and that's what we should do.”

The air-ground task force that Mills referred to integrates ground, aviation and logistics combat elements under a common command element.

MARFORCYBER stood up in January 2010, and will expand to about 1,000 people by 2016, reports the American Forces Press Service.

The following comments from Mills address other Marine Corps cyber issues, as quoted by the American Forces Press Service.

One coordination with other cyber commands: "All four of the component commanders talk regularly to each other and meet regularly at CYBERCOM (U.S. Cyber Command) to coordinate our growth, coordinate our requirements, (provide) input to CYBERCOM and take its guidance and direction, and operate together in big exercises like Cyber Flag (an annual exercise at Nellis Air Force Base, NV).”

On the role of contractors: "One of the challenges of cyber is that it's such a dynamic environment. You need people who are educated and current in their specialties and who are available to stay on the job for long periods of time, whereas Marines come and go in the normal assignment process.

"They all operate under the same clearance requirements, the same authorities, the same rules. That's one of the things that make them so expensive. They come at a cost, but you have to bear it to make sure that your cyber capabilities are current and that you stay on the cutting edge."

On the impact cyber on defensive and offensive operations: "I think cyber commanders now understand when you go forward you have to be able to defend your systems against intrusion by other states, by rogue elements and even by hobbyists who are just trying to break in and infiltrate your nets. But they're also beginning to understand the positive effects cyber can have in your operations against potential enemies. It's a very valuable tool in that quiver of arrows that a commander takes forward, and they want to understand how it operates."

On cyber weapons: A cyber weapon "can be something as simple as a desktop computer. It's also a vulnerability to you, because it's a way in which the enemy can enter your Web system if you put the wrong hardware on there or open the wrong attachment or email. The armories of the cyber world are very sophisticated computers and very sophisticated smart people who sit behind those computers and work those issues for you."

Table of Contents

With Troops and Techies, US Prepares For Cyber Warfare

Posted on Frontier Post, 7 June 2013

WASHINGTON: On the site of a former military golf course where President Dwight Eisenhower once played, the future of US warfare is rising in the shape of the new $358 million headquarters for the military's Cyber Command.

The command, based at Fort Meade, Maryland, about 25 miles north of Washington, is rushing to add between 3,000 and 4,000 new cyber warriors under its wing by late 2015, more than quadrupling its size.

Most of Cyber Command's new troops will focus on defence, detecting and stopping computer penetrations of military and other critical networks by America's adversaries like China, Iran or North Korea.

But there is an increasing focus on offense as military commanders beef up plans to execute cyber strikes or switch to attack mode if the nation comes under electronic assault.

"We're going to train them to the highest standard we can," Army General Keith Alexander, head of Cyber Command, told the Reuters Cybersecurity Summit last month. "And not just on defence, but on both sides. You've got to have that."

Officials and experts have warned for years that US computer networks are falling prey to espionage, intellectual property theft and disruption from nations such as China and Russia, as well as hackers and criminal groups. President Barack Obama will bring up allegations of Chinese hacking when he meets President Xi Jinping at a summit in California beginning on Friday - charges that Beijing has denied.

The Pentagon has accused China of using cyber espionage to modernize its military and a recent report said Chinese hackers had gained access to the designs of more than two dozen major US weapons systems in recent years. Earlier this year, US computer security company Mandiant said a secretive Chinese military unit was probably behind a series of hacking attacks that had stolen data from 100 US companies.

There is a growing fear that cyber threats will escalate from mainly espionage and disruptive activities to far more catastrophic attacks that destroy or severely degrade military systems, power grids, financial networks and air travel.

Now, the United States is redoubling its preparations to strike back if attacked, and is making cyber warfare an integral part of future military campaigns.

Experts and former officials say the United States is among the best - if not the best - in the world at penetrating adversaries' computer networks and, if necessary, inserting viruses or other digital weapons.

Washington might say it will only strike back if attacked, but other countries disagree, pointing to the "Stuxnet" virus. Developed jointly by the US government and Israel, current and former US officials told Reuters last year, Stuxnet was highly sophisticated and damaged nuclear enrichment centrifuges at Iran's Natanz facility.

NEW RULES OF ENGAGEMENT

US government officials frequently discuss America's cyber vulnerabilities in public. By contrast, details about US offensive cyberwarfare capabilities and operations are almost all classified.

Possible US offensive cyber attacks could range from invading other nations' command and control networks to disrupting military communications or air defences - or even putting up decoy radar screens on an enemy's computers to prevent US aircraft from being detected in its airspace.

The shift toward a greater reliance on offense is an important one for a nation which has mostly been cautious about wading into the uncertain arena of cyberwar - in part because gaps in US cybersecurity make it vulnerable to retaliation.

But former Homeland Security Secretary Michael Chertoff said the United States must be ready and should articulate - soon - what level of cyber aggression would be seen as an act of war, bringing a US response.

"One of the things the military learned, going back to 9/11, is whether you have a doctrine or not, if something really bad happens you're going to be ordered to do something," he told the Reuters summit. "So you better have the capability and the plan to execute."

Reuters has learned that new Pentagon rules of engagement, detailing what actions military commanders can take to defend against cyber attacks, have been finalized after a year of "hard core" debate. The classified rules await Defense Secretary Chuck Hagel's signature, a senior defense official said.

The official would not give details of the rules but said, "they will cover who has the authority to do specific actions if the nation is attacked."

'A FRAGILE CAPABILITY'

At Cyber Command, military officers in crisp uniforms mix with technical experts in T-shirts as the armed forces takes up the challenge of how to fend off cyber penetrations from individuals or rival countries.

Even as overall US defense spending gets chopped in President Barack Obama's proposed 2014 budget, cyber spending would grow by $800 million, to $4.7 billion while overall Pentagon spending is cut by $3.9 billion.

Until its new headquarters is ready, Cyber Command shares a home with the US National Security Agency (NSA), which for 60 years has used technological wizardry to crack foreign codes and eavesdrop on adversaries while blocking others from doing the same to the United States. Alexander heads both agencies.

"The greatest concentration of cyber power in this planet is at the intersection of the Baltimore-Washington Parkway and Maryland Route 32," said retired General Michael Hayden, a former CIA and NSA director, referring to NSA's Fort Meade location.

But NSA's role in helping protect civilian, government and private networks has been controversial - and is likely to come under greater scrutiny with this week's revelation that it has been collecting telephone records of millions of Verizon Communications customers under a secret court order.

A January report by the Pentagon's Defense Science Board gave a general picture of how the United States might exploit and then attack an adversary's computer systems.

In some cases, US intelligence might already have gained access for spying, the report said. From there, Cyber Command "may desire to develop an order of battle plan against that target" and would require deeper access, "down to the terminal or device level in order to support attack plans," it said.

Because gaining access to an enemy's computers for sustained periods without detection is not easy, "offensive cyber will always be a fragile capability," it said.

In cyberspace, reconnaissance of foreign networks is "almost always harder than the attack" itself because the challenging part is finding a way into a network and staying undetected, said Hayden, now with the Chertoff Group consulting firm.

PURPLE HAIR AND JEANS

Cyber Command's new Joint Operations Center, due to be complete in 2018, will pull disparate units together and house 650 personnel, officials said. Air Force, Army, Navy and Marine Corps components will be nearby and, a former US intelligence official said, the complex will have power and cooling to handle its massive computing needs.

Those who have worked at Cyber Command say the atmosphere is a mixture of intensity and geek-style creativity. Military precision is present, but it is not unusual to see young civilian computer whiz kids with purple hair, a tie-dyed shirt and blue jeans.

"It's made to be a fun environment for them. These are people who are invested and want to serve their nation. But there is some military rigor and structure around all that - like a wrapper," said Doug Steelman, who was director of Network Defense at Cyber Command until 2011 and is now Chief Information Security Officer at Dell SecureWorks.

Cyber Command's growth and expanding mission come with serious challenges and questions.

For example, how to prevent US military action in cyberspace from also damaging civilian facilities in the target country, such as a hospital that shares an electric grid or computer network with a military base?

And some doubt that the military can train many cyber warriors quickly enough. Alexander has identified that as his biggest challenge.

The former intelligence official said Cyber Command's new teams won't be fully ready until at least 2016 due to military bureaucracy and because it takes time to pull together people with the special skills needed.

"To be a good cyber warrior, you have to be thinking, 'How is the attacker discovering what I'm doing? How are they working around it?' ... Cyber security really is a cat and mouse game," said Raphael Mudge, a private

cybersecurity expert and Air Force reservist. "That kind of thinking can't be taught. It has to be nurtured. There are too few who can do that."

Would-be cyber warriors go through extensive training, which can take years. A recruit with proven aptitude will be sent to courses such as the Navy-led Joint Cyber Analysis Course in Pensacola, Florida, a 6-month intensive training program.

The top 10 percent of JCAC's students will be selected for advanced cyber operations training, said Greg Dixon, a vice president at private KEYW Corp, which conducts intensive training classes.

The company can train a JCAC graduate to become an analyst in five weeks, but it takes 20 weeks to become a cyber operator. Dixon would not divulge what an operator would be capable of doing after graduation, but said it would be "a lot."

"They're going to pick the cream of the crop for the 'full spectrum cyber missions'," the former US intelligence official said, using a euphemism for cyber offense.

Before a future cyber warrior can begin advanced training, he or she has to pass through the arduous security clearance process, which can take six to nine months for personnel who are not already cleared.

Troops earmarked for cyber warfare have found themselves washing floors, mowing lawns and painting at military installations as they bide time waiting for a clearance.

There is the concern about retaliation for a US cyber attack. Some analysts say Iran increased its cyber capabilities after being infected with Stuxnet, which was revealed in 2010.

"The old saying, he who lives in a glass house should be careful of throwing stones ... but if the stone that you threw at someone, when you live in a glass house, is a stone that in some way they could pick back up and throw back at you, that's an even dumber idea," the defense official said. "We definitely think about that as one aspect of considering action."

Table of Contents

Inside the NSA's Ultra-Secret China Hacking Group

By Matthew M. Aid, Foreign Policy, June 10, 2013

This weekend, U.S. President Barack Obama sat down for a series of meetings with China's newly appointed leader, Xi Jinping. We know that the two leaders spoke at length about the topic du jour -- cyber-espionage -- a subject that has long frustrated officials in Washington and is now front and center with the revelations of sweeping U.S. data mining. The media has focused at length on China's aggressive attempts to electronically steal U.S. military and commercial secrets, but Xi pushed back at the "shirt-sleeves" summit, noting that China, too, was the recipient of cyber-espionage. But what Obama probably neglected to mention is that he has his own hacker army, and it has burrowed its way deep, deep into China's networks.

When the agenda for the meeting at the Sunnylands estate outside Palm Springs, California, was agreed to several months ago, both parties agreed that it would be a nice opportunity for President Xi, who assumed his post in March, to discuss a wide range of security and economic issues of concern to both countries. According to diplomatic sources, the issue of cybersecurity was not one of the key topics to be discussed at the summit. Sino-American economic relations, climate change, and the growing threat posed by North Korea were supposed to dominate the discussions.

Then, two weeks ago, White House officials leaked to the press that Obama intended to raise privately with Xi the highly contentious issue of China's widespread use of computer hacking to steal U.S. government, military, and commercial secrets. According to a Chinese diplomat in Washington who spoke in confidence, Beijing was furious about the sudden elevation of cybersecurity and Chinese espionage on the meeting's agenda. According to a diplomatic source in Washington, the Chinese government was even angrier that the White House leaked the new agenda item to the press before Washington bothered to tell Beijing about it.

