Information Operations Newsletter

Compiled by: **Mr. Jeff Harley**

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

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

ARSTRAT IO Newsletter on Phi Beta Iota

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

Table of Contents

Vol. 12, no. 10 (August 2012)

Disinformation Flies in Syria's Growing Cyber War

By Peter Apps, Reuters, 7 August 2012

LONDON (Reuters) - On Sunday, it was a hijacked Reuters Twitter feed trying to create the impression of a rebel collapse in Aleppo. On Monday, it was another account purporting to be a Russian diplomat announcing the death in Damascus of Syrian President Bashar al-Assad.

As the situation on the ground becomes ever more bloody, both sides in Syria are also waging what seems to be an intensifying conflict in cyberspace, often attempting to use misinformation and rumor to tilt the war in reality.

On Friday, Reuters was forced to temporarily shut down its system for posting blogs on www.Reuters.com after the appearance of a series of unauthorized, and inaccurate, reports citing opposition military reverses in Syria.

On Sunday, the company took similar action to suspend the @ReutersTech Twitter account after it appeared to have been seized, renamed and used to send a series of false tweets apparently designed to undermine the rebel Free Syrian Army. Both incidents remain under investigation.

The attacks were not the first time a major media or other organization had been targeted apparently by supporters of Assad. Some - including the defacement of a Harvard University website last year to post a picture of Assad in military uniform -- have been claimed by the "Syrian Electronic Army".

But Assad's government too have had their own embarrassments in cyberspace. Hacker group Anonymous claimed credit for stealing thousands of internal Syrian government e-mails including personal communications between Assad and his wife. The entire tranche was later published online by Wikileaks.

"It's not surprising that Syria has attempted to develop a cyber warfare capability. It's in line with their chemical and biological warfare programs and their aspirations as a regional power," said John Bassett, former senior official at British signals intelligence agency GCHQ and now a senior fellow at London's Royal United Services Institute.

"But the regime's technical capabilities look pretty basic, and the opposition hacking of the personal emails of Assad and his wife earlier this year show the regime's cyber defenses have serious weaknesses."

The opposition too, many suspect, have been doing what they can do to spread rumors about their opponents. On Monday afternoon, a Twitter account purporting to be that of a senior Russian official said Assad had been killed in Damascus, prompting a flurry of speculation and telephone calls by agencies such as Reuters before the Russian Foreign Ministry confirmed the news was fake.

"Cyber attacks are the new reality of modern warfare," said Hayat Alvi, lecturer in Middle Eastern studies at the US Naval War College. "We can expect more... from all directions. In war, the greatest casualty is the truth. Each side will try to manipulate information to make their own side look like it is gaining while the other is losing."

With Assad's opponents desperate to attract defectors - such as Prime Minister Riyad Hijab who fled on Monday - and the government keen to avoid further foreign support for rebels already backed by Turkey, Saudi Arabia and Qatar, the stakes are undoubtedly high. The Alawite-dominated government needs to demonstrate it can survive, while the rebels must present themselves as a coherent government in waiting and keep down talk of potential Al Qaeda infiltration.

In recent months, the "Syrian Electronic Army" (SEA) in particular looks to have adopted a strategy to target media outlets to spread disinformation helpful to the Damascus government or harmful to its foes.

In April, Saudi-based broadcaster Al Arabiya briefly lost control of one of its twitter accounts, which was then used to spread a string of stories suggesting a political crisis in Qatar. Tweets included claims that the Qatari prime minister had been sacked, his daughter arrested in London and that a coup orchestrated by the army chief was underway.

In July, Al Jazeera suffered a similar attack, with one of its Twitter feeds used to send a series of pro-Assad messages including accusing the Qatar-based channel of fabricating evidence of civilian casualties in Syria.

Such exchanges, experts say, are increasingly becoming part of any conflict. During the 2008 Georgia war, Russian and Georgian hackers - either state-backed or operating independently - each mounted a range of attacks on each other's official websites.

STRICTLY LIMITED EFFECT

In reality, however, there seems little sign such incidents made a significant difference either on the ground in Syria or to the wider geopolitical picture.

The assorted Reuters blog postings on Friday published through a now closed vulnerability in the WordPress software used to manage the site, bore a superficially convincing resemblance to other genuine entries.

But the written style - as well as some of the grammar and style - were notably different to real Reuters reports, which continued to be posted without difficulty and disseminated to Reuters media, financial and other clients.

While some of the false blog posts were at least briefly shared via social media by readers who believed they were honest reports from Aleppo, it is far from clear whether anyone in the embattled city itself ever saw them.

A Reuters reporter on the ground quickly confirmed the reported rebel collapse in several key named suburbs appeared to be false, and postings themselves were quickly removed - although occasional screenshots remain on the Internet.

Nor does it appear that anyone was particularly convinced by the Sunday flurry of tweets from the captured @ReutersTech Twitter account, hastily renamed @ReutersME in an apparent attempt to present itself as a Middle East-based feed.

Again, there was a series of messages detailing a supposed rebel defeat in Aleppo, where heavy fighting continued on Monday with opposition forces still in control of much of the city. The account said rebel forces were out of ammunition and in "a sad situation" while the Syrian army boasted the fight was like "shooting fish in a barrel".

It then went on to claim that the White House had confirmed it was arming Al Qaeda militants within Syria as part of its support for the fight against Assad. In the final handful of tweets before access was cut, the user said Washington had always funded Al Qaeda even in the decade since the September 11, 2001 attacks and then accused Reuters itself of being in the "iron grip" of the Rothschild banking dynasty.

"The problem with these attacks is that they are always quickly noticed and even if they are successful in grabbing headlines and fooling people for a short period of time, they have very limited effect," said Tal Be'ery, web security research team leader at IT security firm Imperva.

"They are not that technically sophisticated, and my assessment is that they would most likely be from amateurs rather than the regime itself. That tells us that Assad still has some support amongst people able to do this both inside and outside the country, but that is about it."

TRACKING OPPOSITION REAL PRIORITY

Monday's Twitter-fuelled rumors of Assad's demise, knocked down within minutes, could conceivably have shaken some of his supporters but are unlikely to have lasted long.

The true priority for the real computer experts of both the government and opposition, most believe, will be the cat and mouse game between government surveillance systems and the opposition networks they are trying to track.

For Assad's opponents, evading government detection has long been a matter of life and death. Autocratic governments around the world, specialists say, have put considerable effort into tightening their Internet surveillance on potential dissidents since last year's "Arab spring" ousted rulers in Tunisia, Egypt, Libya and Yemen.

"The primary target of SEA is certainly their own citizens," said Alexander Klimburg, cyber security expert and fellow at the Austrian Institute for International Affairs.

"It is hard to estimate how successful they are tracking the protesters, but it seems they are much better at it than the former Tunisian or Egyptian secret police, and seem just as good as the Iranian security forces in this regard."

Some believe Assad may be getting technical support from his long-term allies in Tehran, who successfully crushed their own post-election protests that were in part organized over the Internet. China and Russia too are has amongst the world leaders in managing online political activism and dissent, with the latter at least also seen likely helping out in Syria.

"We know that they have been having a lot of success with fake online Facebook profiles, ssl certificates and other methods to break into the opposition," said Imperva's Be'ery. "We know that Russia was very involved in setting up the Syrian signals intelligence system and it is possible they still have access to Russian expertise and even experts."

The opposition too may also have foreign support. Some suspect the hand of a western signals intelligence agency in the Assad e-mail leak, while the U.S. State Department says it has given them technical advice and equipment to help stay one step ahead of government monitoring.

But Syria's Assad, experts say, has long taken an interest in the Internet and its potential uses. Before taking the presidency, he was president of the "Syrian Computer Society", a group now widely believed to have been something of a precursor to the "Syrian Electronic Army".

"It is probably not officially integrated into the security services," Klimburg said. "As such, it performs similar tasks to the "Shabbiha" militias - intimidation of local anti-government forces and direct operations that the Assad regime thinks are best not associated with it."

Table of Contents

The Nature of China’s Information Operations Strategy

Posted by Michael, XeroCrypt blog, August 13, 2012

Recently I set myself the task of coming up with a summary or digest of the PRC’s information operations, based on what’s known rather than what’s widely assumed from the numerous reports of industrial espionage. Given the number of cases being reported and (rightly or wrongly) attributed to China, this is something everyone in the infosec field should aim to understand, but that’s easier said than done with all the background noise over APT and targeted attacks.

The Three Factors of China’s Information Operations

Logically the best place to look is the PRC itself, or the Peoples’ Liberation Army (PLA). Three central factors shaped the PRC’s current information operations strategy, it seems.

According to Global Defence: ‘China does not publish equivalents to the US National Security Strategy, National Defence Strategy, or National Military Strategy. Rather, China uses “white papers,” speeches and articles as the principal mechanisms to communicate policy and strategy publicly.’

Most the literature is contributed by influential officers within the PLA. What this indicates is the PLA’s command has a highly academic and collaborative approach to formulating long-term strategies for gaining information superiority.

Next was the unification of civilian and military telecommunications. With most nations the latter is technologically 20 years behind the civilian world, as any former signals personnel would attest. Chairman Jian Zemin recognised this gap, and in 1991 called for a common telecoms network suitable for both peacetime and military use, according to Lt. Col. Timothy L. Thomas in the Military Review (May 2001).

This is important, because the idea was the PLA would establish a reserve force to maintain the backbone of civilian comms, in particular the Internet, and that reserve would be a sizeable contingent of highly-qualified personnel that could readily assist the PLA’s information operations. In effect, ‘information warfare’ becomes a ‘peoples’ war’. I believe there are currently large reserve units (around 20,000 strong) maintaining the Golden Shield at the border gateways.

The third formative influence in the PLA/PRC’s strategy were the actions of various patriot hacker groups in response to real-world events around 1999/2000, namely the bombing of the Chinese embassy. The PLA were quick to see the benefits of enlisting these hacker groups as proxies in its information warfare efforts.

So, bringing the three factors together, this is essentially where we are now – a PLA reserve with the qualifications and experience to run civilian comms infrastructure in support of military operations, a command with high academic ability, and an unknown number of highly-skilled patriot hacker groups at its disposal to put strategy into practice.

Compare this to the situation in the west, where we’re reliant on the corporate infosec industry that’s short of actual hackers and places too much importance on policies and procedures. The PRC obviously has the advantage, skill-wise, and they’ve been working towards that for a long time.

APT Characteristics and Methods

So we come to the ‘Advanced Persistent Threat’, a term that’s become fashionable in the infosec field, even if there’s confusion over what constitutes ‘advanced’ and ‘persistent’. Often APT is automatically associated with China, in a similar way highly advanced malware is fast becoming a trademark of the United States. The way I see it, there are two defining attributes to a genuine APT:

1) Advanced – Technical skills, intelligence gathering capabilities and perhaps extensive resources provided by a government or corporation. The threat agents have the ability to develop and combine intrusion techniques specifically for the target.

2) Persistent – The threat will focus on the target and attempt to maintain access to a system undiscovered over a prolonged period, or penetrate the network to achieve some longer-term objective.

Basically APT will involve a skilled hacking group, but that group will have the backing of a government or corporation with advanced intelligence gathering capabilities, and perhaps there'll also be a team of engineers and consultants. That's the long and short of it.

What are the typical methods of APTs, if there are any? Corporate networks have a very large 'attack surface', so there's a wide range of options available to someone attempting to penetrate them. Any network that becomes a target of an APT will get compromised, one way or another, and the idea that a commercial security product can prevent it is BS.

It seems the main thing the PRC are commonly accused of is electronic espionage, in particular the theft of 'intellectual property' from corporate networks. What I've noticed is that each round of attacks tends to focus on groups of companies operating within a single given sector, further suggesting there are multiple hacking groups being co-ordinated by one entity.

Compromising a network and maintaining persistent access requires a considerable amount of intelligence gathering, analysis, footprinting and planning. The attacker must (and probably will) evade whatever monitoring and auditing measures are in place, and do the job without raising any suspicion.

This suggests a Remote Access Tool with a very small memory footprint will be the common feature of an APT, and it would most likely be installed on a system that's rarely booted with a static IP address – fewer connections established between the compromised system and the C&C server will vastly reduce the chances of discovery. Malware has to do something in order to be detected, so this kind of rootkit could remain dormant until needed.

The above traits are ones I'm quite certain are common across almost all true APTs. The unknown here is the method of intrusion.

The attacker doesn't even have to compromise the target machine directly, and that would be out of the question anyway if the target is too well-protected. Using intelligence gathering or espionage, it's possible to find employees with access to the specific machine, and infect their personal computers with malware that transfers itself to a portable device. There would be a strong chance one of those would then plug the infected device into the target.

Another possible method of intrusion is through compromising another organisation in the target's supply chain with lower security.

The Problems of Attribution

Tracing an IP address to China, and tracing an attack to the PRC are two different things. For all we know, a corporation, or even a criminal group operating in another country might be the culprit. Attribution would require successfully tracing an attack to agents with a proven link to the government or military. Of course the lack of publicly-available evidence for this, along with the denials from Chinese government officials, mean we might never know for certain how many attacks are wrongly attributed to the PRC.