So the Chinese began to hit back. Senior Chinese officials have publicly accused the U.S. government of hypocrisy and have alleged that Washington is also actively engaged in cyber-espionage. When the latest allegation of Chinese cyber-espionage was leveled in late May in a front-page Washington Post article, which alleged that hackers employed by the Chinese military had stolen the blueprints of over three dozen American weapons systems, the Chinese government's top Internet official, Huang Chengqing, shot back that Beijing possessed "mountains of data" showing that the United States has engaged in widespread hacking designed to steal Chinese government secrets. This weekend's revelations about the National Security Agency's PRISM and Verizon metadata collection from a 29-year-old former CIA undercover operative named Edward J. Snowden, who is now living in Hong Kong, only add fuel to Beijing's position.

But Washington never publicly responded to Huang's allegation, and nobody in the U.S. media seems to have bothered to ask the White House if there is a modicum of truth to the Chinese charges.

It turns out that the Chinese government's allegations are essentially correct. According to a number of confidential sources, a highly secretive unit of the National Security Agency (NSA), the U.S. government's huge electronic eavesdropping organization, called the Office of Tailored Access Operations, or TAO, has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China.

Hidden away inside the massive NSA headquarters complex at Fort Meade, Maryland, in a large suite of offices segregated from the rest of the agency, TAO is a mystery to many NSA employees. Relatively few NSA officials have complete access to information about TAO because of the extraordinary sensitivity of its operations, and it requires a special security clearance to gain access to the unit's work spaces inside the NSA operations complex. The door leading to its ultramodern operations center is protected by armed guards, an imposing steel door that can only be entered by entering the correct six-digit code into a keypad, and a retinal scanner to ensure that only those individuals specially cleared for access get through the door.

According to former NSA officials interviewed for this article, TAO's mission is simple. It collects intelligence information on foreign targets by surreptitiously hacking into their computers and telecommunications systems, cracking passwords, compromising the computer security systems protecting the targeted computer, stealing the data stored on computer hard drives, and then copying all the messages and data traffic passing within the targeted email and text-messaging systems. The technical term of art used by NSA to describe these operations is computer network exploitation (CNE).

TAO is also responsible for developing the information that would allow the United States to destroy or damage foreign computer and telecommunications systems with a cyberattack if so directed by the president. The organization responsible for conducting such a cyberattack is U.S. Cyber Command (Cybercom), whose headquarters is located at Fort Meade and whose chief is the director of the NSA, Gen. Keith Alexander.

Commanded since April of this year by Robert Joyce, who formerly was the deputy director of the NSA's Information Assurance Directorate (responsible for protecting the U.S. government's communications and computer systems), TAO, sources say, is now the largest and arguably the most important component of the NSA's huge Signal Intelligence (SIGINT) Directorate, consisting of over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers.

The sanctum sanctorum of TAO is its ultramodern operations center at Fort Meade called the Remote Operations Center (ROC), which is where the unit's 600 or so military and civilian computer hackers (they themselves CNE operators) work in rotating shifts 24 hours a day, seven days a week.

These operators spend their days (or nights) searching the ether for computers systems and supporting telecommunications networks being utilized by, for example, foreign terrorists to pass messages to their members or sympathizers. Once these computers have been identified and located, the computer hackers working in the ROC break into the targeted computer systems electronically using special software designed by TAO's own corps of software designers and engineers specifically for this purpose, download the contents of the computers' hard drives, and place software implants or other devices called "buggies" inside the computers' operating systems, which allows TAO intercept operators at Fort Meade to continuously monitor the email and/or text-messaging traffic coming in and out of the computers or hand-held devices.

TAO's work would not be possible without the team of gifted computer scientists and software engineers belonging to the Data Network Technologies Branch, who develop the sophisticated computer software that allows the unit's operators to perform their intelligence collection mission. A separate unit within TAO called the Telecommunications Network Technologies Branch (TNT) develops the techniques that allow TAO's hackers to covertly gain access to targeted computer systems and telecommunications networks without being detected. Meanwhile, TAO's Mission Infrastructure Technologies Branch develops and builds the sensitive computer and telecommunications monitoring hardware and support infrastructure that keeps the effort up and running.

TAO even has its own small clandestine intelligence-gathering unit called the Access Technologies Operations Branch, which includes personnel seconded by the CIA and the FBI, who perform what are described as "off-net operations," which is a polite way of saying that they arrange for CIA agents to surreptitiously plant eavesdropping devices on computers and/or telecommunications systems overseas so that TAO's hackers can remotely access them from Fort Meade.

It is important to note that TAO is not supposed to work against domestic targets in the United States or its possessions. This is the responsibility of the FBI, which is the sole U.S. intelligence agency chartered for domestic telecommunications surveillance. But in light of information about wider NSA snooping, one has to prudently be concerned about whether TAO is able to perform its mission of collecting foreign intelligence without accessing communications originating in or transiting through the United States.

Since its creation in 1997, TAO has garnered a reputation for producing some of the best intelligence available to the U.S. intelligence community not only about China, but also on foreign terrorist groups, espionage activities being conducted against the United States by foreign governments, ballistic missile and weapons of mass destruction developments around the globe, and the latest political, military, and economic developments around the globe.

According to a former NSA official, by 2007 TAO's 600 intercept operators were secretly tapping into thousands of foreign computer systems and accessing password-protected computer hard drives and emails of targets around the world. As detailed in my 2009 history of NSA, The Secret Sentry, this highly classified intercept program, known at the time as Stumpcursor, proved to be critically important during the U.S. Army's 2007 "surge" in Iraq, where it was credited with single-handedly identifying and locating over 100 Iraqi and al Qaeda insurgent cells in and around Baghdad. That same year, sources report that TAO was given an award for producing particularly important intelligence information about whether Iran was trying to build an atomic bomb.

By the time Obama became president of the United States in January 2009, TAO had become something akin to the wunderkind of the U.S. intelligence community. "It's become an industry unto itself," a former NSA official said of TAO at the time. "They go places and get things that nobody else in the IC [intelligence community] can."

Given the nature and extraordinary political sensitivity of its work, it will come as no surprise that TAO has always been, and remains, extraordinarily publicity shy. Everything about TAO is classified top secret codeword, even within the hypersecretive NSA. Its name has appeared in print only a few times over the past decade, and the handful of reporters who have dared inquire about it have been politely but very firmly warned by senior U.S. intelligence officials not to describe its work for fear that it might compromise its ongoing efforts. According to a senior U.S. defense official who is familiar with TAO's work, "The agency believes that the less people know about them [TAO] the better."

The word among NSA officials is that if you want to get promoted or recognized, get a transfer to TAO as soon as you can. The current head of the NSA's SIGINT Directorate, Teresa Shea, 54, got her current job in large part because of the work she did as chief of TAO in the years after the 9/11 terrorist attacks, when the unit earned plaudits for its ability to collect extremely hard-to-come-by information during the latter part of George W. Bush's administration. We do not know what the information was, but sources suggest that it must have been pretty important to propel Shea to her position today. But according to a recently retired NSA official, TAO "is the place to be right now."

There's no question that TAO has continued to grow in size and importance since Obama took office in 2009, which is indicative of its outsized role. In recent years, TAO's collection operations have expanded from Fort Meade to some of the agency's most important listening posts in the United States. There are now mini-TAO units operating at the huge NSA SIGINT intercept and processing centers at NSA Hawaii at Wahiawa on the island of Oahu; NSA Georgia at Fort Gordon, Georgia; and NSA Texas at the Medina Annex outside San Antonio, Texas; and within the huge NSA listening post at Buckley Air Force Base outside Denver.

The problem is that TAO has become so large and produces so much valuable intelligence information that it has become virtually impossible to hide it anymore. The Chinese government is certainly aware of TAO's activities. The "mountains of data" statement by China's top Internet official, Huang Chengqing, is clearly an implied threat by Beijing to release this data. Thus it is unlikely that President Obama pressed President Xi too hard at the Sunnydale summit on the question of China's cyber-espionage activities. As any high-stakes poker player knows, you can only press your luck so far when the guy on the other side of the table knows what cards you have in your hand.

Table of Contents

Internet Gurus Fear Iranian Assassins

From Strategy page, 11 June 2013

June 11, 2013: For two years now Iran has been more energetically getting into Information War. This includes defense (a special Internet censorship unit) and offense (a Cyber War operation that is being detected more frequently on networks outside Iran). While the Cyber War attacks have the attention of

thousands of Internet specialists world-wide, fighting the censorship campaign against Iranian Internet users depends on volunteers, especially Iranians living abroad. There are actually thousands of these, often just informally helping family and friends back in Iran. But there are some volunteers who are extremely annoying for the Iranian censors. The Revolutionary Guard in Iran has made it clear that it is very angry with these expatriate Iranians, and there is some fear that they might resort to assassination to eliminate the most troublesome of these expatriate Internet experts. Such killings are rare these days. But from 1980 to the late 1990s Iranian assassins killed over 110 Iranian exiles who had been marked for death by the new religious dictatorship in Iran. International outrage forced the Iranians to back off, and that pushback turned into more and more sanctions against the religious fanatics running Iran. After September 11, 2001, it became even more difficult for Iran to carry out these murders because Western nations were more alert to the presence of Iranian killers and Iranian agents in general. But these killing still take place, or at least they are planned. In the last few years several assassination operations have been discovered and shut down before anyone got killed. But the Iranians are still trying.

The Iranian government is having more success at cutting most Iranians off from the Internet. The primary effort is building an internal Internet just for those in Iran who cannot be trusted with the World Wide Web. That means most Iranians are finding it more and more difficult to reach the international Internet. Late in 2012, Iran introduced a heavily censored local version of YouTube, as YouTube itself is banned in Iran. China is helping Iran, as well as a lot of other countries, to censor use of the Internet.

China is leading a worldwide tendency for police state governments to tightly control how their subjects use the Internet. While China is considered the most vigorous and effective censor of the Internet, many other nations are using the same techniques and equipment, often obtained from China. These include Cuba, Egypt, Iran, Myanmar, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, and Vietnam. None of these nations are democracies. All are police states or monarchies determined to keep their subjects from having free use of the Internet. In most cases, the real purpose is to prevent the people from overthrowing the rulers. But there are many other nations, most of them democracies, who are also striving to control the Internet to protect their citizens from unsavory material. These nations include Australia, Bahrain, Belarus, Eritrea, Malaysia, Russia, South Korea, Sri Lanka, Thailand, Turkey, and the United Arab Emirates. Most other nations are watching these efforts, as there are many people on the planet who see the Internet as more of a threat than an opportunity.

China leads the way in all this. But it isn't all about politics. Iran, for example, wants to block its citizens from seeing pornography, anything critical of Islam, and most Western entertainment. China, has made a major effort to "protect" adult Internet users from pornography and children on the Internet from, well, everything. The government does this via its Great Firewall of China (officially the "Golden Shield") system, that filters, and eavesdrops on, Internet traffic coming into, and leaving, China. In fact, Golden Shield is more about controlling what is said by Internet users inside China than in controlling what they have access to outside China.

The growing number of governments seeking to control Internet content is all concerned about how they have lost control of information flow because of the Internet. This control is a matter of life and death for a dictatorship but can be very annoying for leaders (honest or otherwise) in a democracy. No leader (elected or not) likes to have contrary opinions popping up. Something must be done.

Iran, like North Korea, is trying to create its own Internet and prevent most Iranians from having any access with the international Internet. This is only possible if your economy is not highly dependent on worldwide Internet access. That is the case in North Korea, but Iran has an economy that deals a lot with foreign suppliers and customers. That is changing, because of the growing list of international economic sanctions placed on Iran because of their nuclear weapons program and support for terrorism. Iran also wants more control over Internet use inside Iran because it fears that foreign spies, saboteurs, and assassins are using it to collect information about targets and to carry out operations.

Table of Contents

NSA's Keith Alexander Seeks Cyber Shield For Companies

By Tony Romm, Politico, June 16, 2013

Even as he defends controversial government surveillance programs, the head of the National Security Agency is asking Congress for another authority sure to inflame critics — legal immunity for companies that help the feds fight cyberattackers.

Gen. Keith Alexander has petitioned Capitol Hill for months to give Internet service providers and other firms new cover from lawsuits when they rely on government data to thwart emerging cyberthreats.

That may be a powerful perk to persuade companies to work with Washington toward bolstering the country's digital defenses. But it's also a source of alarm for some civil liberties advocates, who are already peeved with the NSA's vast electronic spying regime. Those critics' new fear: Companies acting with the government's blessing in cyberspace could skirt legal accountability if they hit the wrong target.

"If the government asks the company to do something to protect the networks, or to do something and a mistake is made, and it was our fault, then they should have liability protection for that," Alexander told a Senate committee Wednesday.

Digital countermeasures in theory can encompass everything from the benign blocking of suspicious IP addresses to more aggressive and eye-opening efforts to poison hackers' home bases. Done effectively, these tactics can help companies stop attacks or remove spies from their networks. But there's always risk: Bad intelligence could lead a company to block legitimate Web traffic, for example, or perhaps kick perfectly legal Internet users offline. The most aggressive countermeasures — like actively hacking back a known hacker — are banned under current U.S. law.

As Congress rethinks the private sector's powers to defend itself, however, lawmakers have struggled to provide a clear definition as to what companies can do and what legal protections they should receive. Exactly what the Obama administration seeks isn't clear either. Alexander, for his part, has never revealed the full set of tools he believes companies should have at their disposal when acting on government intelligence. The NSA declined further comment — as did the Pentagon, where the general also leads U.S. Cyber Command.

A White House official speaking anonymously to POLITICO said the administration could support a change to law that allows companies to take some defensive countermeasures in cyberspace, with narrow legal protections and strong oversight. But the official said the White House hasn't put forward its own definition of what qualifies as a "defensive countermeasure" because it's not writing legislation.

In a separate statement, an administration spokeswoman stressed the need for limits on legal immunity given to companies that take "defensive action" based on "specific, tailored cyberthreat information" from the government that turns out to be faulty.

Most of official Washington is focused on the NSA now because of its broad phone record collection program and its Internet surveillance effort known as PRISM. Amid that controversy, lawmakers are engaged in a long-standing debate over how the government and private companies can work together to identify and defeat foreign hackers and spies.

Many members of Congress agree there's need for the public and private sectors to exchange more intel about emerging cyberthreats. There's division, though, as to how companies should defend their own networks — and the sort of legal protections the government should afford private businesses that assist in the cybersecurity cause.

Companies, for their part, want to be shielded from as many lawsuits as possible, especially if they're on the front lines. And the government, in the past, has granted such immunity in the realm of surveillance — like when Congress during the Bush era shielded telecoms from lawsuits as they assisted the NSA's warrantless wiretapping program.

When it comes to cyber countermeasures, sources say Alexander has long been a proponent of a more aggressive approach.

One former White House aide told POLITICO that Alexander has been asking members of Congress for some time to adopt bill language on countermeasures that's "as ill-defined as possible" — with the goal of giving the Pentagon great flexibility in taking action alongside Internet providers. Telecom companies, the former aide said, also have been asking Alexander for those very legal protections.

While Alexander hasn't been very specific in his public comments, he's dropped some clues about his thinking on companies that act as "agents of the government," as he explained at an April hearing of the Senate Armed Services Committee.

"We send a signature [to a company] that says, stop this piece of traffic," Alexander told lawmakers at the time. But if the government were to "mischaracterize" the threat, leading an Internet provider to have "stopped some traffic they didn't intend to," Alexander said, "in that venue we've got to give [companies] immunity."

The general quickly added he was "not talking about giving them broad, general immunity, and I don't think anyone is."

Alexander initially promised in April to provide one committee member, Sen. Bill Nelson (D-Fla.), a more complete explanation of his thinking, but the NSA declined to make that document available, and the senator's office did not comment to POLITICO.

The lack of clarity has irked civil liberties advocates still peeved about the NSA's alleged overreach in cyberspace. Given the "recent revelations about the NSA's surveillance activities that seem to go well beyond its statutory authorities, I think any authorization to enlist companies in related activities … is going to have a lot of people up in arms," said Greg Nojeim, senior counsel at the Center for Democracy and Technology.

As the debate proceeds, the NSA does have some receptive allies on Capitol Hill. Chief among them may be Sen. Dianne Feinstein (D-Calif.), the leader of the chamber's Intelligence Committee and co-author of a forthcoming bill on cybersecurity information sharing.

It was Feinstein who asked Alexander about liability protection at a high-octane Wednesday appropriations hearing. She began her question by noting lawmakers have consulted with the NSA leader on lawsuit immunity and countermeasures.

Feinstein's office declined comment for this story. The senator backed limited defensive countermeasures in her previous 2012 cybersecurity bill. Companies deploying them would not have gained full liability protections but could have made a good-faith defense in court.

This year, though, there's new chatter about codifying the government's role working with private companies against cyberthreats. New legislation could grant the government some ability to approve or recommend the use of countermeasures, according to a congressional aide familiar with the discussions. And that could come with stronger liability protections, too, the source indicated.

Meanwhile, Feinstein's counterpart on the Senate Intelligence Committee — ranking Republican Sen. Saxby Chambliss of Georgia — also told POLITICO there's still appetite for the idea.

"Providing the private sector with full liability protection from frivolous lawsuits for all information sharing and for the use of certain countermeasures is essential to encouraging better cybersecurity, both within the private sector and the federal government," he said in a statement. "Any bill we pass must contain these vital protections."

His office cautioned, though, that it's only "defensive countermeasures" that lawmakers have in mind — but he declined to offer specifics.

The concept, if it advances in Congress, could spark heated argument if history is any guide.

A major Senate cybersecurity bill that reached the chamber floor last year specified companies could only act with defensive interests in mind. It still failed to assuage the concerns of critics, who felt the language may have permitted Internet providers to snoop on their users and take significant action without any legal penalty for wrongdoing. Sen. Al Franken (D-Minn.) at the time led an effort to delete the offending section, though the bill never became law. Similar complaints dogged a House-passed bill that at one point earned the president's veto threat.

As the debate returns, privacy hawks and civil liberties advocates promise to press the issue. There might be a way to balance competing security and privacy interests, explained Michelle Richardson, legislative counsel at the American Civil Liberties Union — but she emphasized it would come down to specifics.

"You don't want to give too much protection so companies are acting recklessly and causing all sorts of collateral damages or unintended consequences," she said.

Table of Contents

Killing with Kindness: How Foreign Aid Backfires

By Malou Innocent, US News, June 10, 2013

Whether Washington calls it capacity building, counter-insurgency, short-term emergency relief or long-term foreign assistance, its multi-decade mission to bring economic development to faraway lands often falls short of achieving its desired outcomes. At the Cato Institute last Wednesday, George Mason University Economics Professor Christopher J. Coyne explained why, presenting the central arguments of his new book, "Doing Bad by Doing Good: Why Humanitarian Action Fails."

As summarized in this Cato Daily Podcast, Coyne argues that even though coercive and non-coercive forms of state-led humanitarian action can alleviate short-term human suffering, it cannot replicate individual instances of success systematically. Challenging those arguments was Dr. M. Peter McPherson, president of the Association of Public and Land-grant Universities.

Their discussion proved informative, contentious and was overall well-received, but left under-explored one of the book's key conclusions, specifically about the allocation of aid – that is, political competition among entrenched bureaucracies typically trumps the selfless moral imperative to help those in need. Humanitarian efforts typically flop because of vested interests, perverse incentives and clashing missions.

Similar problems hamstrung a major food aid initiative in Vietnam, as retired Foreign Service Officer Jaime L. Manzano shared with me and Coyne after the book forum:

> U.S. agricultural surpluses available under PL 480 [the law that created the Office of Food for Peace] can be granted or sold in less developed countries to generate local currencies. These funds are used to cover budgets in recipient countries and meet U.S. agency needs to cover local budgetary expenditures that their operations require.
>
> In the early 60's, the U.S. Mission in Vietnam requested PL 480 to ship rice to the country. The rice was to be sold in the Saigon market for local currencies and then used to pay for the training and salaries of South Vietnamese soldiers.
>
> Vietnam was a rice exporting country. It had no shortage of the commodity. But the country team argued that the cost of rice was high, and that it needed local currency to pursue the war.
>
> A review of the program showed that local rice was indeed available, and that should PL 480 rice be sent to Saigon, prices would plummet. Rice producers, the small farmers in rural areas where the war was being fought, would become disaffected from the government of Saigon and have reason to ally themselves with the insurgents. The direction of trade would shift toward the Cambodian market, with insurgents functioning as middlemen. Such a change would run counter to the purposes of the U.S. presence in Vietnam.
>
> The PL 480 review team, composed of the AID Vietnam desk officer and the AID Far East program officer, participated in the preparation of a position paper that was vetted through the Department of State, the Pentagon and the Department of Agriculture. State sat on the fence, Pentagon strongly supported the country team and USDA pushed to get rice out of its silos.
>
> The AID PL 480 team continued to point out that the use of rice undermined the reasons for America's presence in the region. Firstly, it pointed out that if the U.S. continued to bend to the needs of the government of Saigon, the war in Vietnam would become one for which the U.S. would become responsible and not the South Vietnamese government. Secondly, because the rice would alienate the rural constituency in South Vietnam, the U.S. would be losing the hearts and minds of the Vietnamese people who were precisely the ones we wanted to wean away from the insurgents.
>
> The issue went up to the White House. Politics worked its wondrous ways and the rice to Vietnam was approved. Those who argued against the shipments were accused of "disloyalty" to the administration. Within months, those who had the temerity to question the country team were transferred to other posts.
>
> I was one of them.

That anecdote exemplifies the incentives created by political institutions, regardless of the conflict.In his 2012 book, "Little America: The War Within the War for Afghanistan," Washington Post Senior Correspondent Rajiv Chandrasekaran uncovered similar inter-agency turf battles that harmed diplomatic efforts to end America's longest war.

Despite rhetoric about "lessons learned," development experts and policymakers seemingly fail to fully grasp that political competition is immutable to bureaucracies. Coyne explains that agencies and departments, focused on their own discretionary budgets and discrete visions of success, continually jockey to influence policy and advance their narrow self-interest. Citing fellow economists Gordon Tullock and the late William A. Niskanen, "Doing Bad by Doing Good" knocks down the popular view that policies always serve a higher benevolent purpose. Among his many conclusions, Coyne argues that competition, much like waste, corruption and other factors that good intentions can never eliminate, "is a logical outcome of the industrial organization of government bureaucracies."

Table of Contents

Cyber Careers New Center, School to Bring Signals, Cyber, EW Together

By Joe Gould Army Times, July 1, 2013

Army Chief of Staff Gen. Ray Odierno has approved a new cyber school for soldiers to consolidate training of the Army's growing cyber force in one location at Fort Gordon, Ga., the first step in what could be a significant reorganization of soldiers with connections to cyberspace operations.

The new Cyber Center of Excellence will incorporate the Signals Center of Excellence and unify training and modernization efforts for cyberspace operations, electronic warfare, cyber electromagnetic activity and cyber-related signals intelligence, Army officials said.

Training and Doctrine Command commander Gen. Robert W. Cone has publicly called for the cyber school and also for a cyber career field, and plans to create the latter are underway.

Officials say the new career field for officers, enlisted soldiers, warrant officers and civilians has the potential to absorb certain cyber, intelligence and signals soldiers from other branches because of their cyber skills.