Graham Clueley of Sophos said as much:

'If you were to investigate the IP address of the computer which sent spam into your mailbox today you'd probably find a good proportion of it came from a PC based in China. Going by the latest stats that we produced, 9.9% of spam is coming from that part of the world… You'll probably find that a lot of it is promoting pharmaceuticals coming out of North America, Russian brides, or a cheap college diploma.'

With so many attacks being traced to China, a proxy there would provide excellent cover for anyone with the ability to translate the Chinese hosting companies' web pages. Sure, any corporation or government could hire the translators for that, which would neatly explain why the objective seems corporate espionage. Conversely, if this fact was widely known, it would also provide decent cover for the attacks the PRC actually were sponsoring.

Attack Case Studies

Not all attacks the PRC is accused of take the form of Advanced Persistent Threats. GhostNet, named by the Information Warfare Monitor in 2009, is one of the better-known examples of what's widely believed to be a PRC state-sponsored attack, but it wasn't particularly advanced or persistent. The method of infection was too basic – the Trojan was sent as an email attachment, which would have raised suspicions anyway. But 1,295+ computers across 100+ countries were infected by the Trojan, with foreign embassies and the exiled Tibetan government centres reportedly being the primary targets. Overall, a substantial amount of information would have been collected during a brief period, and that may have been enough for whoever was behind it. So, GhostNet wouldn’t have been an example of APT, unless it was being used for reconnaissance for another attack we don’t know of yet.

And what about the ACAD/Medre.A virus that was discovered just a few months ago? Its purpose was to exfiltrate AutoCAD files from several Peruvian companies, which means whoever was responsible was after ‘intellectual property’ instead of something immediately sellable. It was also distributed, it is believed, through infected AutoCAD templates.

Here it was interesting because the malware wasn’t crafty enough to evade detection – it sent blueprints autonomously to a couple of email accounts. The Chinese government also apparently co-operated in this case in defeating the malware.

Table of Contents

Executives advocate a military approach to cybersecurity

By Suzanne Kelly, CNN, 14 Aug 2012

A new study being released by a private Internet security company highlights cyberworld weaknesses when it comes to gathering intelligence on hackers and suggests that businesses take a more military-minded approach to defense.

The cybersecurity company CounterTack polled 100 information security executives at companies with revenues greater than $100 million. Nearly half of the respondents said their organization had been the victim of a targeted cyberattack within the past year.

Some 80% of those polled believe that taking a more military-minded approach to the cyberwar could benefit business, according to CounterTack CEO Neal Creighton, whose firm released the poll Monday. For Creighton, that means incorporating more military-style intelligence gathering into companies' cyberworld defenses.

"We're talking about that great intelligence real-time situational awareness," said Creighton, who added that hackers will get into systems, and when they do, companies need to know in real time not only that the intrusion has occurred, but also what the hacker's intentions are.

"Today's attacks are very targeted, so when they come after you, they probably have something that no one else has seen before, so what we're advocating is once they have penetrated the network, that you have technologies that look at behaviors based on what the attacker is going to do," Creighton said.

CounterTack is one of several companies in the private sector that focus on gathering information on the threat as it is happening as a key strategy for defense, in addition to building effective firewalls.

But the CounterTack survey, though not a scientific one, found that those capabilities are lacking.

Surveyed executives said their most pressing challenges when it comes to combating "advanced persistent threats are "disparate systems that don't talk to each other" (63%) and having trouble gathering relevant attack 'intelligence' in real time (61%).

Cybersecurity experts have often warned that by the time a company realizes it has been hacked, the damage has already been done.

When it comes specifically to the issue of training these new cyberwar soldiers, 44% of executives, according to the CounterTack study, said that their team members didn't have the necessary technical skills to combat the threat.

CounterTack has hired retired Admiral William Fallon, who has experience heading both U.S. Central Command and Pacific Command to help them in their push to get companies to focus on this military-minded approach.

Government is also making the case for better recruitment cyber warriors.

The head of U.S. Cyber Command, Gen. Keith Alexander, made a rare appearance at a hacker's conference in Las Vegas last month encouraging those with advanced cyber skill sets to put them to work for the U.S. government.

The Senate recently failed in its effort to pass basic cybersecurity legislation that would have allowed a closer public-private partnership when it comes to information sharing on cyberworld threats.

In light of that, the White House is mulling its options.

The President's homeland security adviser, John Brennan, suggested last week that the president may issue an executive order that would allow the government to use more of the tools it has on hand to combat the growing threat. Brennan added that such a measure would likely encompass a combination of resources from the Department of Homeland Security, the National Security Agency and the FBI.

Table of Contents

Dysinformatsia redux

By Arnaud De Borchgrave, UPI, Aug. 13, 2012

WASHINGTON, Aug. 13 (UPI) -- WASHINGTON, Aug. 13 (UPI) -- We are living in an age of fakery and fiction alongside reality and truth, concludes Huffington Post Books Editor Andrew Losowsky. The new Transmedia Project, he says, is part of a boundary-pushing genre that has so far kept to the edges of the mainstream.

These days, anyone with the skills can make a Web site that appears to be that of a major company.

A YouTube video can appear to show real events that are fabrication, enough to make aging KGB veterans of the old Soviet dezinformatsia -- a tissue of falsehoods weaved around a kernel of truth -- nostalgic. They go viral on the World Wide Web where they become part of our permanent institutional memory.

The Middle East today is a geopolitical kaleidoscope of information, misinformation and disinformation superimposed by a civil war in Syria, a shadow war of Israel versus Iran that may soon become a hot one that drags in the United States.

In Egypt's Sinai desert, the Egyptian army is hunting down pro-al-Qaida tribesmen who killed 16 Egyptian soldiers on the Israeli frontier. At least that is what Cairo media announced. But a National Public Radio correspondent dropped in on some of the Sinai's tribal settlements that were alleged targets and the jobless men told her they hadn't heard a single shot fired in anger.

Back in Cairo, Egyptian President Mohammed Morsi, the Muslim Brotherhood's standard bearer, fired the cumbersome military chief Field Marshal Mohamed Hussein Tantawi, 76, in the job 17 years, and his deputy Gen. Sami Anan.

The military still control roughly 40 percent of Egypt's economy and its leaders aren't about to return to barracks quietly.

In Syria, in February 1982, President Hafez Assad ordered his army to crush a rebellion in the city of Hama. In less than a week, the Syrian army killed 25,000. His son, President Bashar Assad, is at 19,000 killed after 19 months of civil war.

And the chorus of geopolitical and political voices demanding the United States intervenes to stop the killing and speed Assad's departure into exile -- or to meet his maker -- grow louder every day. But those who have served in or known Syria as frequent travelers for decades are urging caution.

Facebook and Twitter moved video showing insurgents throwing the bodies of slain Syrian soldiers off the roof of a post office in Al-Bab.

Al-Qaida terrorists in Iraq recently managed to attack 11 cities and towns the same day. Some of them have crossed the border into Syria and are posing as elements of either Free Syrian Army for Syrian Liberation Army. But this underground army is also an alphabet soup of Islamist brigades and groups of dubious origin.

Voices seeking U.S. military intervention emanate chiefly from Israel and its principal backers in Congress and the Obama administration. They see a geopolitical opportunity to kill two evils in one blow -- the Assad regime in Syria and its close ally Iran.

Syrian weapons of mass destruction are the main concern of policy makers. WMD in the regime's arsenal include nerve agents, mustard gas, radiological and biological instruments that can wipe out thousands of lives. Both Russia and China are standing by the Assad regime, presumably to deter anyone with similar ideas in their own countries.

U.S. President Barack Obama's critics offer up the successful NATO campaign in Libya as a precedent to emulate in Syria. But Libya, as one wit jested, "is a long beach dotted with oil wells and dozens of tribes that can't stand each other." Syria is a modern long-time client state of the Soviet Union before Russia inherited the only base Moscow has in the Mediterranean.

U.S. decision makers are also ever mindful of two recent engagements that didn't quite pan out the way they were planned. The $1 trillion spent on the Iraq war has given Iran more influence in Baghdad than the United States – despite the erection of a $1 billion new U.S. Embassy complex with some 1,200 diplomats and officials from various and sundry U.S. administrations.

Obama inherited the Afghan war and is winding it down. But the outlook for the planned 2014 exit is bleak. The ouster by Parliament of the two most powerful Afghan ministers -- Defense chief Gen. Abdul Rahim Wardak and Interior Minister Gen. Besmullah Mohammadi -- wasn't a good omen.

U.S. Marines and Army advisers to Afghan military and police units are being gunned down with alarming frequency by their trainees. Three such rogue operations in four days isn't a good omen for a peaceful NATO withdrawal by the end of 2014.

In one attack an Afghan police commander and several of his men killed three U.S. Marines after inviting them to a Ramadan breakfast to discuss security. Next day, an Afghan police officer killed 10 fellow officers for siding with the Americans.

This year, there have been 26 "green-on-blue" attacks on allied troops in seven months that killed 35, a sharp increase on the previous year with 21 attacks and the same number gunned down.

Taliban insurgents lost no time posting on Twitter the attacks "clearly summed up the mood of the Afghan nation toward foreign occupation."

Looming larger than Afghanistan is Iran -- and the distinct possibility that Israel may attack some of Iran's nuclear installations before year's end.

Presumptive GOP candidate Mitt Romney would applaud loudly and Obama would have no choice but to join the chorus. This would automatically bring the United States into the conflict as Tehran would then retaliate against U.S. targets in the Persian Gulf.

The U.S. State Department's Coordinator for Counter-terrorism Daniel Benjamin and the Treasury's Undersecretary for Terrorism and Financial Intelligence David S. Cohen coordinated statements to warn the world that Hezbollah in Lebanon had been training and advising the Syrian army.

But the opposite has been true for years. Syria occupied Lebanon from 1976-2005 and aided and abetted the creation of Hezbollah, a politico-religious organization that remains more dependent on Iran than on Syria.

With disinformation, misinformation, information, and propaganda, it is becoming increasingly difficult to sort fact from fiction. Newspapers are read on line these days but "read" is a gross exaggeration. Thousands of blogs and millions of tweets leave little time for newspapers. These continue to bleed with a shrinking readership of retirees.

Table of Contents

Hezbollah Under Attack

From Strategy page, 14 Aug 2012

August 14, 2012: Two months after American and Israeli officials finally confirmed that the industrial grade Cyber War weapons (Stuxnet, Duqu, and Flame) used against Iran in the last few years were indeed joint U.S.-Israel operations, yet another such Cyber War weapon has been detected. This one, called Gauss, appears concentrated in Lebanon (plus some infected machines in Israel and the Palestinian territories) and is seeking details on how Hezbollah gets its money and moves it around the international banking system. Hezbollah has long sustained itself via cash from Iran and a number legal (charities and businesses) and illegal (charities and criminal enterprises) sources. This would seem to indicate Israel has the author of Gauss, because Hezbollah is dedicated to the destruction of Israel (and gaining control over all of Lebanon).

The U.S. and Israel have not provided any details about their Cyber War activities, although many more rumors are now circulating. The U.S. and Israel were long suspected of being responsible for these "weapons grade" computer worms. Both nations had the motive to use, means to build, and opportunity to unleash these powerful Cyber War weapons against Iran and others that support terrorism.

The U.S. Department of Defense had long asked for permission to go on the offensive using Cyber War weapons. But the U.S. government regularly and publicly declined to retaliate against constant attack from China, mainly because there were fears that there could be legal repercussions and that weapons used might get out of control and cause a lot of damage to innocent parties. Now it's believed that the secret war has begun in earnest, including attacks against China.

Iran is another matter. Although not a serious Cyber War threat to the United States, Iran was trying to build nuclear weapons and apparently Israel had already been looking into using a Cyber War weapon to interfere with that. Given the nature of these weapons, which work best if the enemy doesn't even know they exist, don't expect many details to be released about this Cyber War program. What is known is that the Cyber War weapons unleashed on Iran were designed to concentrate only on very specific targets. So far, only three weapons that we know of have been used. One (Stuxnet) was designed to do damage to one specific facility, the plant where Iran produced nuclear fuel for power plants and atomic weapons. That one worked. The other two (Duqu and Flame) were intelligence collection programs. They also apparently succeeded, remaining hidden for years and having lots of opportunity to collect enormous quantities of valuable data.

It was only in the last few months that the latest of these Cyber War "super weapons" were uncovered. First there was Flame, which was designed to stay hidden and collect information from computers it got into. It apparently did both, for up to five years (or more), in Iran, Lebanon, the Palestinian West Bank, and, to a lesser extent, other Moslem countries in the region. Like the earlier Stuxnet (2009) and Duqu (2011), Flame has all the signs of being designed and created by professional programmers and software engineers. Most malware (hacker software) is created by talented and, often, undisciplined amateurs and usually displays a lack of discipline and organization. Professional programmers create more capable and reliable software. That describes Stuxnet, Duqu, Flame and Gauss. The U.S. and Israel spent big bucks to craft these Cyber War weapons and get them to their targets. Both nations have access to the best programming talent on the planet and already have organizations that can recruit and supervise highly secret software development.