The school would unify and integrate training for disciplines that cover computer hacking, jamming and eavesdropping on electromagnetic signals, which the Army considers separate but related.

"From a war-fighter perspective, whether you're signal or intel, this gives the cyber workforce a new sense of futuristic identity and of the increased importance of their role in warfare," said Col. Michael A. Marti, the chief of mission command, intelligence and cyber at the Army Capabilities Integration Center, TRADOC, Fort Eustis, Va.

"Because we will blend these very nuanced technical skills, it will make them an elite capability."

The plans, which were awaiting the ultimate approval of Army Secretary John McHugh as of June 21, have not been publicly announced. However, military and civilian sources close to the effort say McHugh is expected to affirm Odierno's decision.

"This is the boldest and most forward-looking thing I've seen the Army do," said Jeff Moulton, a senior cyber researcher with the Georgia Tech Research Institute who works with the government. "Putting cyber, [signals intelligence] and EW together is a big deal."

The school would merge the Army's force modernization proponent for cyber space operations and electronic warfare "to achieve unity of effort for capability development, integration and the force modernization process," according to TRADOC's June 4 order to establish the school.

The cyber school would remove some conceptual barriers to create a "nuanced blending" of signals intelligence, electronic warfare and cyber electromagnetic activity skills, which the Cyber CoE will "fully integrate" for cyberspace operations, Marti said.

Odierno on May 31 approved the strategy and schedule to create the cyber school. TRADOC would transition the signals school at Fort Gordon into the cyber school in a process that begins Aug. 1and must be complete by Oct. 1, 2015.

The school's name and some command relationships related to the new school are set to change in August, but the related organizations and personnel will not physically move, at least at first. Fort Gordon is expected to build facilities to accommodate the physical moves over the next two years, according to sources close to the effort.

The school will assume command of the force modernization proponent for cyberspace operations and electronic warfare, which today are held respectively by Army Cyber Command, Fort Meade, Md., and the Combined Arms Center, Fort Leavenworth, Kan. Force modernization proponents determine future capabilities, development efforts and requirements for doctrine, organizations, training, materiel, leadership, personnel and facilities.

The organization would achieve initial operating capability through "matrixed relationships," Marti said.

"On 1 Aug., the Army cyber proponent folks at Fort Meade will take off their Army Cyber patch and put on a TRADOC patch and start reporting to the newly established Cyber Center of Excellence at Fort Gordon, Ga.," he said. "The same goes for the EW folks; they'd stay working at Leavenworth, and their school is at Fort Sill, [Okla.] at the Fires Center of Excellence."

At initial operating capacity, the Cyber CoE would oversee a signals school and provisional cyber school.

The school's signals capability development integration directorate, or CDID, will become a cyber CDID. The organization's job will be to envision the future operating environment and future scenarios and plan how future concepts and capabilities should be developed over time to meet that future. At least for now, EW and cyber will have separate capabilities managers under the CDID.

"As opposed to the signaleers deciding how do we create a network for our soldiers to talk on, now that CDID will have to expand that thinking to how do we [operate] related to cyber, electronic warfare and cyber-electromagnetic activities," Marti said. "If I'm a signaleer or an intel professional working in a job related to cyber, I'd see this as a tremendous step forward."

A TRADOC analysis, now underway, will determine which signals jobs are distinct from cyber, Marti said. Those jobs would receive related training at the signals school within the Cyber Center of Excellence, when it is fully operational in 2015.

Discussions are underway in Congress about whether Army Cyber Command, split between Fort Meade and Fort Belvoir, Va., would eventually move to Fort Gordon, one source said. The move would take Army Cyber Command from near National Security Agency headquarters to NSA's facility at Fort Gordon.

The plan for the school raises other questions about future mergers and moves for cyber, signals intelligence and electronic warfare personnel and organizations. The Army is moving quickly to transition the school at Fort Gordon, but other potential changes require more deliberation.

"This initial step institutionally will open up other possible changes organizationally, but we will be in the build, test, assess and refine mode on this Cyber Center of Excellence at least for the next 24 months," Marti said.

Gen. Keith B. Alexander, the chief of U.S. Cyber Command and the NSA, in a recent speech called for a merger of signals and military intelligence troops who respectively perform defensive and offensive cyber operations. Cyber CoE officials are expected to re-examine how the Army conducts offensive and defensive operations and clarify the chains of responsibility for cyber operations.

"The institutional change we're making will be the vanguard for other operational changes," Marti said.

How far the Army plans to draw the border of the possible cyber career field, and what related organizational changes may result, is to be decided by senior Army leaders in the coming months, according to three sources. Marti acknowledged that officials at Army Cyber and the Army staff are conducting an internal study to determine the form a cyber career field could take.

Marti said officials want to move quickly, which Odierno has prodded them to do. But they also want to ensure the Army's workforce best serves the needs of the service, as well as the joint U.S. Cyber Command. "This management model has to be informed by all of those echelons, which is why Gen. Alexander's vision is so important," Marti said.

Some institutional resistance is said to remain because of the potential redistribution of personnel and authorities.

"People have been saying for years there should be a cyber career specialty, but the MI and signal folks have been saying, 'No, we don't need that; we're doing fine,' " a civilian source told Army Times. "When they stood up the Rangers and Deltas, the people most opposed to it [were] the infantry because they're going to take the cream of the crop. It's a zero-sum game."

Not so, according to Marti.

"From the time we took lead on this, everyone has come to the plate and played ball, and it's been liberating and invigorating to watch," he said.

One of the largest unanswered questions is what this all means for the 29-series career field for electronic warfare officers, warrant officers and enlisted personnel - a field that is four years old - particularly, whether it will be subsumed into a cyber career field.

The cadre's creation came with a storm of internal debate over the relationship between electronic warfare and cyber, and in doctrine, the two are considered separate but related.

"Those stances have changed, but senior Army leaders are saying, 'Over your objections, we're going to do it,' " one civilian source said. "There are valid issues, but it doesn't mean they can't be worked through."

According to Marti, it's too soon to say what will happen to the 29 series, though he said it is "feasible" that signals intelligence and electronic warfare skill sets could come together under a single cyber career field.

The chief of the Army's electronic warfare directorate, Col. Jim Ekvall, told Army Times he considers cyberspace operations and electromagnetic warfare as "separate and distinct from one another." He acknowledged the two have a symbiotic relationship and are becoming more closely aligned, but likened the two to infantrymen and field artillerymen, who conduct synchronized operations but make up separate branches.

Even if the cyber and electronic warfare specialists aren't the same people, they will at least be working together in fights, Ekvall said. A maneuver commander might one day have access to a cyber-electromagnetic operations cell on an as-needed basis or as part of the force structure.

Within that cell, an EW officer, for instance, would be responsible for synchronizing and integrating all cyber-electromagnetic activities into the maneuver commander's plan.

At present, units do not have resident cyber experts, so commanders rely on EW, signals and intelligence officers who each may have some expertise on the matter and will come together and work, Ekvall said.

"The Army's got to make a decision about whether there's a requirement for... a corps of cyberspace operators, just like there are electronic warfare operators," Ekvall said. "The Army has to do the requisite analysis for how they're going to man, train and equip a cyber force - if they are going to man, train and equip a cyber force."

Table of Contents

"Electronic Warfare is Becoming More Important and More Complex"

By Amir Rapaport, Israel Defense, 13/6/2013

"In the past, you purchased an electronic protection system and installed it onboard the aircraft in order to provide the pilot with alerts pertaining to various threats. Today, electronic warfare resources are a part of the over-all protective suit of the aircraft and are also a part of its weapon systems. They are no longer a stand-alone element – and that has been a quantum leap."

The speaker is Edgar Maimon, the CEO of Elisra, a member of the Elbit Systems Group, regarded as Israel's electronic warfare (EW) house and one of the world's leaders in the field of EW. In a first-ever interview, Maimon tells IsraelDefense about the revolution taking place within the field of electronic warfare and about a few surprising directions that the company, intends to take under his direction.

An IAF Man

Maimon was appointed to head Elisra about a year ago, having replaced Brig. Gen. (Res.) Itschak Gat (who will be appointed to the position of chairman of the board of Rafael this summer). Like many other top executives of the Israeli defense industry, Edgar Maimon had had a long career in the IDF. As an electronics engineer he started out in relatively junior positions in the electronic warfare layout of the IAF. Before his discharge, in 2003, he was responsible for the IAF's major aircraft procurement deals and had served as head of the Systems and C4I Branch at the rank of colonel.

Maimon joined Elisra immediately after the conclusion of his IDF service, and went through several incarnations with the company: ten years ago, Elisra, originally established as a private initiative in 1966, was still a part of the Koor concern, whose leadership had decided to pull out of all of the defense holdings it had.

30% of Elisra's stock were sold during the last decade to IAI, and the remaining 70% were sold to Elbit Systems. About two years ago, Elbit Systems purchased IAI's share for $60 million, thereby gaining complete control over the company.

Elisra is involved in all of the activities and derivatives of the realm of electromagnetic warfare. Although its name is synonymous, first and foremost, with electronic warfare, CEO Maimon says that "Elisra belongs not just in the EW world. It is, in fact, a Company that specializes in information warfare, EW, intelligence and C2. Elisra's vision is derived from our mission and uniqueness, according to which we provide system-wide, complete solutions in these worlds. We aspire to be world leaders, and when I examine our accomplishments in the context of some of those elements, notably electronic warfare, we are, indeed, the leaders. As far as the other elements are concerned – we are on our way to the top."

Global competition is not a trivial matter?

"18 companies around the world are engaged in electronic warfare, and almost none of these companies are engaged in this field exclusively. Most of the EW companies were acquired over time by larger corporations – just like we were acquired by Elbit Systems. Today, we are leading the field along with such US companies as Northrop Grumman and ITT. If the US market had opened for fair competition to Elisra, we would have occupied an entirely different position today, as technology-wise, we are far ahead of other companies, and that is why I am speaking about a global leadership status. We compete in the world's markets with the best companies, and we often win."

Elisra's sales turnover is estimated at more than a quarter of a billion US dollars each year. Among the contracts the company won in the last year was the installation of EW systems on aircraft in Brazil (at a scope of $90 million, as part of a joint project of Elbit Systems and the Brazilian company Embraer).

Elisra has recently won a huge project in Asia, worth $115 million, and is currently developing new generations of EW systems for the Israeli Navy. It is also developing a new system for dealing with IEODs for the IDF - an upgrade of Elisra's EJAB IEOD protection system, known in the IDF as "Shalgon", which jams frequencies used for wireless charge activation, until the convoy being protected has passed).

An EW Superpower

For many years, Israel has been regarded as an EW superpower, first and foremost in the aerial field. During the First Lebanon War in 1982, IAF fighters recorded an amazing kill ratio of 81 to 0 vis-à-vis the Syrian Air

Force. Much of that achievement was attributed to electronic countermeasures which provided the IAF fighters with an effective protective suit. IAF has always insisted on electronic protective suits made in Israel that would provide it with a qualitative edge on the aerial battlefield, where Arab countries, including Saudi Arabia and Egypt, possess identical US-made fighters like F-15 and F-16. Even the future fighter F-35, which is to be delivered to Israel, will include EW protective components by Elisra.

Air-to-air combat encounters are a thing of the past, owing, to a considerable extent, to the total air superiority of IAF. Electronic warfare enables the IAF fighters to effectively cope with the enemy's surface-to-air missile batteries as well – first and foremost by identifying them and disrupting their operation. According to foreign sources, while the IAF was attacking the Syrian nuclear reactor at Deir-Ez-Zour in September 2007, the Syrian air defense batteries were completely unaware of the presence of IAF aircraft over Syrian territory. This was probably because of the use of a series of electronic countermeasures and cyber warfare resources. The IAF is presumably preparing to employ electronic countermeasures against the state-of-the-art SAM batteries Syria has acquired from Russia in recent years, SA-17 and SA-300.

"The importance of electronic warfare has increased tenfold," adds Edgar Maimon. "The technological development in this field has been considerable. In the old systems, pilot alerts and electronic jamming were two distinct and separate functions - the issue of assembling a joint picture of the combat zone was considerably complex. Each system had a certain reception capability with different accuracy rates. Today, the systems are unified and integrated, and when everything operates out of a central, single location you can achieve much higher capabilities within the same box, with regard to detection as well as with regard to the active response."

Do you mean that EW systems are currently used for the offensive element, not just for protection?

"Yes. When the same weapon system provides alerts and jamming and even ELINT (Electronic Intelligence, based on the analysis of electronic signals) with precise locating (capabilities), you have done you part. That is where the world is heading. The smart thing is keeping ahead of the others, and in some areas we are the trailblazers.

"In EW, the main idea in the past was diverting the missile away from the aircraft. Today, everything is so sophisticated, that from an F-16 fighter aircraft you are able not just to divert the incoming missile, but to launch your own missile at the battery that had fired at you.

"This goes beyond the individual aircraft," continues Maimon. "If you fuse the data arriving at the same time from a hundred different aircraft, you will be able to get an accurate documentation of the targets. From this point, launching a missile of one type or another at the target will be very simple. In this respect, the fact that we have been cooperating with IAF for decades offers a major advantage. If you examine a US F-15 fighter, you will find parts of protective suits by different manufacturers, and fusing between them will be much more difficult.

"In the case of the IAF, there are systems by Elisra on each and every aircraft, and that is an excellent foundation for data fusion."

Flagship Products

10 to 15 years ago, Elisra invested heavily in the development of solutions in the IR frequency band. Today, the company is reaping the rewards of its investment, as one of the leaders in this field.

According to Edgar Maimon, Elisra sells complete protective solutions and not just protective systems, and incorporates in its solutions products by its sister companies in the Elbit Systems Group, such as sensors by Elop. Reciprocally, Elisra's detection systems are incorporated in Elop's Music system – a system developed by Elop to provide aircraft with effective protection against man-portable SAMs.

The classic aircraft protection system Elisra offers is designated V5.

One of the company's flagship products in the airborne systems category is the system known as PAWS (Passive Approach Warning System). This system consists of various sensors located in various boxes onboard the aircraft. The smart thing about this system is the processor, which receives data from the various sensors and uses the data to assemble a complete picture.

"We have switched to integrated systems, and we are consolidating this approach of a single, small and compact system capable of detecting, identifying and handling the threat. We have sort of taken the world by storm with these systems," claims Edgar Maimon.

The Land

"One of the major advantages is that the realm of ELINT evolved out of the realm of aerial EW," adds Maimon. "This compelled us to focus on miniaturized systems that accomplish a lot. Now, these miniaturized systems provide us with substantial operational capabilities when they are mounted on land platforms, too."

Maimon says that Elisra made a strategic decision to enter the field of land-based radars about three years ago. In the context of this initiative, Elisra acquired a Hungarian company, PPE, whose core product was a personnel surveillance radar system. Elisra presented that radar in the Elbit pavilion at the 2012 Eurosatory exhibition in Paris, and is currently upgrading the original radar design.

Elisra has been involved in the realm of soft-kill protection for air, naval and land platforms for decades, but Edgar Maimon has revealed here, for the first time, that the company decided to become involved in the development of threat detecting radars for vehicles, for the purpose of providing hard kill (namely active) protection, like the radars in Rafael'sTrophy and IMI's Iron Fist active protection systems. The radar of Rafael's active protection system is currently produced by IAI's Elta division, while the radar of IMI's active protection system is produced by Rada, and it would appear that the Elbit Systems Group is about to enter the competition in this field.

Table of Contents

Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda

By Nico Prucha and Ali Fisher, CTC Sentinel, Jun 25, 2013

Almost all forms of online media allow, enable and empower users to generate their own content and interact by posting comments, questions or responses. Online media platforms facilitate a blend of audiovisual media interspersed with writings that further sanction and explain specific ideological dimensions of jihadist activity.[1] As the range of online platforms has expanded, jihadist groups have increasingly used sites such as Twitter,[2] Facebook, YouTube,[3] and Tumblr.[4] The role of the "media mujahidin" has been approved,[5] sanctioned[6] and encouraged with the release of suggested strategies,[7] although not all jihadists have perceived the move away from the traditional discussion forum websites as positive.[8]

The classical jihadist discussion forums remain the vital hub for authoritative and cohesive propaganda online.[9] The importance given to Twitter by jihadist groups, however, was highlighted in the 11th issue of Inspire magazine, which was released by al-Qa`ida in the Arabian Peninsula (AQAP) in May 2013.[10] Indeed, within the complex network of interconnecting sites, Twitter has become the main hub for the active dissemination of links guiding users to digital content hosted on a range of websites, social media platforms, and discussion forums.

This article discusses the emergence of jihadist social media strategies, explains how the Syrian jihadist group Jabhat al-Nusra (JN) has used Twitter to disseminate content, and analyzes content shared by JN. Using an interdisciplinary approach to the analysis of jihadist propaganda, this article demonstrates how jihadist groups are using Twitter to disseminate links to video content shot on the battlefield in Syria and posted for mass consumption on YouTube. Data for this article is derived from analysis based on more than 76,000 tweets, containing more than 34,000 links to web-based content. Through the mining of this data, this article identifies a content sharing network of more than 20,000 active Twitter accounts and a collection of YouTube video files that have been viewed nearly 450,000 times.[11]

Twitter: The New Beacon for Jihadist Activity Online

Recent martyr biographies reveal that the growth in social media use has led to a new generation of jihadists. These jihadists decided to engage in physical violence after being active within the virtual dominions of al-Qa`ida where exposure to the media had an impact on their personal lives and understanding of religious conduct.[12] This trend reflects to a great extent a specific zeitgeist, a contemporary as well as generational shift from texts and scripts to a "visual literacy." Ideology is presented by iconographic, habitual, and rhetorical means. Elements shown in jihadist videos are thus most appealing to initiated consumers who can read and identify the greater ideology at work.[13] The most prominent visual element is the use and role of the specific black banner crafted by the Islamic State of Iraq, which today is the most credible identity marker for pro-al-Qa`ida jihadist groups.[14]

The main al-Qa`ida forums have adopted this trend and are active on Twitter, promoting their official Twitter accounts on the main jihadist web forum pages.[15] Jihadist media activists and fighters on the ground use Twitter on a regular basis to upload their personal pictures and videos that were made with their cell phone cameras. This material enters the jihadist online sphere where it is immediately used and re-used to strengthen the worldview of al-Qa`ida and affiliated groups. As a result, new communication channels have emerged through which the new generation of activists and fighters, including those working for, or on behalf of, al-Qa`ida in the Islamic Maghreb (AQIM), AQAP, al-Shabab, and JN, can interact with potential influence multipliers and sympathizers.

Groups such as the Somalia-based al-Shabab rely on Twitter to publish pictures, statements, and links to YouTube jihadist videos primarily in Arabic and English. Al-Shabab used Twitter to update their followers regarding the failed French operation to free Denis Allex, who had been taken hostage by the group in 2009.[16] Pictures of an alleged dead French soldier and his gear were posted on Twitter and Facebook,[17] with the al-Shabab Twitter account (@HSMPress) claiming that they executed one of the French hostages in revenge for the raid.[18]

The Afghan Taliban (@ABalkhi), AQIM's media department al-Andalus (@Andalus_Media), and the Islamic State of Iraq's (AQI) al-Furqan media branch (@abo_al_hassan[19]) all have Twitter accounts and frequently publish and disseminate new and old content. AQAP, for example, recently resorted to using Twitter to link to official statements.[20]

These "official" media channels facilitate active communication with sympathizers and followers on Twitter. For example, an official al-Qa`ida user on jihadist web forums advertised for AQIM's al-Andalus Media's Twitter account.[21] Four days later, on April 1, 2013, an "open interview" was announced via the forums with "Shaykh Ahmad Abu `Abd al-Ilaha, the head of the Media Board for al-Andalus," setting a time window for individuals to ask him questions on Twitter using the al-Andalus account.[22] On April 18, the Twitter account posted a link to a PDF document containing all of the shaykh's answers to the questions.[23]

The use of twitter by jihadist media activists was further highlighted by the "AQTweets" section in the recent edition of AQAP's English-language Inspire magazine, which highlighted tweets about the Boston bombings of April 2013.[24]

Jabhat al-Nusra on Twitter

Following the outbreak of fighting in Syria, Syrian non-violent activists used, and continue to use, Twitter as a medium to document human rights abuses and war crimes committed by the Bashar al-Assad regime. Jihadists, however, soon adapted that content and the platform for their own propaganda purposes. By rebranding and reframing the content created by civil society activists, jihadists used these grievances to support a key jihadist theme: the obligation to defend and protect the Sunni population in Syria.

The primary jihadist rebel group in Syria, which maintains active links to al-Qa`ida, is JN. Although JN's official Twitter account, @jbhatalnusra, has been quiet since April 10, 2013, there has been a steady increase in their followers.[25] In addition to collecting and analyzing tweets posted by @jbhatalnusra, the authors also identified and analyzed influential users,[26] the most shared links and the content to which those links directed users. A total of 76,000 tweets containing JN related content were captured over 50 days from January 27, 2013, to March 18, 2013.

JN disseminates content using the hashtag #جبهة_النصرة, the original short version of the name in Arabic for which the group has become known. Through an analysis of the tweets containing the Arabic hashtag for Jabhat al-Nusra, the network of users sharing content via Twitter was identified.[27] The following is a list of users who frequently tweeted using the #جبهة_النصرة hashtag during the 50-day period: @Nasser1437: 1,257 tweets; @zhoof21: 593 tweets; @al_khansaa2: 363 tweets; @qmzp1434: 359 tweets; @alshohdaa: 300 tweets; @az_241: 287 tweets; @Jalaaad_alshi3a: 265 tweets; @SaifAlbayan: 254 tweets; @shame210: 230 tweets; @ROOH_GNAN: 223 tweets.

Active users are defined as those who share a lot of content, but it does not indicate whether other users read or followed their content. To determine whether a user can be considered "influential," the most frequently "mentioned"[28] users in tweets containing #جبهة_النصرة were identified. Over the 50 days of data collection, users sharing tweets containing the #جبهة_النصرة tag created 45,959 connections[29] among 20,459 users. A total of 96.5% of these users were part of a single interconnected network.[30] The most influential users are those who have been most frequently mentioned. Those Twitter users are as follows:

- @JbhatALnusra;
- @Jalaaad_alshi3a;
- @zrgahalyman;
- @Wesal_TV;
- @Ahraralsham;
- @ezaah1;
- @1AbualWalid;
- @the_free_army;
- @zhoof21;
- @omarz7.

The two most influential Twitter accounts using the JN hashtag are @jalaaad_alshi3a, who appears to be an extremist al-Qa`ida follower probably based in northern Syria, and @Wesal_TV, the "official account of the [Saudi] Wesal [satellite] Television Network."[31]

Wesal TV is a particularly important node in this network. In addition to airing recruitment videos for the Free Syrian Army[32] on television, Wesal TV disseminates links to JN and other jihadist groups on YouTube to its 290,000 Twitter followers.

This highlights a key finding: twitter has become the main hub for the active dissemination of links directing users to digital content hosted on a range of other platforms.