As researchers continue studying these four software packages, they find ever more surprising features. Until the appearance of Flame and Gauss, the most formidable Cyber War weapon encountered was Stuxnet, a computer worm (a computer program that constantly tries to copy itself to other computers) that showed up two years ago. It was designed as a weapons grade cyber weapon and was designed to damage Iran's nuclear weapons manufacturing facilities. It succeeded. A year after Stuxnet was discovered (in 2010), security experts uncovered Duqu. Like Flame, Duqu was collecting information on large computer networks and apparently preparing for an even broader attack on industrial targets.

It appeared that Stuxnet and Duqu were but two of five or more Cyber War weapons developed (up to five years ago) from the same platform. Flame was not apparently related to Stuxnet and Duqu. The basic Flame platform appears to have been built to accept numerous additional software modules, giving each variant different capabilities. Some of the modules made use of specific computer features, like a microphone, wireless communication, or the camera. Flame appears to be a very different design from Stuxnet and Duqu but also spreads via a USB memory stick or the Internet.

Gauss shows many signs of being from the same organization that created the other three Cyber War viruses. All have the same high level of craftsmanship and organization. No hasty, if somewhat inspired hacks here. This is carefully planned and executed software.

For over two years now, hundreds of capable programmers have been taking Stuxnet and Duqu apart and openly discussing the results. While these programs are "government property", once they are turned loose they belong to everyone. The public discussion on the Internet has provided a bonanza of useful criticism of how the programs were put together, often describing in detail how flaws could be fixed or features improved. But even when such details were not provided, the programmers picking apart these programs usually mentioned what tools or techniques were needed to make the code more effective.

On the down side, this public autopsy of this stuff makes the inner workings of the software, and all the improvements, available to anyone. Then again, security professionals now have a much clearer idea of how this kind of weapon works and this can make future attempts to use similar weapons more difficult.

Weapons like Stuxnet and Duqu are nothing new; for nearly a decade Cyber War and criminal hackers have planted programs ("malware") in computer networks belonging to corporations or government agencies. These programs (called "Trojan horses" or "zombies") are under the control of the people who plant them and can later be used to steal, modify, destroy data, or shut down the computer systems the zombies are on. You infect new PCs and turn them into zombies by using freshly discovered and exploitable defects in software that runs on the Internet. These flaws enable a hacker to get into other people's networks. Called "Zero Day Exploits" (ZDEs), in the right hands these flaws can enable criminals to pull off a large online heist or simply maintain secret control over someone's computer. Flame was apparently using high-quality (and very expensive) ZDEs and possibly receiving new ones as well.

Stuxnet contained four ZDEs, two of them unknown, indicating that whoever built Stuxnet had considerable resources. ZDEs are difficult to find and can be sold on the black market for over $250,000. The fact that Stuxnet was built to sabotage an industrial facility spotlights another growing problem - the vulnerability of industrial facilities. The developers of systems control software have been warned about the increased attempts to penetrate their defenses. In addition to terrorists, there is the threat of criminals trying to extort money from utilities or factories with compromised systems, or simply sniff around and sell data on vulnerabilities to Cyber War organizations. But in the case of Stuxnet, the target was Iran's nuclear weapons operation, although some hackers dissecting Stuxnet could now build software for use in blackmail schemes.

Stuxnet was designed to shut down a key part of Iran's nuclear weapons program, by damaging the gas centrifuges used to enrich uranium to weapons grade material. Iran eventually admitted that this damage occurred and recent Western estimates of how soon Iran would have a nuclear weapon have been extended by several years. So, one can presume that Stuxnet was a success.

Duqu appears to be exploiting the success of Stuxnet in spreading to so many industrial sites and is designed to sniff out details of places it ends up in and send the data to whoever is planning on building Stuxnet 2.0. Several different versions of Duqu have been found so far, and all of them have been programmed to erase themselves after they have been in a computer for 36 days.

Stuxnet was believed to have been released in late 2009, and thousands of computers were infected as the worm sought out its Iranian target. Initial dissection of Stuxnet indicated that it was designed to interrupt the operation of the control software used in various types of industrial and utility (power, water, sanitation) plants. Eventually, further analysis revealed that Stuxnet was programmed to subtly disrupt the operation of gas centrifuges.

The Stuxnet "malware" was designed to hide itself in the control software of an industrial plant, making it very difficult to be sure you have cleaned all the malware out. This is the scariest aspect of Stuxnet and is making Iranian officials nervous about other Stuxnet-type attacks having been made on them. Although Iran eventually admitted that Stuxnet did damage, they would not reveal details of when Stuxnet got to the centrifuges nor how long the malware was doing its thing before it was discovered and removed. But all this accounts for the unexplained slowdown in Iran getting new centrifuges working. Whoever created Stuxnet probably knows the extent of the damage because Stuxnet also had a "call home" capability.

The U.S. and Israel have been successful with "software attacks" in the past. This stuff doesn't get reported much in the general media, partly because it's so geeky and because there are no visuals. It is computer code and arcane geekery that gets it to its target. The earlier attacks, especially Stuxnet, Duqu, Flame and Gauss, spread in a very controlled fashion, sometimes via agents who got an infected USB memory stick into an enemy facility. Even if some copies of these programs get out onto Internet connected PCs, they do not spread far. Worms and viruses designed to spread can go worldwide and infest millions of PCs within hours.

Despite all the secrecy, this stuff is very real and the pros are impressed by these high-grade Cyber War weapons, even if the rest of us have not got much of a clue. The demonstrated capabilities of these Cyber War weapons usher in a new age in Internet based warfare. Amateur hour is over and the big dogs are in play. Actually, the Cyber War offensive by the U.S. and Israel appears to have been underway for years, using their stealth to remain hidden. There are probably more than three of these stealthy Cyber War applications in use, and most of us will never hear about it until, and if, other such programs are discovered and their presence made public.

Table of Contents

For Army's Electronic Warriors, Greater Foes than Afghanistan's Await

By Sebastian Sprenger, InsideDefense.com, August 3, 2012

While the Army's electronic-warfare specialists have managed to gain the upper hand in countering remote-controlled bombs buried by insurgents in Afghanistan, those experiences may count little in predicting how the ground service would fare in future conflicts covered under the Air-Sea Battle doctrine, according to experts and officials.

The electromagnetic spectrum is one of the domains in which the U.S. military is able to operate at will against poorly equipped insurgents in Iraq and Afghanistan. Still, despite a large investment in hardware, it took years to make the technology for jamming remote-controlled detonators useful enough that enemy fighters turned instead to mechanical triggers for their explosives.

Army Col. Jim Ekvall, chief of the service's electronic warfare division, said commanders in Afghanistan have reported a "marked decrease" in radio-frequency IEDs, although insurgents still sometimes "get lucky" with them.

A factor in that success may be that fighters in the impoverished country have not tried to use the electromagnetic spectrum to their advantage. Instead, U.S. forces have developed methods to not only jam IEDs, but to detect and disrupt enemy cell phone and radio communications with great precision, Ekvall told Inside the Army in an Aug. 1 interview.

However, in the Pentagon's new Asia strategy, in which China is the proverbial elephant in the room, that may not be so easy. "When you have millions of dollars and a world of technology ahead of you, such as we might have in the Pacific Rim, I can't begin to tell you the advances they made in the last 10 years," Ekvall said. "I suspect they are probably fairly [commensurate] with the advances that we made in the last 10 years."

Ekvall has been touting the Army's Integrated Electronic Warfare System as a key capability for ground commanders. Asked about the impact of the Pentagon's new Asia strategy on the program, he argued the system is needed "immaterial of the enemy we face."

Over the last year, the system has left the concept stage and is moving toward a milestone A acquisition decision scheduled for the first quarter of fiscal year 2013, Ekvall said. The system is envisioned as a suite of ground-based and aerial electronic-attack tools. A complementary planning and management tool is also in development. Officials hope that portion of the program can enter the acquisition process at milestone B, according to Ekvall.

After years of ad hoc solutions and systems provided to the ground service by the Navy, IEWS would be the first dedicated Army program.

"For the most part, in Iraq and Afghanistan, our primary adversary in the electrons has been ourselves," Peter Singer, who directs the 21st Century Defense Initiative at the Brookings Institution, said in an interview. Singer was referring to instances of powerful electronic-warfare equipment disabling the communications gear of nearby units or even knocking out electronic systems in hospitals and other civilian facilities.

In the case of IEDs, insurgents used "old technology in a new way," Singer said. With an eye toward the Pacific, state powers in that region could well employ "new technology in a novel way," thus surprising U.S. strategists, he said.

Defense officials have long acknowledged DOD's vulnerabilities would increase as technology formerly considered military-grade proliferates around the world. According to Ekvall, the Army has done well in anticipating technologies that could one day pose a threat, and devising countermeasures. Verifying such claims is nearly impossible, as they rely on classified intelligence and secret defense planning scenarios.

Ekvall said future adversaries may possess the ability to degrade at a large scale the GPS signal on which many U.S. systems rely for navigation and targeting. But, he added, "Will they be able to exploit it to their advantage? I don't think they will be able to easily."

One electronic-warfare technology has repeatedly been the subject of recent correspondence with Congress. In a February reprogramming request Pentagon Comptroller Robert Hale asked for a plus-up of $38 million for the Army's Integrated Air and Missile Defense (IAMD) program. The extra money is needed to conduct "detail digital radio frequency modulation (DRFM) countermeasures studies and simulations" to address "this threat change," Hale wrote.

The reprogramming request describes DRFM as an "emerging sophisticated threat capability that will be faced by several Army air-defense systems," including Patriot and Sentinel radars. U.S. Pacific Command initiated the funding request, Hale wrote.

The technology for DRFM has been around since the 1980s, according to Air Force Maj. Randel Gordon of the Future Capabilities Division in PACOM's J-8 branch. It can jam radars, essentially disabling them. It can also trick them, which is called spoofing. "We've only really seen [interest in the technology] from a nation-state kind of level," Gordon said in an interview.

At least one research paper found online -- purportedly written by a Chinese doctoral candidate in information technology -- discusses the application of DRFM to jam synthetic aperture radar systems with a ground moving target indicator functionality.

There is no guarantee that a U.S. system is invulnerable to DRFM attacks, Gordon said. Similar to the counter-IED business of bigger bombs and bigger armor, the development of new radar attack methods and countermeasures is a cycle of "continuous escalation," he said. "I don't think anything we have is 100 percent immune to anything."

An Army spokesman declined to comment for this article, saying information on the topic of the DFRM and the specific systems outlined in Hale's reprogramming request is classified. A spokeswoman for Raytheon, the maker of Patriot and Sentinel, said industry is "aware of the jammer technology that exists and is continually working to improve performance to counter it."

Gordon, the PACOM official, acknowledged his command's concerns with DRFM are based on the assumption that other countries have the technology given its worldwide proliferation. No attacks on U.S. systems have actually been observed, he said. Unlike in cyberspace, where aggressive actions are constant, DRFM attacks would be discrete events, playing out most likely during "some kind of kinetic activity," Gordon explained.

The possibility of such kinetic activity, particularly involving China, has spawned a major debate within DOD. Some in the Army have pushed back against the Air-Sea Battle concept, arguing it contributes to a path of escalation in America's dealings with Beijing.

An internal assessment prepared for the Marine Corps commandant, as reported by The Washington Post last week, warned that "an Air-Sea Battle-focused Navy and Air Force would be preposterously expensive to build in peace time" and would lead to "incalculable human and economic destruction" in a war with China.

Table of Contents

Cyber Command Struggles To Define Its Place On A Shifting Battlefield

By Aliya Sternstein, NextGov, 16 Aug 2012

The U.S. Cyber Command, which directs network offensive operations for the Pentagon and protects its networks, is becoming more open about the military’s capabilities in cyberspace. Recently, the Defense Department was forced to show part of its hand when leaks surfaced about U.S.-manufactured cyber weapons and cyber espionage missions. Still, since 2011, the department has told the world it stands prepared to protect U.S. national security interests through cyberspace maneuvers.

With intrusions becoming ever more frequent and public—Defense and the Office of the Director of National Intelligence have called Chinese hackers a continuing and concerning threat—the military is focusing its constrained budgets on cyber. The Pentagon in January announced a spending strategy that switches priorities from ground wars in the Middle East to the Asia-Pacific maritime region and cyber operations.

But a cyber fighter shortage and the U.S. force’s dedication to civil liberties may be dragging down the agenda.

Cyberspace demands a new breed of warrior whose skills are scarce even by private sector standards. Troop size aside, cyber weapons could backfire on U.S. civilians, because of the amorphous nature of the cyber domain. And the very idea of an Internet corps scares the people Cyber Command aims to protect: Americans who value free speech and free markets.

The Pentagon is cognizant of the staffing, privacy and security challenges of mobilizing in cyberspace, current and former military officials say. Defense knows the competition for able cyber professionals presents a hurdle, but the command stands ready to vie for them using special incentives. The extras that Gen. Keith Alexander, head of Cyber Command, has mentioned include bonuses like the ones pilots and nuclear officers receive, as well as opportunities for education and advanced degrees.

Operations online likely will require a combination of physical and mental acuity if the recent Stuxnet campaign is any indication. The U.S.-Israeli-engineered computer virus that reportedly seized Iranian nuclear centrifuges was inserted manually through a jump drive, rather than propagated over the Internet from a safe distance. The Pentagon plans for cyber specialists from the Air Force, Army, Marines and Navy to coordinate with Cyber Command headquarters in Maryland on executing operations abroad, according to Alexander.

“One of the challenges is finding and holding the people we need to do this mission. We have to recruit, train and retain a cyber cadre that will give us the ability to operate effectively in cyberspace for the long term,” Cyber Command spokesman Col. Rivers J. Johnson Jr. says. “Gen. Alexander has indicated that it is going to take time for us to generate the force,” Johnson says, adding the Cyber Command chief is optimistic he eventually will get the specialized force desired.

Once troops are in place, activating them may require patience, due to the risk of accidentally unleashing viruses into the wild. The Flame worm, a suspected U.S. government invention, has long been harvesting information from computers in Middle Eastern countries using a compromised Microsoft product. Microsoft had to block three of its own digital certificates to stop less well-intentioned programmers from exploiting the weakness. Stuxnet, which undermined a computer system that operated nuclear plant equipment, could theoretically ram other Iranian infrastructure, such as civilian water utilities, for instance.

Another complication with an armament such as Flame is the potential for eavesdropping on communications between innocents. Kaspersky Labs, the security firm that discovered the cyber spy tool, describes the bug as “the largest cyber weapon to date,” referring to its 20 megabytes. The worm can scoop up massive amounts of valuable information such as screen shots of online chats, audio recordings from internal microphones and storage files. Many American privacy activists and foreigners are nervous about proposed legislation that would let U.S. intelligence and military communities scan citizens’ correspondence for signs of illicit activities and viruses embedded by nation state actors.

Both big business and human rights activists—not always best friends—are largely on the same side about any government regulations that demand sensitive information in return for greater computer protections. As much as civil libertarians would like the United States to facilitate the free flow of information in oppressive regimes, they aren't so eager if it means monitoring all digital messages to find the bad guys.

Yet, on the whole, some former government hackers say they've been surprised to see the Obama administration taking considerable care to minimize such civil liberties and cybersecurity risks. Recently uncovered attacks have involved "techniques that could have been used against us just as effectively," says Dave Aitel, chief executive officer of cybersecurity firm Immunity Inc. and a former National Security Agency computer scientist. He was referring to the chance of a cyber backlash if adversaries figured out how to apply the same tactics against U.S. citizens.

The order to implant the Stuxnet virus reportedly was made after thorough deliberation by the highest power in U.S. government—and not a Pentagon official. Defense's strategy for operating in cyberspace states the commander in chief has the ultimate say-so to engage in confrontations. "Obama has to say yes or no," Aitel says. "It's not completely like 'Go crazy, Cyber Command.' "

Pentagon officials have said they strongly respect Americans' rights during operations. Defense spokeswoman Lt. Col. April Cunningham says, "DoD is committed to protecting the individual privacy of communications on the Internet and the civil liberties of the American people."

Retired Gen. John P. Casciano, a former Air Force director of intelligence, surveillance and reconnaissance, says the U.S. government will never have 100 percent assurance that a cyber offensive will work as planned. Americans, however, have more to fear from adversaries and cyber crooks than from feds. "I'm not terribly concerned about the U.S. government spying on us," says Casciano, now a private consultant.

Some former Defense officials say cyber weapons are subject to the 1978 Foreign Intelligence Surveillance Act, which regulates the monitoring of U.S. international communications during counter-espionage activities. "All new cyber weapons must adhere to all the U.S. federal laws," says retired Air Force Lt. Gen. Harry Raduege Jr. Or, more specifically, "it's U.S. people who employ cyber weapons who are subject to FISA. It's really the people." Raduege is now chairman of the Deloitte Center for Cyber Innovation.

Casciano says he trusts the current legal framework will protect Americans in cyberspace.

Many civil liberties activists have argued otherwise, based on their long-standing criticism of FISA for sweeping up Americans' calls, emails and text messages. Flame so far has spread in a controlled manner among certain nation-state groups and academic institutions and has not self-replicated, according to Kaspersky researchers.

Jeffrey Carr, a cybersecurity consultant and author of Inside Cyber Warfare (O'Reilly Media, 2009), makes a distinction between cyber weapons intended to destroy systems such as Stuxnet, and cyber espionage tools such as Flame that compromise systems. With cyber weapons, collateral damage could harm civilians who use a targeted network, he says. "How do we know which networks should be targeted and which ones should be off limits?" he says. "I would think that [U.S. officials] would be concerned about their rules of engagement."

Cunningham notes the Pentagon does not discuss operational matters as a manner of long-standing policy and will not comment specifically on the development of cyber offensive tools. But she says, "DoD will organize, man, train and equip for operating effectively in cyberspace. DoD is in the process of developing the organizations, processes and procedures to ensure that the [combatant commands] have the appropriate cyber force structure and capabilities to operate effectively in their theaters."

Table of Contents

Pursuing Soft Power, China Puts Stamp on Africa's News

By Andrew Jacobs, New York Times, August 17, 2012

NAIROBI, Kenya - China's investment prowess and construction know-how is widely on display in this long-congested African capital. A $200 million ring road is being built and partly financed by Beijing. The international airport is undergoing a $208 million expansion supported by the Chinese, whose loans also paid for a working-class housing complex that residents have nicknamed the Great Wall apartments.

But Beijing's efforts to win Kenyan affections involve much more than bricks and concrete. The country's most popular English-language newspapers are flecked with articles by the Chinese state news agency, Xinhua. Television viewers can get their international news from either CCTV, the Chinese broadcasting behemoth, or CNC World, Xinhua's English-language start-up. On the radio, just a few notches over from Voice of America and the BBC, China Radio International offers Mandarin instruction along with upbeat accounts of Chinese-African cooperation and the global perambulations of Chinese leaders.

"You would have to be blind not to notice the Chinese media's arrival in Kenya," said Eric Shimoli, a top editor at Kenya's most widely read newspaper, The Daily Nation, which entered into a partnership with Xinhua last year. "It's a full-on charm offensive."

At a time when most Western broadcasting and newspaper companies are retrenching, China's state-run news media giants are rapidly expanding in Africa and across the developing world. They are hoping to bolster China's image and influence around the globe, particularly in regions rich in the natural resources needed to fuel China's powerhouse industries and help feed its immense population.

The $7 billion campaign, part of a Chinese Communist Party bid to expand the country's soft power, is based in part on the notion that biased Western news media have painted a distorted portrait of China.

"Hostile international powers are strengthening their efforts to Westernize and divide us," President Hu Jintao wrote this year in a party journal. "We must be aware of the seriousness and complexity of the struggles and take powerful measures to prevent and deal with them."

Beijing's bid to provide a counterpoint to Western influence, however, is raising alarms among human rights activists, news media advocates and American officials, who cite a record of censorship that has earned China a reputation as one of the world's most restrictive countries for journalism.

"We are engaged in an information war, and we are losing that war," Secretary of State Hillary Rodham Clinton warned a Congressional committee last year, citing the growing influence of state-backed outlets like Russia Today and CCTV.

Many fear that the impact of China's news media juggernaut will be especially pronounced in countries where freedoms are fragile. In Venezuela, China is building and financing communications satellites for a government that has exercised increasing control over the news media. Similarly, the Ethiopian government received $1.5 billion in Chinese loans for training and technology to block objectionable Web sites, television and radio transmissions, according to exile groups.

"The Chinese are not interested in bringing freedom of information and expression to Africa," said Abebe Gellaw, a producer for Ethiopia Satellite Television, an exile-run network whose broadcasts are frequently jammed by Chinese equipment. "If they don't provide these freedoms to their own citizens, why should they behave differently elsewhere?"

Chinese news media officials say such fears are overblown.

"Xinhua is filing hundreds of stories every day for our English service, and these reports are not propaganda," Zhou Xisheng, the agency's vice president, said in an interview. "What really matters is which perspective you are coming from."

The Chinese government has allowed some independent and investigative journalism in recent years. But Xinhua and CCTV - both of which answer to the Communist Party's propaganda ministry - retain a monopoly on all international news. And domestically, when it comes to politically delicate subjects like Tibet, jailed dissidents or the maneuvering for power among the party's top leaders, Xinhua and CCTV have glaring blind spots.

CCTV America provided only very limited coverage of the Bo Xilai scandal or the drama surrounding Chen Guangcheng, the blind activist who took refuge in the American Embassy in Beijing and later made his way to the United States.

"The fundamental difference is that Western-style media views itself as a watchdog and a protector of public interests, while the Chinese model seeks to defend the state from jeopardy or questions about its authority," said Douglas Farah, a senior fellow at the International Assessment and Strategy Center in Washington.

At home, Chinese officials make little effort to conceal their view of journalism as a servant of the Communist Party. "The first social responsibility and professional ethic of media staff should be understanding their role clearly and being a good mouthpiece," Hu Zhanfan, the president of CCTV, said in a speech. "Journalists who think of themselves as professionals, instead of as propaganda workers, are making a fundamental mistake about identity."

China's lavishly financed news media expansion is also aimed at making inroads in the West. Last year, Xinhua christened its new North American headquarters in a Manhattan skyscraper and emblazoned its logo on a sign in Times Square. In February, CCTV opened a production center in Washington with 80 journalists. The anchors are mostly non-Chinese, as are the correspondents, who report from cities across North and South America.

CCTV News, which claims 200 million viewers outside China, is now available in six languages; one of its latest ventures is an Arabic news channel. To increase its reach - and compete with Western news organizations -

Xinhua often gives away dispatches to financially struggling news media outlets in Africa, Latin America and Southeast Asia.

At the same time, governments in Europe and the United States are scaling back support for independent journalism in the developing world, even as most private broadcasters and newspapers have closed foreign bureaus.

The overseas newscasts of CCTV have shed the shrill ideological bombast of the Maoist years, adopting the professionalism and slick production values of their Western counterparts. But ideology often still trumps impartiality. During the protests that wracked the Arab world, for example, China's coverage strenuously avoided the word "democracy" and emphasized the chaos that accompanied the demise of authoritarian governments, news media analysts say.

In a widely circulated blog post during the early days of the uprising in Libya, Ezzat Shahrour, the Beijing bureau chief for Al Jazeera Arabic, complained that Chinese coverage was faithfully relaying the propagandistic outbursts of Col. Muammar el-Qaddafi. "Every time I see Chinese media reports on the Arab revolution I feel like my blood pressure is starting to rise," he wrote.

CCTV and Xinhua coverage of the unrest has since become more evenhanded. But they still find plenty of occasions to echo Beijing's view of the advantages of single-party rule.

When pitching their services in Africa, Chinese officials stress what they see as Western bias.

"Although they are geographically far apart, China and Africa have long learned about each other through Western media," Li Changchun, the propaganda chief, said during a seminar with African news media executives. "However, Western reports did not always reflect the truth."

Chinese news media officials chose to set up shop in Nairobi because of its role as a news hub for the English-speaking countries in East Africa. So far, the Chinese have made only limited headway against Kenya's domestic newspapers and radio and television stations.

Vivien Marles, managing director of InterMedia Africa, a research firm here, said that Kenyans remained devoted to a vibrant news media menu of local politics, scandal and pop culture. Those interested in international affairs, she said, generally turn to CNN, the BBC or Al Jazeera. But China Radio International is "gaining some momentum," she said.

But in their eagerness to see their articles and photographs in circulation, the Chinese sometimes come across as overbearing. Since signing the news-sharing agreement with Xinhua, editors at The Daily Nation say they have been peppered with phone calls, e-mails and even visits to the newsroom from Xinhua officials pressing them to print articles and photographs.

"To be honest, how many photographs of Chinese children doing martial arts or soldiers rescuing flood victims can I run?" asked Joan Pereruan, a photo editor.

Still, she and other editors agreed that Xinhua had improved substantially, hiring scores of local journalists for its 23 bureaus in Africa.

Across town at the Standard Group, which owns two newspapers as well as a TV and radio station, Woka Nyagwoka, a managing editor, praised the Chinese construction projects but said many editors were reluctant to rely on the Chinese news media for foreign news, particularly from places like Sudan, where Beijing supports the brutal government of Omar Hassan al-Bashir. "Kenyans are skeptical of a free lunch," Mr. Nyagwoka said. "Especially when it's made in China."

Table of Contents

Pakistan's Army Steps Up Radio Wars

By Aijaz Maher, BBC, 14 August 2012

The army is considered to be one of Pakistan's shrewdest commercial operators, running bakeries, factories and even expanding into tourism.

It has been bitterly criticised for aggressively pursuing such lucrative ventures, but its latest foray into the corporate world may be of some use to its battle against militancy in Pakistan's restive north-west.

The army has a radio station - FM 96 was set up to counter militant propaganda in the Swat Valley, but it is now expanding its broadcasts into the semi-autonomous tribal belt.

Many in Pakistan are still suspicious of the power of the military, which has ruled the country for more than half of its history.

But Pakistan's far north-west presents a particularly intractable challenge - it is a region renowned for its complex rivalries, power struggles and the changing loyalties of various tribal groups.

'Mullah Radio'

FM 96 was first set up around the time that the army launched a huge military offensive to win back control of Swat from the Taliban, which had swept to power in the once peaceful and lush valley. The Taliban had been running radio stations for some time - the brainchild of notorious Taliban cleric, Maulana Fazlullah.