Links on YouTube

To further investigate the use of Twitter to disseminate links, all shortlinks found in the dataset were identified.[33] After the shortlinks only shared once were discarded, the remaining shortlinks had been shared 34,850 times. Each individual link was shared a mean of 6.4 times, with a median of three. The top 10 most shared shortlinks were as follows: http://t.co/uBFlnqZ0YU: 245 times; http://t.co/MYkNDkYI: 200 times; http://t.co/zSyRYqdzC4: 197 times; http://t.co/pXjBzxJy: 180 times; http://t.co/JeqZAmqs: 150 times; http://t.co/EjGyfCxmgo: 133 times; http://t.co/OpWK6S7WwZ: 129 times; http://t.co/EYMjObQ9: 129 times; http://t.co/Mzh1SBHPsC: 118 times; http://t.co/PJ2YFiiNoW: 117 times.

Of the 20 most shared shortlinks, 80% lead to YouTube videos, while the other shortlinks direct to pictures shared via Twitter or Facebook. The most frequently shared shortlinks to YouTube content lead to 15 video files that have been watched a total of 440,200 times, although one video file accounted for 250,000 of those views. These videos are on average 273 seconds in duration and have an average Twitter "rating" of 4.9 out of 5.

Three of the video files had more than one shortlink associated with them, meaning that they were hosted on multiple websites. These video files are:

- The Moment of Attaining Martyrdom by One Member of JN (23,599 views, shared twice);
- JN: The Biggest Martyrdom Operation in al-Sham [Syria], March 11, 2013 (241,551 views);
- The Martyr Khalid Abu Sulayman al-Kuwayti of JN (41,622 views).[34]

The Visual Literacy of Role Models, Indoctrination & Radicalization

The metadata from YouTube for the video files to which the most shared shortlinks lead was also collected. Seven shortlinks were duplicates, or triplicates, in the sense that more than one shortlink leads to the same video file.[35] This process resulted in the identification of 12 unique YouTube video files among the shortlinks disseminated prominently via Twitter. Although detailed analysis will only be provided for one of the video files, all 12 clips were in Arabic, with one exception that was in Turkish.[36] All the videos related to Syria. The video file most frequently shared within the authors' Twitter dataset had more than 17,000 views on YouTube. It showed "the capture of one of the officers of Assad's army by the heroes of the Free Syrian Army and JN."[37]

The second most shared video file demonstrated vividly the multilayered and multifaceted dimension of jihadist video culture on the internet. It had more than 10,000 views and consisted of a short sequence from another video, The Sincere Promise, published by JN's media department, al-Manarat al-Bayda',[38] on al-Qa`ida web forums and other jihadist outlets online. The original one-hour video was published on May 22, 2012,[39] and is available as a full high definition version. It was a classical jihadist video but seemed influenced by AQI, resembling the general layout, the quality, as well as the military operations common to that organization. The video began by showing abuse and torture conducted by the Syrian regime, and then JN pledged a "sincere promise" to seek revenge and restore the dignity of Sunnis in Syria.

While one may expect that the most bloodiest and brutal scenes of the film would be chosen for the Twitter clip—such as the testimonies of the portrayed martyrdom operatives (istishhadiyyun), the executions of captured soldiers, or sequences showing the torture of civilians by al-Assad's shabiha militias—the sequence instead highlighted the moral actions of JN, such as moving a civilian out of the line of fire and aborting an improvised explosive device (IED) attack to prevent collateral damage. The first part of the sequence allegedly showed JN fighters engaged in Syria's northeastern city of Idlib. During a firefight between JN and government forces, one mujahid took care of a civilian, shielding him behind a wall. A grey arrow highlighted "safeguarding Muslims" to counter any possible discrediting of JN, a lesson learned from Iraq and Algeria[40] where al-Qa`ida affiliates indiscriminately bombed targets resulting in the deaths of scores of Sunni civilians.[41] The scene is further detailed on JN's official forum, describing themselves as the "mujahidin who are the ones bringing death to the shabiha. In another place the mujahidin bring humanitarian aid."[42]

The later sequences showed planned IED attacks on cars, minivans, and buses purportedly carrying troops loyal to Bashar al-Assad. In another scene, a pedestrian was branded as “Muslim” by a grey arrow, as the targets (marked as “targets”) passed by, with JN deliberately aborting the operation to avoid a civilian casualty. One of the mujahidin said off-camera, “we did not blow the car up as Muslims are here. We ask God that He may protect us, sparing their blood.”

In this case, JN is implementing lessons learned from past conflicts and has adopted its ideology in coherence with messaging from al-Qa`ida’s senior leadership.[43]

Within a few days, the sequence uploaded on YouTube under the title Jabhat al-Nusra Forbids the Carrying Out of Operations Due to the Presence of Civilians[44] was viewed about 10,000 times. In general, the comments were positive, admiring the professionalism, implementation of their ideology, and pledge to fight for the defense of Sunni Muslims. The proper operationalization of the propagated ideology was applauded by the member “soraqh,” who stated that “the jihad of our brothers in JN is [based] on the correct creed, and the blood of any Muslim is without doubt forbidden (haram).”

Conclusion

Twitter functions as a beacon for sharing shortlinks to content dispersed across numerous digital platforms. Videos shot on the battlefield in Syria are being uploaded onto YouTube and shared with followers via Twitter. Today’s social media zeitgeist facilitates emergent behavior producing complex information-sharing networks in which influence flows through multiple hubs in multiple directions.[45]

Within this zeitgeist, new jihadist files show ideological coherence, while individual consumers are able to seek guidance or further explanation should decisions, actions or deeds seem unclear. With the density of jihadist, al-Qa`ida-dominated material online, local groups such as JN or AQIM seek to frame their actions as part of this global war under the ideological umbrella of al-Qa`ida. Understanding what aspects are most appraised allow governments or analysts to potentially rate and measure elements most vital for radicalization processes in general.

While the technology can be disruptive for authorities, these platforms can also be empowering for those seeking to understand user behavior within these complex digital environments. Social media platforms produce vast quantities of data. This creates the opportunity to leverage genuine interdisciplinary approaches, which combine in-depth knowledge of big data techniques and network analysis, with rich multilingual understanding of the ideological, religious, and cultural foundations of jihadist propaganda. Ultimately, “the potential in the era of big data comes not from drowning in a sea of data but navigating the most useful ways to derive insight and develop innovative strategies.”[46]

Nico Prucha is a fellow at the Institute for Peace Research and Security Policy (IFSH), University of Hamburg. His research focuses on textual and audiovisual content analysis of al-Qa`ida activity online, specifically focusing on jihadist Shari`a law interpretation of hostage taking and executions. He has written frequently on the subject, such as for Jane’s and blogs at Jihadica. He is currently completing his Ph.D. at the Department at Near Eastern Studies at the University of Vienna.

Dr. Ali Fisher is an adviser, strategist and author on methods of achieving influence across a range of disciplines including public diplomacy and strategic communication, counterterrorism, child protection, human security, and public health. Across these diverse disciplines, his work enables organizations to identify and build networks of influence. His book, Collaborative Public Diplomacy, was published earlier this year.

Notes

[1] The persistent as well as ideologically cohesive presence of jihadist propaganda online, framed as authoritative rulings and determinations, has become an open sub-culture. The jihadist narrative, enforced by audio and visual elements, strengthens in-group cohesion and affects mainstream Muslim culture, the main targeted audience.

[2] For an introduction to the jihadist presence on Twitter as well as the social media strategy deployed since the outbreak of violence in Syria, see Ali Fisher and Nico Prucha, “Jihadi Twitter Activism – Introduction,” Jihadica.com, April 27, 2013.

[3] Cori E. Dauber, “YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer,” U.S. Army War College, 2009.

[4] Tumblr is a microblogging platform and social networking website. According to Rüdiger Lohlker, it “looks like a hybrid between blogging and Facebook. It’s in a layout similar to a blog, but it has all sorts of sharing features you may meet on Facebook. On tumblr, you will post text, photos, quotes, links, music, and videos from wherever you happen to be in a tumblelog.” See Rüdiger Lohlker, “Tumbling Along the Straight Path – Jihadis on tumblr.com,” University of Vienna, August 2012.

[5] “Al-Manhajiyya fi tahsil al-khibra al-i’lamiyya, Mu’assasat al-Furqan & Markaz al-Yaqin, part 1,” Markaz al-Yaqin and al-Furqan, May 2011.

[6] The sanctioning of jihadist activity is related to the existing core fatawa (authoritative rulings and ideological decrees). Thus, any local jihadist, al-Qa`ida-affiliated action is placed under the virtual umbrella, increasing the appeal. See Prem Mahadevan, “The Glocalisation of al-Qaedaism,” Center for Security Studies, March 22, 2013.

[7] Discussed in Fisher and Prucha, “Jihadi Twitter Activism – Introduction”; Nico Prucha, “Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors,” Orient 4 (2011). Members of the Ansar al-Mujahidin forum and Shumukh al-Islam have posted advice encouraging fellow users to develop social media profiles to disseminate their message to a wider group of users. See for example: “The Twitter Guide // the Most Important Jihadi Users and Support Accounts for Jihad and the Mujahideen on Twitter,” available at www.shamikh1.info/vb/showthread.php?t=192509;

[8] The jihadist success in using Twitter has had its impact on leading jihadist writers such as Abu Sa`d al-`Amili to highlight the shift of “major [jihadi] writers and analysts,” lamenting the general decline in participation in jihadist online forums. Furthermore, al-`Amili issued a “Call (nida’) to the Soldiers of the Jihad Media” demanding that they “return to their frontiers (thughur)” elevating their status. Al-`Amili himself is a high profile cleric, but is also quite active on twitter under @al3aamili. Also see Cole Bunzel, “Are the Jihadi Forums Flagging? An Ideologue’s Lament,” Jihadica.com, March 20, 2013.

[9] Twitter has become an addition to the classical forums but is attracting more interaction among members subscribed to the jihadist worldview. Within the “jihadiscape” on Twitter, members re-publish and disseminate “official” al-Qa`ida content, upload their personal files, such as pictures via their mobile phones, or link to extremist content on YouTube. Twitter has become the new beacon for jihadist propaganda and, more importantly, a free zone for extremist users online. The jihadist forums, however, are the first place where new jihadist core content is injected and then promoted by initiated users. On the importance of online forums, see Evan F. Kohlmann, “A Beacon for Extremists: The Ansar al-Mujahideen Web Forum,” CTC Sentinel 3:2 (2010).

[10] “AQTweets,” Inspire 11 (2013): p. 17. The cover story and a colorful picture commemorating Tamerlan Tsarnaev elaborated the “AQTweets” section. In the picture, the Boston bomber is depicted as sending an SMS from paradise to his mother: “My dear mom, I will lay down my life for Islam. I’m gonna die for Islam Inshaa Allah.” Reactions taken from Twitter include the user Abu Shamel, who stated: “Allahu Akbar, I feel so happy, only 2 soldiers of Allah defeated America, it’s army & #intel America can never stop the decree of Allah.” The magazine took credit for having successfully inspired not only the Boston bombers, but also the Woolwich assailants, in a reasoning phrased as an “eye for an eye,” revenge for the occupation of Islamic countries and the deployment of unmanned drones.

[11] Solely appearing in this list of users should not be considered evidence of jihadist affiliation. For example, academics and commentators writing about the phenomena may also appear in this list of 20,000.

[12] Recent martyr biographies—such as Abu Qasura al-Gharib, a 19-year old Libyan fighting for Jabhat al-Nusra—outline how the internet and the regular consumption of ideological materials have impacted a new generation. The biography, a eulogy written by one of his brothers in arms published on the Shumukh al-Islam forum, highlighted how Abu Qasura (Muhammad al-Zulaytni) used his

iPad to improve his knowledge, embrace al-Qa`ida ideologues, and remain active online within the jihadist spheres while he fought in Syria. The virtual footprint of real-life martyrs and their internet habits is part of the advocated role model. He was killed on January 4, 2012. For details www.shamikh1.info/vb/showthread.php?t=193834.