Known as "Maulana Radio", Fazlullah used to run a network of FM frequencies in the region to preach extremist Islamic views. The stations aired Islamic programmes and sermons of religious leaders. Appeals for donations were regularly made.

The same phenomenon can be witnessed in Afghanistan, where the Taliban broadcast from makeshift radio stations.

"Pakistan's state institutions decided to respond to the propaganda aired by Maulana Fazlullah in Swat. For security reasons it was not possible to do it without the army's involvement," says FM 96's chief executive Aqeel Malik, who is also a serving officer of the Pakistani army.

Although the army eventually triumphed, driving militants out and allowing the many thousands who fled their repressive regime to return, it was not long before the army itself stood accused of abuses such as extra-judicial killings.

The army strenuously denied all such accusations, but mistrust between the security forces and the population has lingered.

The region is still at the centre of a propaganda duel as Maulana Fazlullah was never caught and militants continue to broadcast propaganda from a number of radio stations.

The army's radio station seeks to soften the image of the all-powerful security forces and the army is clearly hoping it can extend this image to the tribal areas.

It says FM 96 is simply there to provide people with entertainment and information. But experts say the main focus of the station is to reach areas where militants have more influence than the army itself - even if it is through the lilting melody of a Bollywood love song.

Reaching out

These areas include Pakistan's semi-autonomous tribal belt and parts of the province of Balochistan.

Simply being present in people's lives in such places is enough, observers contend. From its studios in Islamabad, the army is now broadcasting to 16 cities and towns in areas where militants once held power - including Swat and Malakand. The army has plans to expand this coverage to 44 cities.

Current affairs content features in the broadcasts, but most radio time is taken up by entertainment shows. Live callers are frequently encouraged to phone in and request songs and this has boosted the station's popularity.

Ironically, for an army which has for decades been preoccupied by the perceived threat from India, the choice of music for FM 96 is Bollywood's latest hits.

Hakeem Zada, who lives in the north-west of the country, listens to the station's morning show called Informed Morning.

"This show discusses our everyday problems like power outages and inflation. I like to contribute to the discussions and try to highlight my area. This is a really good show," she says.

But critics including author Ayesha Siddiqa have wasted no time in branding the broadcasts an army publicity stunt intended to boost the military's commercial interests. Many argue such interests are problematic in a country where the military often appears to be in unacknowledged conflict with the civilian government.

In a country with a history of frequent military coups, such critics are sensitive to such military ventures.

Army empire?

Dr Siddiqa's influential book, Military Inc, details the army's commercial interests.

"They are not planning more than 50 such channels for nothing. They are definitely using it for propaganda," she said.

"Who knows what they'll say on these channels against the Pakistani government or even neighbouring countries?"

Dr Siddiqa points out that when the military recently launched its own transport fleet, senior officers argued that it was only for military purposes.

"But later it spread to the extent that it took over most of country's cargo movement, throwing the national rail service into huge losses."

The army strongly denies these claims. Col Malik argues that FM 96 is being run on a non-profit basis. But he admitted that there were plans to expand the station.

For callers to the phone-in shows, however, these arguments are somewhat prosaic. For them, it is the entertainment that matters most, although many still talk about security.

"I hope and pray that situation in our valley improves significantly and quickly," an unidentified caller tells the host during one live programme.

FM 96 may be gaining ground in troubled parts of country, but it is far from certain if that is sufficient to win the loyalty of people under pressure in Pakistan's volatile tribal belt.

Table of Contents

Pakistani Bloggers Accused of Hate Videos

From UPI, Aug. 20, 2012

NEW DELHI, Aug. 20 (UPI) -- Doctored videos showing apparent violence against Muslims in Assam that created panic originated on Pakistani blogs, an Indian minister said.

Union Home Secretary R.K. Singh told The Times of India newspaper that the government believes most of the incendiary videos of atrocities allegedly committed on Muslims in the state of Assam as well as in Myanmar came from Pakistan.

"Technical investigation has established that a bulk of the incendiary images was first uploaded on blogs in Pakistan," he said.

He said the object was to incite inter-ethnic violence within India and New Delhi will be raising the issue with Pakistani officials.

"I am sure they (Pakistan) will deny it but we have fairly accurate technical evidence to show that the images originated and were circulated from their territory," he said.

"As many as 110 Web sites were involved in spreading the doctored clips. We have blocked 76 of them and are in the process of getting others deactivated," he said.

The government also is seeking cooperation from Google and other Internet search engines, Singh said.

Last week federal and state ministers as well as police authorities held their breath as Assamese Muslims living and working in Bangalore engulfed the train station after rumors of the Web site information swept through their community.

Rail authorities and train companies in Bangalore, in the southwest state of Karnataka, put on extra trains to Assam in the northeast to cope with the influx of people who said they feared an outbreak of ethnic violence.

The Times of India reported that some of the Web sites had doctored images of death and destruction caused by a cyclone to appear as if the carnage was the result of an attack on Muslims in Assam.

In other videos, bodies of victims of an earthquake that occurred months ago were altered to make it appear the people had been killed by Buddhist monks, the newspaper reported.

A report by The Hindustan Times quoted Assam Chief Minister Tarun Gogoi saying he suspected "from the very beginning that foreign forces were behind this."

"It is not merely a clash between (the ethnic group) Bodos and minorities. The Union Home Ministry report that Pakistani elements were involved has vindicated our stand," Gogoi told the Press Trust of India.

"We will institute a probe to find out details regarding the involvement of foreign elements in the violence," Gogoi said.

Despite the tensions created by the Web sites, little violence was attributed to the videos.

However, some people from the northeast have been attacked in the cities of Pune in Maharashtra state and Hyderabad in Andhra Pradesh state. A Tibetan was stabbed in Mysore in Karnataka in what appeared to be a case of retaliation against alleged brutalities on Muslims, The Times of India said.

Last week Indian Prime Minister Manmohan Singh immediately called for calm as soon as the problem became known.

"All political parties must work together to give a feeling of confidence to all affected people," he told reporters at his residence in Delhi during an Iftar event -- the evening meal when Muslims break their fast during the Islamic month of Ramadan.

Thousands of people flocked to Bangalore's main train station demanding tickets back home. One day along, more than 2,000 tickets more than usual were sold to people traveling to Guwahati, the largest city in Assam.

The situation at the city railway station was chaotic as thousands of people from northeastern India and Nepal, Bhutan and Tibet nationals thronged to get tickets, The Times of India report said.

Assam, similar to other states in India's remote northeast, has an ongoing conflict between the government and several rebel groups which are demanding more autonomy or independence.

Table of Contents

The Return of Dr. Strangelove

By Jan Kallberg & Adam Lowther, the Diplomat, August 20, 2012

How fiscal austerity will push the United States towards nuclear arms and cyber-warfare.

With the prospect of sequestration looming, the United States may find itself increasingly relying on nuclear and cyber deterrence as an affordable means of guaranteeing national sovereignty and preventing major conflict between the U.S. and potential adversaries in the Asia-Pacific. While earlier defense planning and acquisition were based on economic conditions that no longer exist, Congress's options to balance the budget by cutting defense spending are politically palatable because far fewer American are "defense voters" relative to "social welfare voters," according to a number of recent public opinion surveys.

The simple fact is China's rise has yet to present a clear danger to American interests in the minds of most Americans.

The first steps in this process are already underway and exemplified by the administration's new strategy – published in January 2012. When the official requirement that the Department of Defense (DoD) be able to fight two major wars simultaneously disappeared, an opportunity to downsize the armed forces presented itself. From Congress's viewpoint, the budget crisis must be solved without unseating its members. Ironically, austerity may cause Americans to stop worrying about a hypothetical rogue detonation and learn to love the bomb. Dr. Strangelove may return with a vengeance, but this time with a cyber doomsday device under one arm and its nuclear counterpart under the other. After all, dollar for dollar, nuclear weapons—in particular—provide American taxpayers the greatest level of security and stability of any weapon the nation has ever fielded. The fact that at an estimated $30 billion per year—5% of the defense budget—the nuclear arsenal is cheap, may spur Congress to take a pragmatic position toward the nation's most powerful military capabilities (as the federal budget is increasingly engulfed by social welfare programs) and support an effective nuclear deterrent along with the development of devastating cyber capabilities.

It is important to keep in mind that both areas—nuclear and cyber—are a primary focus of Chinese military developments. Failing to maintain an advantage in both may prove unwise for the United States.

Some in the scientific community argue that this perspective is unrealistic. Politics, being what they are, is all about getting elected; complex strategic calculations in the Asia-Pacific offer little comfort during a tough reelection fight that is focused on the domestic economy. With Congress having a number of incumbents whose constituencies loathe the thought of cuts to Medicare, Medicaid, Veterans' benefits, and Social Security, taking greater risks in national security is a more tangible option. As the nation borrows over $1 trillion per year, the quest to balance the budget is impossible without dramatic spending cuts given the unacceptability of tax increases.

The nation's deficit crisis may soon turn the United States' geopolitical posture from one that is ideologically based on global interventionism—popular with both Republicans and Democrats—to one more akin to defense non-intervention. While international trade will continue and expand, the United States may cease to be a shining city upon a hill and the global policeman. It is somewhat paradoxical that after the country demonstrated overwhelming conventional superiority in the last two wars—Afghanistan and Iraq—the cost of that capability may lead to a renaissance of nuclear deterrence and the development of cyber deterrence as a strategic policy, a move that may be more useful in an "Asia-Pacific century" than many realize. In comparison to large conventional forces and the decades of veteran's benefits that follow, the nuclear arsenal is far more affordable over the long term. Cyber is also more cost effective when it comes to R&D and expensive acquisition programs.

With a per-unit price estimated at about $4 billion, a new Ohio-class-replacing nuclear ballistic missile submarine (SSBN-X) can produce strategic deterrence for less than an army division of 10,000 career soldiers whose compensation—with pensions and benefits—continues for an additional 40 years after these soldiers have served. A key policy driver in coming years may prove to be the limited costs of upgrading and maintaining existing nuclear weapons when a cash-strapped federal government seeks to reduce the deficit.

Maintaining and upgrading existing nuclear weapon systems is inexpensive by comparison. Even if nuclear weapons are bound—as Kenneth N. Waltz states—to make people uneasy because of their immense destructive power, nuclear arms may prove to be a budgetary emergency exit.

For many Americans, Peter Sellers's portrayal of nuclear deterrence policies in the 1950s and 1960s remains a reality. While Dr. Strangelove (1964) is an iconic film, its black comedy addressed the dangers of nuclear weapons, doomsday devices, missile gaps, and the intricate webs of deterrence and geopolitics of a bygone era where the world was still coming to grips with the destructive power of "the bomb." In one scene, Dr. Strangelove carefully explains for the president deterrence and the doomsday device saying, "Mr. President, it is not only possible, it is essential. That is the whole idea of this machine, you know. Deterrence is the art of producing in the mind of the enemy the fear to attack."

Admittedly, this psychological aspect has not changed, but technology and operational experience have made nuclear weapons a safe and secure means of deterring conventional and nuclear attack, which may prove critically important in deterring an increasingly assertive China. It is cyber deterrence that is in a similar position to where nuclear deterrence was at the time of Dr. Strangelove.

After a generation of neglect, deterrence, in its broadest meaning, is experiencing an overdue renaissance among scholars and policy wonks. For those advocates of nuclear zero who thought conventional precision attack would serve as a panacea for the nation's security challenges, the past twenty years were a disappointment. They failed to deter a number of adversaries America has fought over the last two decades. Most importantly, they have proven all too expensive and are not deterring a rising China, a resurgent Russia, or an unpredictable North Korea.

Budgetary Realities

Despite disengaging from Iraq and the start of reductions in Afghanistan, the federal budget has a trillion dollar plus deficit. And with the 2012 defense and national security budgets equaling 63% of discretionary spending, cuts are likely to come to defense many times in the future. Cuts of 25% or more have an historical precedent and the examples that exist where the warfare and welfare state collide are inevitably won by the welfare state

Dwindling Conventional Forces

Policymakers are realizing there is a limited return on investment when using a counterinsurgency (COIN) military strategy to occupy foreign countries. Two schools of thought in national security have been vying for preeminence in the post-Vietnam era. The First, as embodied by the Weinberger Doctrine, suggests that the U.S. should only employ military force in conflicts with: an expected outcome, a given duration, public support, and where vital national interests are at stake. In short, realism is seeking to reassert itself. In such a way of thinking, there are no proverbial land wars in Asia. The second and, at least within the Beltway, more dominant view advocates employing economic and military power to accelerate the inevitable expansion of democracy. President Bill Clinton's globalization and President George W. Bush's doctrine of preemption are two sides of the same coin.

This latter school of thought gave Americans Somalia, Bosnia, and Kosovo during the 1990s and Afghanistan and Iraq in the 2000s. While the nation's military took an "acquisition holiday" during the 1990s, the 2000s saw defense spending increase dramatically in an effort to fight two wars. And while the Iraq war is over and Afghanistan is winding down, the bill for replacing the nation's worn-out aircraft and ships is leaving Congress with sticker shock.

Personnel are also an expensive asset. With the largest number of personnel, the Army represents a third of defense costs. It is likely that the nation's occupation force will be the prime target for reduction in size and capability and rightfully so. It was the Army that grew by almost 20% to meet the demands of Iraq, and it is the Army that should shrink in its aftermath. This is not an issue of inter-service rivalry, but a question of shifting strategic threats. The Marine Corps also grew during the 2000s and must also return to pre-conflict levels. For the Navy and the Air Force, the past decade was a hard time because acquisition dollars went to fight the wars in Afghanistan and Iraq instead. Absent the services and the DoD finding a way to bring down acquisition costs, this decade may prove even tougher as defense spending is increasingly squeezed by entitlement growth.

With all of the previous doom and gloom assessments, realist advocates of the nuclear arsenal have an opportunity to offer a different and more cost effective vision for national security, but it must include cyber. First, and most importantly, they must overcome Washington's predilection toward costly action and offer a compelling case for restraint on a grand scale. By in large, China has given the United States a model for such restraint—thus far. Second, they must move beyond nuclear deterrence and offer a full spectrum of deterrence options, with cyber deterrence the central addition.

Cyber Deterrence

Had Dr. Strangelove been an advisor and scientist in today's Department of Defense, it is certain that cyber deterrence would play a central role in his deterrence thinking. With cyberspace all the rage within the national security community, it should come as no surprise that cyber deterrence is a rapidly developing area of opportunity. While cyber weapons lack digital lethality (so far), the ability to kill other systems and create havoc in an adversary's society—with significant human suffering as a side effect— creates the potential to deter an adversary. Deterrence is built on the certainty that a response to one's actions will outweigh the potential gains of taking those actions.

While it is true that cyber weapons have yet presented a visible threat of mass destruction—as nuclear and conventional arms have—this is changing. It is important to understand both the options embedded in cyber deterrence and the actions that are feasible. Cyber weapons have global reach at a limited cost, but questions remain about their actual lethality and attribution.

After the Stuxnet attack in which malicious code entered the computer networks of the Iranian nuclear program and physically destroyed equipment by manipulating operating speeds, the legal community started a review of cyber weapons. According to some international legal theorists, there was no control over where, how, and when Stuxnet proliferated in computer systems. Therefore, it was assumed that it could create civilian harm and in doing so would become illegal by international law standards. A combination of the absence of destructive power and the soon-established precedence that cyber weapons are not precise military targets and, therefore, in conflict with international law, erode the opportunity of replacing conventional deterrence with cyber deterrence preparing the way for further reliance on nuclear deterrence. Thus, cyber deterrence is in need of significant development. This is particularly important because of the vast penetration of American private and public sector networks originating from China. Thus far, the United States has found no effective way to deter such attacks.

Nuclear Deterrence

In the coming decades, nuclear arms can play a greater role in comparison to the last two decades. They are the only weapons that project power from Montana to Macau simultaneously, without moving military hardware or personnel. Political theorist Kenneth N. Waltz argued that the power of nuclear arms lies in not what you do with them, but what you can do; an argument he was not alone in making. Under severe budgetary pressures, nuclear arms maintain the nation as a great power regardless of economic, cultural, or other influence—a point the Chinese, North Koreans, and Russians understand well. This reasoning also led the United Kingdom to make building nuclear-capable submarines a priority, even after the deepest defense cuts since the post-World War II drawdown.

Reliance on nuclear arms to maintain geopolitical equilibrium is visible in Siberia and Russia's Far East, where a resource-rich wilderness borders a resource-craving China. Russia's ability to defend and uphold the territorial sovereignty of its Far East relies heavily on nuclear arms. Nuclear arms are returning as a tool of power—even if incrementally.

Boom Time for Boomers, Bombers, and Ballistic Missiles

Austerity and extensive defense budget cuts are triggering renewed interest in the nuclear triad. While the price of boomers, bombers, and intercontinental ballistic missiles (ICBM) may seem relatively high, at less than 10% of the defense budget, both figuratively and literally they offer the greatest bang for the buck. Nuclear submarines project awe-inspiring and stealthy power beyond the force any armored division or army corps can ever achieve. Bombers allow the president to signal adversaries in a way submarines and missiles cannot. ICBMs increase the threshold for launching an attack against the United States by forcing an adversary to attack the homeland should they seek to destroy our ability to return fire. While the triad may, at first glance, have appeared expensive and outdated after the Cold War, a fiscally constrained military that seeks to maintain stability across the globe requires a robust arsenal as means to preventing great powers from beginning and/or escalating conflicts that could go nuclear. In short, they deter and limit great power conflicts, which have proven costly for the United States.

Affordable Deterrence

The United States has no other option than to seek innovative ways to decrease defense costs without losing deterrent power and risking national security. Henry Kissinger once argued that "The absence of alternatives clears the mind marvelously." The future of American deterrence will be connected to affordability. After the era of endless money, as Robert Gates calls the years after 9/11, there are tough decisions to make at the start of the Asia-Pacific century. Even if defense cuts are imminent, there are several advantages for the U.S. that can be exploited to achieve affordable defense; the nuclear arsenal being the most important one.

Despite advances in technology the U.S. still enjoys geopolitical advantages. For example, the Pacific and Atlantic oceans protect the country from a variety of conventional military threats. In comparison to other nations, the country is safe geopolitically. The cost to defend the homeland is far less than conducting large-scale, counterinsurgency operations in remote countries—invade, occupy, and rebuild. In general, neighbors to both north and south are friendly.

From a long-term financial viewpoint, defense focused on the American homeland requires a smaller land force in comparison to the present one. With deterrence, intelligence, and the ability to intercept incoming aircraft or missiles enabled by systems that are capital intensive and sophisticated, fewer personnel are required to defend the homeland and protect American interests in Asia.

According to Waltz, deterrence is what you can do, not what you will do. Throughout history, adversaries have taken steps toward each other that escalated quickly because they underestimated the options and determination of the other based on the presence of resources of war at hand. Because of this, it is important that America is clear about its intentions and capability.

The United States is the only nation that has used nuclear arms at war when it eradicated two Japanese cities at the end of World War II. None have yet to employ the nuclear option—an all-out attack, in cyberspace. America is, after all, the only nation that has used nuclear weapons—credibility that should not be frittered away. For any potential adversary, it is a lethal fact. America are likely able in near time to create disproportional digital exploitation responses (DDER) to any power that crosses the line and challenge U.S. cyber supremacy with significant destabilizing effect on the targeted society. It might not color the minds of the current American leadership, but it influences foreign leaders. Deterrence relies upon will and capability. If the United States can no longer deter with conventional forces; international sanctions are ineffective; and coalition building is beyond others' financial reach; nuclear deterrence becomes the primary upholder of strategic deterrence. When austerity removes other strategically deterring options and the United States is left with nuclear deterrence, Dr. Strangelove and his doomsday machines (cyber and nuclear) can make their triumphal return.

America's ability and willingness to wage all-out war is validated by strategic deterrent patrols, bombers sitting on alert, launch-ready missiles, and an offensive cyber-Armageddon capability. With these assets ready to reach global targets, deterrence can be successful. No matter whether we want it, believe it, like it, or imagine it, federal austerity will force radical change in the nation's defense posture, which is likely to lead to a greater reliance on nuclear and cyber arms. Succeeding in Asia will depend upon the United States realizing its position sooner rather than later.

Table of Contents

Tagging and Tracking Espionage Botnets

From Krebs on Security blog, 30 July 2012

A security researcher who's spent 18 months cataloging and tracking malicious software that was developed and deployed specifically for spying on governments, activists and industry executives says the complexity and scope of these cyberspy networks now rivals many large conventional cybercrime operations.

Joe Stewart, senior director of malware research at Atlanta-based Dell SecureWorks, said he's tracked more than 200 unique families of custom malware used in cyber-espionage campaigns. He also uncovered some 1,100 Web site names registered by cyberspies for hosting networks used to control the malware, or for "spear phishing," highly targeted emails that spread the malware.

Although those numbers may seem low in the grand scheme of things (antivirus companies now deal with many tens of thousands of new malware samples each day), almost everything about the way these cyberspying networks are put together seems designed to mask the true scope of the operations, he found. For instance, Stewart discovered that the attackers set up almost 20,000 subdomains on those 1,100 domain names; but these subdomains were used for controlling or handing out new malware for botnets that each only controlled a few hundred computers at a time.

"Unlike the largest cybercrime networks that can contain millions of infected computers in a single botnet, cyber-espionage encompasses tens of thousands of infected computers spread across hundreds of botnets," Stewart wrote in a paper released at last week's Black Hat security convention in Las Vegas. "So each botnet…tends to look like a fairly small-scale operation. But this belies the fact that for every [cyber-espionage] botnet that is discovered and publicized, hundreds more continue to lie undetected on thousands of networks."

Once you get past all the technical misdirection built into the malware networks by its architects, Stewart said, the infrastructure that frames these spy machines generally points in one of two directions: one group's infrastructure points back to Shanghai, the other to Beijing.

"There have to be hundreds of people involved, just to maintain this amount of infrastructure and this much activity and this many spear phishes, collecting so many documents, and writing this much malware," Stewart said. "But when it comes time to grouping them, that's when it gets harder. What I can tell from the clustering I'm doing here is that there are two major groups in operation. Some have dozens of different malware families that they use, but many will share a common botnet command and control infrastructure."

Domains connected to different cyber-espionage botnets typically trace back to one of two destinations in China, according to Dell SecureWorks.

I also attended Black Hat (co-keynoting with novelist Neal Stephenson on Thursday morning); Prior to that, I spent a little over an hour interviewing Stewart about his research. Excerpts from that interview are below.

BK: The report you just released describes a number of malware attacks that appear to be different attacks, but which share some pretty common characteristics. In your view, is there a marked diversity in these malware samples, or are they pretty uniform?

Stewart: It's more different implementations of the same thing over and over again. There are not a lot of features or widely varying techniques. It's as if you went into a computer programming class and gave an assignment, and said your malware should do this and this, and everyone pumps out a tiny little program that does that, and you have 20 different malware samples that none of the antivirus programs are going to detect. While they might share a few subroutines — the bulk of the malicious programs appear to be different source code, communicate differently — but essentially they are the same thing: There will be some sort of backdooor and downloader, and then some kind of obfuscation of traffic so that it's not transferred in plain text. Occasionally, it will use SSL, but not very often.

BK: How about the detection? It seems the detection for this type of malware is pretty low, is that right?

Stewart: Yep. But it's strictly because they are being developed custom to this purpose and distributed in low numbers. They're not often packed with conventional packers, because that in itself is often suspicious. If they have any obfuscation at all, it's [to alter] the code by one byte and load it in with a minimal decryption stub.

BK: How often do you get a chance to see the method of delivery for a given attack that you're tracking?

Stewart: Maybe 5-10 percent of the time. A lot of the intel we build up is simply from seeing a spear phish and the accompanying document that's infected. We look at the host names involved, the IP addresses used, then we go out and try to find other malware samples that talk to those same IPs or domains, or another domain with the same registrant. Then we pull in those samples out of malware feeds and public sandboxes, and run them and see where they try to connect with. And when you repeat that process over and over, it becomes one big feedback loop.

BK: You said in your paper that there are many thousands of other DNS names you are tracking but for which you had no accompanying malware samples. How does that happen?

Stewart: My suspicion is that those samples are not being detected or not shared with the antivirus companies.

BK: But how is it that you know to track DNS names you believe are related?

Stewart: Because these guys are trying to save a little bit of work. Instead of registering a new domain for every piece of malware deployed, they'll just use the same domain for number of years, and have several dozen or more subdomains for that, which will each act as a new command and control point for different malware. Then we can use things like passive DNS to find other subdomains that might be hiding under that domain, and we can reach out and find other malware samples that are related. But like I said, 90 percent of the time, we don't find that malware sample. We know that domain was specifically created by a [cyber espionage] actor for command and control, and we track it to see what else is related to that IP, but we don't often come across the malware sample.

The truth is that if we if we graphed all of this activity, you wouldn't be able to view each part without the whole thing literally covering all the walls of my office. I've got them all tracked, but If I try to draw them all for you, it's a big mess. So what we did with this graph is just to take the malware we know about and have in hand, and to show you how that's related to other IPs and domains and subdomains. That graphic in our paper probably represents about 10 percent of what we know about.

BK: What do you think is the reason for all of these small, but ultimately interconnected [cyber espionage] operations or botnets? Is it a strength in numbers thing, or is it more likely that there are multiple groups doing their own thing and only later joining forces?

Stewart: I feel like there are multiple groups doing their own thing, and then in those, there are probably different actors that have different preferences for how they conduct operations. Some actors just don't like domains and just want to host it on some IP somewhere. Everyone has their own method of operation and they don't all follow the same manual. But we know that many of them do share resources, because scale of the activity we see coming out of these two major groups…I would find it hard to believe that there are just a small number of people writing all that malware and controlling all those domains and IPs.

BK: Given the access that you have, is there a way to extrapolate how much data is being exfiltrated?

Stewart: I don't have any access, except for the sinkholing operations. Once you do that, you remove their ability to go ahead and exfiltrate. All the graphing and stuff I'm doing to map the actor side is being done through malware samples, passive DNS and the victim data is connected to the sink holing, but that doesn't tell me what data they're stealing or how much of it they're stealing.