[13] On the strategy and tactic of how the primarily Arabic language ideology is conveyed by individual preachers and activists, in this case for Germany and Austria, see Nico Prucha, "Die Vermittlung arabischer Jihadisten-Ideologie: Zur Rolle deutscher Aktivisten," in Guido Steinberg ed., Jihadismus und Internet: Eine deutsche Perspektive (Berlin: Stiftung Wissenschaft und Politik, 2012), pp. 45-56.

[14] See also Rüdiger Lohlker, "Religion, Weapons, and Jihadism Emblematic Discourses" and Philipp Holtmann, "The Symbols of Online Jihad," in Rüdiger Lohlker ed., Jihadism: Online Discourses and Representations (Göttingen: Vienna University Press, 2013).

[15] The Ansar al-Mujahidin network, a tier-one jihadist forum, for example, advertises its Twitter account

(@as_ansar) on its main page. The lesser renowned al-Minbar al-I'lami al-Jihadi forum does the same

(@alplatformmedia). When the Shumukh al-Islam forum was down recently, a forum member active on Twitter cheered in appraisal with a picture of the forum after it went back online. The caption, in "Twitter-speak," read: "all praise be God, #shabakat_shumukh_al-Islam has returned back working, may God reward those who set it up good and maintain it pure for the media of Jihad."

[16] "Denis Allex: French Agent 'Killed' by Somalia al-Shabab," BBC, January 17, 2013.

[17] Al-Shabab circulated the Facebook link to its Arabic account on Twitter to increase awareness.

[18] This "press release," claiming the execution of Denis Allex, went online on January 16, 2013, four days after the French attempt to free the hostage. It further stated, "the death of the two French soldiers pales into insignificance besides the dozens of Muslim civilians senselessly killed by the French forces during the operation. Avenging the deaths of these civilians and taking into consideration France's increasing persecution of Muslims around the world, its oppressive anti-Islam policies at home, French military operations in the war against Islamic Shari'ah in Afghanistan and, most recently, in Mali, and its continued economic, political and military assistance towards the African invaders in Muslim lands, Harakat Al-Shabaab Al Mujahideen has reached a unanimous decision to execute the French intelligence officer, Dennis Allex."

[19] He updated his profile after announcing the merger of Jabhat al-Nusra with the Islamic State of Iraq, claiming to be the media account for the "Islamic State of Iraq and al-Sham [Syria]."

[20] At the end of January 2013, AQAP disseminated three statements via Twitter. A high profile jihadist Twitter user, @STRATEAGY, "retweeted" these. A member of the Ansar al-Mujahidin forum posted a screenshot of the subsequent "retweets" on the forums, to gain more attention for AQAP. See "Urgent – Three New Statements by AQAP," available at www.as-ansar.com/vb/showthread.php?t=79875.

[21] "Statement Regarding the New Twitter Account," available at www.as-ansar.com/vb/showthread.php?t=85175.

[22] "Now the Open Interview with Shaykh Ahmad Abu `Abd al-Ilaha, the Head of the Media Board for al-Andalus," available at www.as-ansar.com/vb/showthread.php?t=85501&highlight=andalus_media.

[23] The questions and answers, in Arabic, can be accessed here: http://ia801703.us.archive.org/11/items/answersI.1/answersI.pdf.

[24] "AQTweets," Inspire 11 (2013): p. 17.

[25] At the time of writing, @jbhatalnusra has just over 60,000 followers, a 33% increase since April 3, 2013, and 6.5% since May 7, 2013.

[26] "Influential users" were determined by those posting content using the Jabhat al-Nusra hashtag.

[27] Analysis of the first two weeks of aggregated data, previously published on Jihadica.com, identified a network of 12,253 connections between 7,051 accounts that were either actively sharing content via retweet or were mentioned in a tweet containing #قرصنة_فجح. Ninety-five percent of the users formed a single interconnected information sharing network. Only 352 of the 7,051 users observed tweeting using #قرصنة_فجح did not interact with at least one member of this network. See Nico Prucha, "Jihadi Twitter Activism Part 2: Jabhat al-Nusra on the Twittersphere," Jihadica.com, May 13, 2013.

[28] On Twitter, "mentioning" another user is when one individual tweets another individual's username in a message.

[29] For the purposes of this study, a "connection" is made when one user retweets or mentions a second user on Twitter.

[30] A smaller version of this network can be seen at Prucha, "Jihadi Twitter Activism Part 2: Jabhat al-Nusra on the Twittersphere."

[31] The Saudi satellite TV station Wesal, a global television network with more than 290,000 followers on Twitter, is essential for Jabhat al-Nusra propaganda-wise. @Wesal_TV actively addresses the ongoing fighting against the al-Assad regime, calling for financial, material, and personal support for the Sunnis in Syria. For a full discussion, see Prucha, "Jihadi Twitter Activism Part 2: Jabhat al-Nusra on the Twittersphere."

[32] See www.youtube.com/watch?v=m1FW-YFu1DE.

[33] URL shortening services save space in microblogs, such as Twitter, due to character limits.

[34] These reflect the number of views per link, not in total. All numbers correspond to the number of views on YouTube, as of May 30, 2013. Three links regarding the "martyr" from Kuwait, Khalid Abu Sulayman, were shared, of which two are identical. The third video is a eulogy in the form of a rhyme with various pictures of the fighter whose real name was given as Khalid bin Hadi al-Dihani al-Mutayri. This video has 9,617 views and includes screen grabs of Twitter where JN sympathizers propagated his "martyrdom." See www.youtube.com/watch?v=1b0a661vKNs.

[35] The author's use of "video file" means a file stored on the YouTube system with a specific ID to distinguish it from two visually similar "videos" that have separate video IDs. Despite the colloquial use of "video," users actually share, view and comment on specific video files.

[36] A 14-minute video showed the radical pro-Chechnya emirate, anti-Russian and anti-Assad demonstration by "Garip-Dar" in front of the Russian Embassy in Ankara, Turkey. It was uploaded on January 27, 2013, by the user "ömer onur belül" who has only posted this one video on YouTube. It received much less traction, with about 2,500 views by February 25, 2013. The clip showed a speaker and his followers holding a "press conference," held in Turkish. This may be the reason for the difference in views. While the majority of Arabic-language Twitter users reposted this clip in support of the jihad in Syria, it was of lesser importance due to the language barrier. See Garib-Der Rusya BüyükelÇiligi Basin AÇiklamasi, available at www.youtube.com/watch?v=wVr4OGB6xGY.

[37] According to the video description, the officer, also named a shabiha, was captured and interrogated in the countryside of Homs. See www.youtube.com/watch?v=9lsPYCaln5o&feature=g-subs-u.

[38] Aaron Y. Zelin, "The Rise of Al Qaeda in Syria," Foreign Policy, December 6, 2012.

[39] Sidq al-Wa'd, The Sincere Promise, can be retrieved on "Jihad Archive" at www.jarchive.net/details.php?item_id=7528 as well as on other jihadist forums.

[40] For a case on how the leadership of AQIM justified two major suicide bombing operations in the capital of Algeria in 2007 after being criticized by sympathizers on the jihadist forums, see Nico Prucha, "A Look at Jihadists' Suicide Fatwas: The Case of Algeria," Research Institute for European and American Studies, 2010.

[41] Scott Helfstein, Nassir Abdullah and Muhammad al-Obaidi, Deadly Vanguards: A Study of al-Qa`ida's Violence Against Muslims (West Point, NY: Combating Terrorism Center, 2009).

[42] For details, see www.jalnosra.com/vb/showthread.php?t=138.

[43] See, for example, Charles Lister, "Jabhat al-Nusra – a Self Professed AQ-Affiliate," Jihadica.com, May 8, 2013.

[44] For details, see www.youtube.com/watch?v=ByRY4bxyZjM&feature=youtu.be.

[45] Ali Fisher, Collaborative Public Diplomacy: How Transnational Networks Influenced American Studies in Europe (New York: Palgrave Macmillan, 2012).

[46] Ali Fisher, "Everybody's Getting Hooked Up: Building Innovative Strategies in the Era of Big Data," Public Diplomacy Magazine Summer (2012): pp. 43-54.

Table of Contents

Facebook Being Used To Recruit Indonesians For Terrorist Attacks

By Niniek Karmini, AP, Jun 22, 2013

JAKARTA – Sefa Riano didn't try to hide his plans or his beliefs. A Facebook page that police traced to him is plastered with photos of bearded men in camouflage uniforms holding rifles and banners hailing "the spirit of jihad."

One status update in late April apologizes to his parents before telling them goodbye. Another declares ominously, "God willing, I will take action at the Myanmar Embassy, hope you will share responsibility for my struggle." It ends with a yellow smiley face.

Days later, police arrested Riano, whose Facebook name is Mambo Wahab, just before midnight in central Jakarta. Police say he and another man were on a motorbike carrying a backpack filled with five low-explosive

pipe bombs tied together. Riano, 29, is awaiting charges related to allegations that he plotted to bomb the embassy to protest the persecution of Muslims in Buddhist-majority Myanmar.

A police investigator revealed Riano's connection to the page, which was still online Thursday. The investigator spoke on condition of anonymity because he was not authorized to talk to reporters.

The investigator said Riano caused his own downfall by publicizing his mission on Facebook, but added that police believe it was another Facebook page that drew him to radical Islam to begin with.

Police said a growing number of young people in Indonesia, the world's most populous Muslim-majority nation, are being targeted for recruitment by terrorists on the social media site. More than one in four of the country's 240 million people are on Facebook, thanks in large part to cheap and fast Internet-capable phones.

While it is not clear how many terrorists are actually recruited through Facebook, the use of social networking to groom potential attackers poses new challenges for authorities struggling to eradicate militant groups that have been weakened over the last 10 years. Though Facebook shuts down pages that promote terrorism when it learns of them, police say new pages are easily created and some have attracted thousands of followers.

Muhammad Taufiqurrohman, an analyst from the Center for Radicalism and Deradicalization Studies who works closely with Indonesian antiterrorism officials, said 50 to 100 militants in the country have been recruited directly through Facebook over the past two years.

He said there are at least 18 radical Facebook groups in Indonesia, and one of them has 7,000 members. Police said some sites where radical discussion takes place focus on Islam, while others engage in talk about committing violence, such as how to make bombs. Access is blocked unless group administrators allow users to participate.

Fred Wolens, a Facebook spokesman, said the company bars "promotion of terrorism" and "direct statements of hate." Where abusive content is posted and reported, Facebook removes it and disables the account, he said.

Gatot S. Dewabroto, spokesman for Indonesia's Ministry of Communication and Information, said Facebook responds quickly when officials ask them to remove such content. But he added that after one page is blocked, others quickly spring up.

William McCants, a former U.S. State Department analyst who studies online Islamic extremism for the U.S.-based Center for Naval Analyses, said governments in many countries "are just waking up to the fact that the conversation (about extremism) is moving to newer social media platforms."

"On Facebook and Twitter, you can really go after people who broadly share your ideology but haven't really committed themselves to violence," he said.

Indonesian police say Facebook is one of many places where they've found terrorist activity online. They have detected militants using online games for attack drills. A group was caught uploading propaganda videos on YouTube and terrorists are known to have purchased weapons using video calls, said Brig. Gen. Petrus Reinhard Golose, the director of operations at Indonesia's anti-terrorism agency.

Golose said the Internet was used to organize recent terrorist acts in the country, including a 2010 attack on police in Solo and a police mosque bombing in Cirebon a year later. He did not elaborate on how the Web was used.

Terrorists have used the Internet for many years, but usually anonymously. Groups such as al-Qaida have employed online discussion forums where people left comments but did not directly interact. Today's smartphone generation appears to be operating more openly: As of Thursday, Riano still had about 900 Facebook friends.