BK: You mentioned at the end of the paper an example of what looks like an overlap between traditional financially-oriented cybercrime and that of state-sponsored activity. Are you really seeing that much overlap?

Stewart: I think we are. It's not something where there have been a lot of public reports about it. But we've certainly seen spearphishes using malware that we haven't seen in prior [cyber espionage] stuff. The payloads look a lot more like conventional Eastern European cybercrime, but the spear phish email looks much more like what you'd expect to see coming from Chinese actors. And obviously, the overlap we've seen for a while now too, the exploits work their way from zero-day targeted attacks, and then turn around a few weeks later and that same exploit is now in BlackHole exploit kit.

BK: But that hasn't changed over the years has it?

Stewart: I think so. In terms of the exploit coming from one side and flowing into the other. We used to see more exploits developed by exploit kit authors or someone paid to put these attack tools in exploit kits, and then on the other side, the espionage actors using older exploits. But at some point, it shifted and zero-days started to be developed by the [espionage] actors. After all, why should the financially-oriented attackers invest all that time and research when these other espionage actors were coming up with some really good stuff?

BK: And do you see any changes in the use of zero-days in these attacks? Last time I checked it was mostly exploits for which there were patches already available.

Stewart: So they use 'em when they got 'em. Lately they've had the XML Core Services stuff, which has gotten them a lot of mileage. But they don't stop operations just because they don't have a zero-day.

BK: Do you have any knowledge of what the cyber-espionage actors are doing to keep the malware that's on the victim systems from being detected by antivirus tools?

Stewart: I haven't seen any signs of that. A lot of this malware doesn't have any update feature at all. But then again I don't do the long-term monitoring of these malware samples like I used to do with a lot of the spam bots. It's a little bit harder to fool a real live actor who has a botnet of maybe 10 machines. It's a little harder to blend in there without being noticed. They can quickly determine who's in the environment that they're not interested in and just delete the code from that host machine.

BK: As far as these subdomains and overarching control domains go, is that changing at all, or are the attackers still hammering the dynamic DNS providers over and over again?

Stewart: It's a dynamic mix of dynamic DNS and actively registered domains, and it all comes down to the preferences of the groups and what they like to use. They may not have as much success with some targets who are used to being hit for years and have just blocked all dynamic DNS providers within their networks, and in those cases the attackers are forced to go with some kind of hard-coded IPs or registering their own domains. So we're seeing a pretty equal mix.

BK: So what's your best guess of the number of distinct groups or actors here?

Stewart: Well, it seems there are two main groups, but you've got a lot of other activity which seems tangentially related. Sometimes it's just a slight connection — an overlapped IP in the past and there's some shared code — but they don't overlap so much with those two groups. And the other collections of malware…we see them in spear phishes and they're going after the same targets, and they don't have any overlap with other groups' infrastructure whatsoever. So from the way we're approaching the problem trying to map them out by network touch points and domain registrations, it's impossible to tell.

But it's pretty clear there are two main groups, very large and active. Then there's a lot of other activity that coalesces into clusters, but yet we can't say that's not two different actors in the same group versus two independent actors who don't know each other. So I don't think anyone can tell you the answer to the question without having legal means to infiltrate these networks, and without having the ability to spy on them and see who’s calling the shots and paying the payroll, but we obviously don’t have the legal ability to do that.

BK: Is hacking back at these guys really illegal?

Stewart: I’m talking about penetrating their networks and spying on where they’re located and their computers and emails. We’ve seen some glimpses of that and leaks in the media from Hardcore Charlie, but I don’t know how credible that is. There was a hacker who released some things on Pastebin who said he’d hacked into a Chinese defense contractor, and he found documents in there outlining their cyber espionage activities, and was somehow tied to Vietnam and some Ukrainian people who were supplying information on U.S. troop movements to the Taliban. My main problem with this information was that it was all supplied in English.

BK: Are you seeing any indication that these attacks are targeting other countries, with the fingerprint of China?

Stewart: Not sure what you’re asking.

BK: People typically assume that the target of these attacks are the U.S. and some of the countries in the Asian region…

Stewart: Yeah, we’re seeing European government entities, Asia and certainly India. The only place I don’t see a lot of activity against is South America. But obviously it seems to be happening there. We heard the whole thing about how the malware was stealing the CAD designs from the company in Peru, right? So it seems to be happening there as well. So it’s pretty much anyone can be a target. You just have to have something they want.

BK: Are you seeing these espionage attacks and the sources tracing back to sources outside of China?

Stewart: Sure. We talked a bit in the paper about one that seems to have been coming from on security company in another Asian nation. But you can kind of tell when you see something that doesn’t completely match the modus operandi.

BK: Can you share the information about which company you’re referencing?

Stewart: We cannot. If law enforcement is interested in that information, we’re happy to share it.

BK: Are you seeing any indication that the antivirus companies are doing better job detecting this stuff?

Stewart: I think some security companies are definitely doing a better job of incorporating protections into their services or products. I don’t know if AV companies are necessarily getting better detection rates, but certainly a lot of companies we’re working with to share information about malware samples and IP addresses are classifying them to incorporate them into detections.

BK: Would you say the activity you’ve measured is just a better understanding that you’ve gained as to the true scope of the problem, or has the problem of state-sponsored espionage gotten more pronounced over the last few years?

Stewart: I think it’s a better understanding. This kind of methodical effort to classify things and separate all of the regular financial malware from the cyber espionage stuff…the samples have shown up on different AV radars over the years. The problem is that there’s just not enough work put into classifying these things so that when we see it again we know what it is. In a lot of these attacks, the next time a piece of malware is detected it has a different name and nobody connects the two. And if I don’t see it on the AV networks with a proper and consistent name, we’ll assign it our own name and call it that going forward. That’s what I’ve been trying to do — eliminate the mystery.

BK: A lot of financially-oriented malware attacks are fairly automated, in that they rely on tools that handle much of the exploitation, and in some cases even the extraction of funds from victim systems. But these state-sponsored attacks tend to be quite a bit more hands-on, don’t they?

Stewart: It’s something where it only works on a human scale for them. It’s not something like cyber crime botnets where they can leverage as many computers as they can pay to have infected. Someone’s got to craft these spear phishes and send them out, and someone has to deal with the documents that are stolen in these operations. They can only get as big as the number of people they have to train and perform these operations. My worry is not that these entities or groups are going to get huge and have lots of more targets, but that there are going to be more and more players that will get into the game because they realize that nobody is getting prosecuted for this and as long as they don’t cross certain lines within our own jurisdiction, they seem pretty free to spy on other companies and other countries. Why not have a contract doing this activity for the government and then on the side make some money doing it for private companies? Then they have some kind of legal shield, because the government can’t come and prosecute them, because they’re doing the same activity for the government. That’s my worry: That we’re going to see a lot more players in this space.

BK: So really, you’re thinking down the road a bit as this becomes a bit more commoditized?

Stewart: Yeah, I guess. Not that they’ll necessarily be advertising this – that they’ll put up an ad at [the RSA Security Conference] and say “We’ll spy on your competitors” — but certainly you can see some enterprising businesses with ties to the government being able to conceive of such a plan and make some pretty good money doing it.

BK: Are you seeing evidence of that activity so far?

Stewart: I think that’s what that security company we wrote about in the report is doing. Based on the targets. Because on the one hand we see them going after foreign militaries, and then also going after commercial targets, and journalists within the same country. And then we ask, ‘Well, why would they be interested in them?,” and then we see those journalists are publishing a news magazine that’s critical of that government.

BK: Can you be more specific about the company that you’ve seen doing this?

Stewart: No.

BK: But pretty much all of those nations have tens of millions of people and millions of businesses…so what’s the harm in naming the country where the allegedly offending company resides?

Stewart: Yes, but they’ve only got so many security companies, and probably only so many companies that also offer ethical hacking courses. But they are an ally of the United States. One of the targets that we saw and alerted was Japan, and I think it was today that the finance minster there went to the news media and notified folks that they suffered a breach. We don’t know if it’s the same thing that we notified them about, but there it is.

Table of Contents

China’s ‘Model Workers’ Head to Cyberspace

By Adam Segal, the Diplomat, August 21, 2012

How an old strategy with a 21st century spin is being used to "to mobilize and motivate citizens."

There is a long tradition of the Chinese Communist Party acknowledging and honoring “model workers,” selfless citizens who contribute to the building of modern China. While in the early years after the revolution these individuals were usually peasants or ordinary workers like Zhang Binggui who worked at a candy counter and could “count out prices and change in his head,” the category has expanded to encompass almost all professions including the astronaut Yang Liwei and NBA-great Yao Ming.

The most famous model of serving the people was Lei Feng, the young soldier who became the subject of a massive propaganda campaign in 1963, a year after his death. As China Daily put it, Lei Feng “is hailed as a cultural icon, symbolizing selflessness, modesty, and dedication. His name creeps into people’s hearts, daily conversation, music, even movies.”

These model worker campaigns serve a number of purposes: to mobilize and motivate citizens; identify qualities and characteristics that would be valued in the new China; and signal political priorities and concerns. Campaigns to “Learn from Comrade Lei Feng” have been rolled out numerous times over the last six years (see this timeline at Danwei) in efforts to divert from corruption scandals and other bad news as well as address the very real growing absence of civic mindedness and public-spiritedness.

The Chinese press has recently introduced two new model workers active in cybersecurity: Li Congna (李聡娜) of the PLA, and the “Legendary Female Cyber Cop,” Gao Yuan (高 媛) of the Beijing Public Security Bureau’s Cybersecurity Defense Division. The stories of these two women repeat many of the same tropes from campaigns in the 1950s and 1960s, especially those focused on what historian Tina Mai Chen calls “female kind first‟—the first woman tractor driver, welder, or train conductor.

The heroes of these stories must overcome both physical and mental hardships. Sun Xiaoju, the first female train conductor, faced temperatures of minus twenty degrees Celsius but refused to let the frostbite affect her. After working on one project for a month, Li Congna lost 7.5 kg, and a marathon coding session left her unconsciousness for three days (physical hardship is missing from Gao’s story; her greatest hardship seems to be someone stole her identity on the instant messaging service QQ). As with Tang Sumei, an ordinary “peasant girl” who knew nothing about the machinery when she first entered a Beijing electric substation in 1952 but was a manager by 1953, hard study and individual resolve save the day. Confronted by source code she couldn’t read or understand, Li stayed late in her office “memorizing related functions, studying protocol mechanisms, researching both foreign and domestic computer program models. In one month, she had written 300,000 lines of code, more than 100 types of functions, more than 60 protocol mechanisms, and more than 20 design algorithms."

What do these model workers tell us about Chinese cyber policy? First is the need for constant innovation. Li keeps confronting problems that require a new, self-developed technological solution. In her office, she has posted the slogan: "Yesterday's technology cannot win tomorrow's wars." Facing a difficult problem, the advice of a teacher rings in Li's ear: "the world of information networks is a game of new knowledge and new technologies."

Second, there is an acknowledgement that traditional top-down, hierarchical organizational and training procedures are not up to the task of network warfare. Several times we are told that Li is not afraid to let others take the lead and in particular she lets "young daring people" assume responsibility as group leaders.

Gao Yuan is a model of how the Chinese government can successfully use Weibo and other social media to bolster public approval by providing useful services and eschewing overt propaganda. Her story is filled with how helpful she is to Chinese netizens—Gao has "tweeted over 1,500 times; spread knowledge about staying vigilant over 700 times; has answered netizens' questions close to 2,000 times; and has provided technological support over 400 times." The political content of Gao's work appears to be low, and as a result she seems to be highly respected. She currently has 1.52 million followers on Weibo, and one follower has started a cartoon series about her. In contrast, a number of commenters were highly critical of the Li Congna story, with several mocking the idea of Li's falling unconscious.

Gender matters to these stories, as information security is a heavily male profession (see for example, the recent discussions about sexism and sexual harassment at DEF CON, the annual hacker conference held in Las Vegas). The descriptions of both Li and Gao as beautiful strike one as unnecessary, if not slightly retrograde; but as Chen notes about the model tractor workers of the past, these stories send an important message about the ability of women to master new technologies. The Li story goes even further noting "female service members will inevitably assume more responsibility, and will make greater achievements." As a result, the PLA will have to adjust: "The armed forces at all levels should provide them with a wide arena."

It is easy to dismiss these stories as out-of-date and heavy-handed. But, assuming the press doesn't turn to new model workers, Li's and Gao's future adventures are likely to provide further insights into some real issues in Chinese cyber policy.

Table of Contents

Symposium on Ancient Chinese Psychological Warfare held in Beijing

By Xue Ningdong and Lu Jun, PLA Daily, August 21, 2012

Jointly hosted by the Sunzi Research Association of Shandong and the Military Psychology Committee under the Chinese Psychology Society, the symposium on Ancient Chinese Psychological Warfare was held on August 18, 2012 at the Psychology Institute under the Chinese Academy of Sciences (CAS).

A total of 45 experts and scholars in the fields of military science, psychology and history throughout the country discussed the historical value and contemporary significance of the book entitled Conquest without Combat – Ancient Chinese Psychological Warfare Thought and Usage as well as the ancient Chinese psychological warfare.