The police investigator said authorities were alerted about "Mambo Wahab's" Myanmar bombing status update by other Internet users. Police used information collected from arrested militants in Riano's online networks to track his Web footprint. After getting his Internet Protocol address and eventually linking that to a mobile phone, authorities say they were able to tap into conversations involving Riano and the plot's alleged mastermind, the investigator said.

The Mambo Wahab page has not been updated since Riano's arrest May 3. Some people in Indonesian jails — even on death row — manage to post status updates, though others may be acting on their behalf.

Some Indonesian police want the law to address online communications that advocate or abet terrorism. Indonesia's information technology laws ban only pornography and illegal online financial transactions.

Police Maj. Surya Putra, who is researching terrorists' use of the Internet at the Institute of Police Science, said intelligence collected online cannot currently be used as evidence in court.

"There are no laws that can effectively charge people who spread hatred," he said.

The government is drafting legislation that would criminalize hate speech and online terrorism activities.

Sidney Jones, a Jakarta-based terrorism analyst from the International Crisis Group, said that although terrorists groups' Internet use is growing, they still do most of their recruiting face-to-face at traditional places such as prayer meetings. She said Riano's case is the first time she has seen a group brought together by Facebook.

She said the site is a "really stupid" way to recruit new members because it lacks privacy and no systematic way to vet credentials. But she added that even amateurish efforts to commit terrorism can cause mayhem and must be taken seriously.

Ansyaad Mbai, who heads Indonesia's anti-terrorism agency, said Facebook has become "an effective tool for mass radicalization," and that police need more authority to respond to online behavior.

"We can't do it alone," he said. " . . . Radical sermons and jihadist sites are just a mouse click away."

Table of Contents

With Social Media, Middle Classes in Brazil, Turkey Grow Stronger, Angrier

By Ashish Kumar Sen, Washington Times, June 26, 2013

Mass protests in Brazil and halfway around the world in Turkey are the latest manifestations of the coming of age of a politically aware global middle class that, armed with little more than Twitter and Facebook, is demanding greater government accountability, basic rights and a more equitable distribution of resources.

In Brazil, protesters garnered a victory late Tuesday when the lower house of Congress rejected legislation that many feared would have made it harder to prosecute government corruption.

The protests were triggered this month by an increase in bus and metro fares in Sao Paulo, Brazil's largest city, and fueled by public frustration with high taxes, poor public services, huge government spending for the 2014 soccer World Cup and 2016 Olympics, and overall government corruption.

In Turkey, protesters first turned out in May to oppose the government's plan to redevelop Gezi Park, an urban park next to Istanbul's Taksim Square. Police responded with a brutal crackdown, and the protests quickly spread to other cities with thousands denouncing what they see as Turkish Prime Minister Recep Tayyip Erdogan's authoritarian style of governing.

Flexing new power

"The emerging middle classes in both Turkey and Brazil are beginning to flex their new power in shaping the policy discourse," said Terra Lawson-Remer, a researcher for civil society, markets and democracy issues at the Council on Foreign Relations.

Much like the protesters in Turkey, most demonstrators in Brazil have jobs and are better educated than the majority of the population.

Unlike countries such as Greece and Spain where weak economies have brought the unemployed out onto the streets, the discontent in Brazil has been created by strong economic growth. As standards of living have risen, so have expectations. The government's failure to meet those expectations has resulted in widespread frustration.

Brazilians are not protesting because they want to overthrow a dictator or are angry about massive unemployment. They are upset about the priorities of the government, said Joseph Bateman, an analyst on Brazil at the Washington Office on Latin America.

Over the past decade, Brazil's economy has grown rapidly, lifting millions out of poverty and creating a larger middle class.

"This middle class expects certain public services to be provided by the government," Mr. Bateman said.

"But now that the economy is beginning to retract, the government is making big cuts in basic public services. And when [the middle class] sees the government putting a priority on the Olympics and the World Cup and not on education and health, they are upset."

Different responses

The Brazilian and Turkish governments have responded very differently to the protests.

Brazilian President Dilma Rousseff, a former leftist guerrilla who was imprisoned and tortured in the 1970s during Brazil's military dictatorship, has said the protesters are proof of a vibrant democracy and has acknowledged their grievances.

The Rousseff administration, however, is in a difficult situation, as it faces the challenge of managing an overheated economy and inflation driven largely by global capital movement, Ms. Lawson-Remer said.

In Turkey, the police crackdown on the protesters marked a turning point.

The protests turned into an "expression of frustration with a prime minister who has become increasingly paternalistic and authoritarian," said Kemal Kirisci, director of the Center on the United States and Europe's Turkey Project at the Brookings Institution in Washington.

"In an ironic way, [the protests are] a product of the success of this government in helping to develop a stronger middle class, especially the highly educated section of the middle class that lives in the cities. … The government's failure to hear their voice and the adoption of policies that these people feel are strangling their individualistic liberties," Mr. Kirisci said.

Mr. Erdogan this week drew comparisons between the protests in Turkey and Brazil.

"The same game is now being played over Brazil," Mr. Erdogan told supporters in the Black Sea coastal city of Samsun. "The symbols are the same. The posters are the same. Twitter, Facebook are the same. The international media is the same. … It's the same game, the same trap, the same aim."

Mr. Erdogan may have compromised on his development plans for Gezi Park by throwing the matter to the courts, but he has been largely dismissive of the protesters.

"The message that is given is 'If you have any problems, wait until the next election.'" Mr. Kirisci said.

Such an attitude has done little to dent Mr. Erdogan's popularity.

Mr. Erdogan is popular among Turkey's more recently urbanized middle class that supports his Justice and Development Party, said Hugh Pope of the Istanbul office of the International Crisis Group. The party "has been an incredibly effective government," he said.

Mr. Pope described the protests in Istanbul as "happy, spontaneous, humorous" events, and that the participants were "mainly concerned with the way the police was so ruthless in putting down the protests."

Arab Spring effect

In Turkey's neighborhood in the past three years, regimes have toppled as they used force to put down the pro-democracy protests of the Arab Spring.

The Arab uprisings are on the minds of leaders in Turkey, but not Brazil, Ms. Lawson-Remer said.

"The current protests suggest a need for a serious reorientation in some of [Turkey's] economic and political priorities and strategies, but Brazil's democratic government is not under threat," Ms. Lawson-Remer said.

"Turkey is a different story. Turkey has seen it's neighbors totter and fall over the past three years, and Turkey is far from a free democracy, so the regime changes precipitated by mass movements throughout the Middle East three years ago are certainly hanging over both Turkey's rulers and the protesters there."

Much as it did in the Arab Spring protests, social media has played a big role in galvanizing the protests in Turkey and Brazil.

In Brazil, protesters have turned out in response to Facebook invitations.

In Turkey, social media has upstaged the mainstream Turkish media, which avoided reporting on the early days of the demonstrations and instead broadcast cooking shows and documentaries on penguins.

"That legacy [of the media] will remain," Mr. Kirisci said.

Table of Contents

Big Pic: How Turkish Protesters Use Google Maps To Track Police

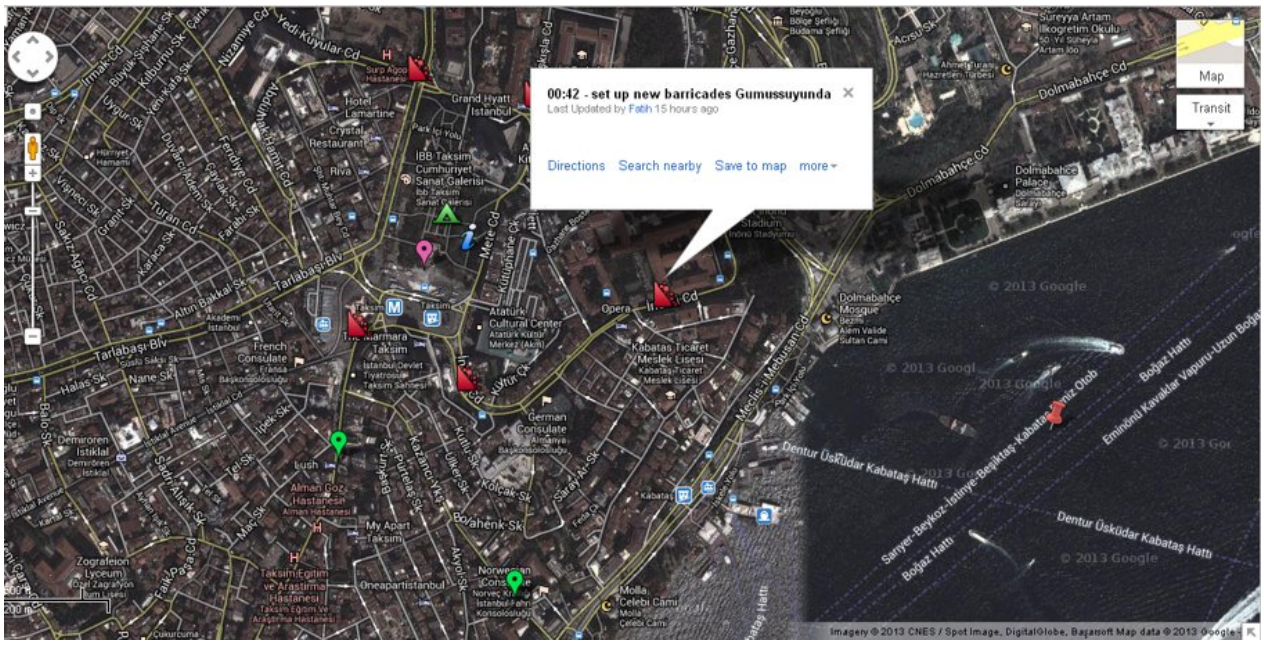
Protesting? There's a map for that.

By Kelsey D. Atherton, PopSci, 06.04.2013

Mapping police actions around Taksim Square, Istanbul Google Maps

Consider it civilian reconnaissance. Protesters in Turkey are using Google Maps to track police movement, plot out barricades, and rally together.

Created Saturday, the map of Istanbul Police Movements centers on Taksim square, the heart of recent (and ongoing) protests against the Prime Minister Recep Tayyip Erdogan's government. It began last week with trees and a barracks. Erdogan's government plans to renovate an Ottoman barracks, a structure dating back at least a century, near the square. To get construction equipment to the barracks, officials wanted to raze trees from the nearby Gezi Park. Protesters prevented this, demonstrating in defense of the green space for over a week. Since then, protests expanded, evolving into a critique of the current ruling party.



Mapping protests and police response in real-time is a relatively new phenomena. In 2010, students protesting in London used a Google Map to track police action, documenting riot vans and helicopters moving against the protesters. But some features of the Turkish protests are straight out of *Les Misérables*, or indeed any number of historical protests. Barricades keep vehicles, police, and even horses away from the protesters, take time to tear down, and protect against thrown objects or gunfire, should the police response turn violent. In centuries past, governments brought in armies to quell protesters, and used cannons to knock down barricades. Paris, the site of so many protests, even underwent a major urban redesign with wider streets to make barricades more difficult.

In addition to the red triangle markers of barricades, here are some features of the map:

- A green tent to mark the heart of Taksim Square
- Road warnings in green, letting people know which one are open and which are blocked
- Pink tags for groups announcing who they are and where they are protesting
- Light blue flags for police locations and reported movements
- Warnings of police tracking servers online, confusingly under light blue as well.
- General rallying cries, slogans, and mottos from protesters are marked with house symbol

Notably absent? Sensitive information, like the location and identity of specific individuals, like volunteer doctors. In the jargon of secrecy, that's called good Operational Security. In plain talk, it's just common sense.

Table of Contents