The monograph entitled Conquest without Combat – Ancient Chinese Psychological Warfare Thought and Usage is written by former vice chairman of the Standing Committee of the Shandong Provincial People's Congress. The book, with 500,000-odd words, comprehensively and systematically expounds the origin and development of ancient Chinese psychological warfare from the pre-Qin period to the Ming and Qing dynasties. It has blazed a trail in building a psychological warfare academic system with Chinese humanist tradition and filled the gap in ancient war theories of China and even the world.

The book has become a textbook for psychological warfare majors of the Chinese People's Liberation Army (PLA).

Table of Contents

Internet Analysts Question India’s Efforts to Stem Panic

By Vikas Bajaj, New York Times, August 21, 2012

MUMBAI, India — The Indian government’s efforts to stem a weeklong panic among some ethnic minorities has again put it at odds with Internet companies like Google, Facebook and Twitter.

Officials in New Delhi, who have had disagreements with the companies over restrictions on free speech, say the sites are not responding quickly enough to their requests to delete and trace the origins of doctored photos and incendiary posts aimed at people from northeastern India. After receiving threats online and on their phones, tens of thousands of students and migrants from the northeast have left cities like Bangalore, Pune and Chennai in the last week.

The government has blocked 245 Web pages since Friday, but still many sites are said to contain fabricated images of violence against Muslims in the northeast and in neighboring Myanmar meant to incite Muslims in cities like Bangalore and Mumbai to attack people from the northeast. India also restricted cellphone users to five text messages a day each for 15 days in an effort to limit the spread of rumors.

Officials from Google and industry associations said they were cooperating fully with the authorities. Some industry executives and analysts added that some requests had not been heeded because they were overly broad or violated internal policies and the rights of users.

The government, used to exerting significant control over media like newspapers, films and television, has in recent months been frustrated in its effort to extend similar and greater regulations to Web sites, most of which are based in the United States. Late last year, an Indian minister tried to get social media sites to prescreen content created by their users before it was posted. The companies refused and the attempt failed under withering public criticism.

While just 100 million of India’s 1.2 billion people use the Internet regularly, the numbers are growing fast among people younger than 25, who make up about half the country’s population. For instance, there were an estimated 46 million active Indian users on Facebook at the end of 2011, up 132 percent from a year earlier.

Sunil Abraham, an analyst who has closely followed India’s battles with Internet companies, said last week’s effort to tackle hate speech was justified but poorly managed. He said the first directive from the government was impractically broad, asking all Internet “intermediaries” — a category that includes small cybercafes, Internet service providers and companies like Google and Facebook — to disable all content that was “inflammatory, hateful and inciting violence.”

“The Internet intermediaries are responding slowly because now they have to trawl through their networks and identify hate speech,” said Mr. Abraham, executive director of the Center for Internet and Society, a research and advocacy group based in Bangalore. “The government acted appropriately, but without sufficient sophistication.”

In the days since the first advisory went out on Aug. 17, government officials have asked companies to delete dozens of specific Web pages. Most of them have been blocked, but officials have not publicly identified them or specified the sites on which they were hosted. Ministers have blamed groups in Pakistan, a neighbor with which India has tense relations, for creating and uploading many of the hateful pages and doctored images.

A minister in the Indian government, Milind Deora, acknowledged that officials had received assistance from social media sites but said officials were hoping that the companies would move faster.

“There is a sense of importance and urgency, and that’s why the government has taken these out-of-the-way decisions with regards to even curtailing communications,” Mr. Deora, a junior minister of communications and information technology, said in a telephone interview. “And we are hoping for cooperation from the platforms and companies to help us as quickly as possible.”

Indian officials have long been concerned about the power of modern communications to exacerbate strife and tension among the nation’s many ethnic and religious groups. While communal violence has broadly declined in the last decade, in part because of faster economic growth, many grievances simmer under the surface. Most recently, fighting between the Bodo tribe and Muslims in the northeastern state of Assam has displaced about half a million people and, through text messages and online posts, affected thousands more across India.

Officials at social media companies, speaking on the condition of anonymity to avoid offending political leaders, said that they were moving as fast as they could but that policy makers must realize that the company officials have to follow their own internal procedures before deleting content and revealing information like the Internet protocol addresses of users.

“Content intended to incite violence, such as hate speech, is prohibited on Google products where we host content, including YouTube, Google Plus and Blogger,” Google said in a statement. “We act quickly to remove such material flagged by our users. We also comply with valid legal requests from authorities wherever possible.”

Facebook said in a statement that it also restricts hate speech and “direct calls for violence” and added that it was “working through” requests to remove content. Twitter declined to comment on the Indian government’s request.

Telecommunications company executives criticized the government’s response to the crisis as being excessive and clumsy. There was no need to limit text messages to just five a day across the country when problems were concentrated in a handful of big cities, said Rajan Mathews, director general of the Cellular Operators Association of India.

“It could have been handled much more tactically,” he said.

Others said the government could have been more effective had it quickly countered hateful and threatening speech by sending out its own messages, which it was slow to do when migrants from the northeast began leaving Bangalore on Aug. 15.

“It has to also reach out on social networking and Internet platforms and dismantle these rumors,” Mr. Abraham said, “and demonstrate that they are false.”

Table of Contents

Information Wars: Assessing the Social Media Battlefield in Syria

By Chris Zambelis for Combating Terrorism Center (CTC), International Relations and Security Network, 22 Aug 2012

Efforts to understand the nuances inherent to the political turmoil in Syria present daunting challenges. While the numerous insurgent factions and the Syrian security forces engage each other in combat in towns and cities to secure tangible battlefield gains, the warring parties are also waging a contentious information war in cyberspace, specifically within the virtual arena of online social media. The various strands of the opposition in Syria—political and violent—have taken to social media since the earliest stages of the uprising to advance their agendas. Analogous to their role in facilitating communication and information exchange during the wave of revolts that have been sweeping the Arab world since 2011, new media platforms such as the array of social media websites and related technologies that are available to the public at virtually little or no cost have become crucial to shaping how the crisis in Syria is portrayed and perceived.

This article examines the social media battlefield in the Syrian uprising with specific attention on the Free Syrian Army's (FSA) online activities. It also addresses the relative impact of the social media battlefield on dictating the course of events in Syria.

The Social Media Landscape

Every serious political or militant actor with a stake in what is happening in Syria has a presence on social media through some combination of officially hosted websites and blogs, as well as Facebook, Twitter, Tumblr, YouTube, Flickr, online chat room forums, Short Message Service (SMS) platforms, and other venues. The leading political opposition factions, namely the Syrian National Council (SNC), National Coordination Committee for Democratic Change (NCC), and the numerous Local Coordination Committees of Syria (LCCs), all operate a network of professionally-designed and maintained websites and social media platforms to broadcast information. The UK-based Syrian Observatory for Human Rights (SOHR), a body closely tied to the SNC, is also widely active on social media. The SOHR publicizes alleged casualty counts and human rights abuses it blames on the Ba`athist regime's security services and irregular paramilitary forces.

Led by the FSA and the numerous insurgent groups that claim to be fighting under its umbrella, the violent strain of the Syrian opposition is also well represented on social media. The Omawi News Live network and Ugarit News are two of the most prominent among a host of outlets that serve as quasi-official information platforms broadcasting a wide range of material on behalf of the Syrian opposition on social media. Both networks air amateur video footage of alleged attacks by Syrian security forces and insurgent operations, reports documenting purported defections of members of the Syrian military, alleged evidence of human rights abuses and atrocities perpetrated by the Ba`athist regime, and other items that cast Damascus in a negative light. The growing radical Islamist current within the Syrian opposition, including Jabhat al-Nusra and other extremist movements that appear to be motivated by al-Qa`ida's style of radicalism are also active on social media. Jabhat al-Nusra announced its formation and claimed responsibility for a series of terrorist attacks across Syria through official declarations and video features produced by its al-Manara al-Bayda Foundation for Media Production and issued on radical Islamist websites and chat room forums. Jabhat al-

Nusra has since carved out its own place on social media through the creation of a dedicated website and affiliated online outlets.

The importance of winning the information war on social media has not been lost to the Ba`athist regime and its supporters. Official Syrian media and information outlets such as the Syrian Arab News Agency (SANA) are active online. The creation of the Syrian Electronic Army (SEA) and a host of associated outlets, however, reflects a greater effort by the Ba`athist regime to combat the opposition's struggle to monopolize the information war. In addition to encouraging supporters of the Ba`athist regime to engage in online activism, the SEA is also involved in cyber warfare and hacking operations. The SEA has produced a recruitment video in Arabic and English that outlines its mission to defend Syria and is reminiscent of the videos issued by the hacktivist group Anonymous in its presentation and tone. In doing so, the SEA relies on a nationalistic discourse that emphasizes Syrian unity and loyalty among Syrians to their country. Social media platforms associated with the Ba`athist regime reflect the narrative presented by Damascus: Syria portrays the crisis as an effort by its primary enemies—the United States, Saudi Arabia, Qatar, and Israel—and their regional allies to undermine and destroy Syria by way of proxy war and encouraging sectarianism, violent insurrection, and radical Islamist militancy. A range of social media outlets operated by supporters of the Ba`athist regime inside Syria and abroad also helps sustain this effort to counter the opposition.

The Free Syrian Army Online

The FSA, the amorphous insurgent movement that has emerged as the armed wing of the Syrian opposition faction directed by the SNC, along with its many armed affiliates are prolific on social media. The inaugural statement declaring the establishment of the FSA by defected Syrian Air Force colonel and subsequent FSA commander Riyad Musa al-Asa'd and seven fellow members of the Syrian military was uploaded to YouTube and other social media outlets. The numerous other militant groups that have proclaimed their allegiance to the FSA and intention to violently resist the Ba`athist regime have likewise taken to social media to announce their motives.

Despite securing varying degrees of financial, diplomatic, materiel, and logistical support from Saudi Arabia, Qatar, Turkey, and the United States, the FSA's ability to defeat the far better trained and equipped Syrian security forces remains in question. Nevertheless, the FSA appears keen to compensate for its tactical and operational inadequacies by exploiting social media as a force multiplier. The circulation of amateur video footage of dead or captured Syrian forces undergoing interrogation by the FSA or a smoldering Syrian military vehicle relayed on social media can have a multiplier effect on domestic and international perceptions regarding the military prowess of the insurgents. This is the case even as the insurgents continue to sustain heavy losses in direct engagements with Syrian security forces. The proliferation of videotaped statements and other items issued by defected members of the Syrian security forces on social media can also work as an effective psychological tool to illustrate declining unity and morale among the ranks of Ba`athist forces even as the numbers of defected forces remain marginal.

Overall, the accessibility of social media enables the insurgents to participate on a leveled information playing field that was previously the exclusive domain of state actors or institutions closely aligned with ruling authorities. Similarly, the advent of social media enables individuals and organizations with little or no formal association with the factions currently operating inside Syria to project their influence into the events on the ground. Extremist ideologues such as Shaykh Adnan al-Arour, for instance, a Syrian Salafist cleric who currently resides in exile in Saudi Arabia, is among the most vocal supporters of the FSA on social media and traditional media outlets, including satellite television.

The FSA and its associates are also exploiting the virtual domain of social media to disseminate propaganda and disinformation to bolster their causes, with an eye toward capitalizing on its inherent multiplier effects. Evidence that activists sympathetic to the FSA have broadcast doctored amateur videos showing alleged battlefield successes executed by the insurgents against Syrian forces, desertions of Syrian troops from their posts, and massacres of civilians and other atrocities blamed on Syrian security forces in the absence of concrete proof implicating the Ba`athist regime is a case in point. Members of the Syrian security forces who undergo questioning by the FSA on video also often appear to recite claims frequently made by the insurgents to validate their positions. Along with the SNC, the FSA accuses Syrian allies Hizb Allah and Iran of actively assisting the Ba`athist regime to violently suppress the uprising. Alleged Shabiha members captured in Idlib Province admitted on a video that was circulated across cyberspace to receiving orders and support from Hizb Allah leader Hassan Nasrallah and Iran, among other claims, in spite of a lack of concrete evidence.

The FSA has also worked hard to refute accusations that radical Islamists and other extremists motivated by sectarian agendas or mercenaries acting on behalf of Syria's enemies make up their ranks. The dissemination of a video showing an alleged Syrian Christian military officer announcing his defection from the Syrian army—the first Christian member of the Syrian security forces to do so, according to the video's title—and decision to join the Sham Eagles Brigade of the FSA is another example of the insurgency’s resort to social media as a force multiplier.

Conclusion

Effective messaging allows for the contesting parties in Syria to present unadulterated versions of their respective narratives and positions to supporters, opponents, and neutral parties alike in Syria and beyond. A successful information campaign also helps sway target foreign audiences that may have little or no stake in what is happening in Syria to choose sides. In this context, the competing factions in Syria are waging a virtual campaign to win over international public opinion. In today's information climate, an item posted to YouTube or Twitter by individual users or activists can easily compete with and often may supersede a breaking dispatch from reputable international media conglomerates in terms of the number of consumers it reaches in the public domain. Raw reports, such as amateur video footage and photography of events such as a public protest organized by opposition activists or a funeral procession for a Syrian who is believed to have perished at the hands of the Syrian security forces, make an impact on social media in such a way that is impossible to emulate through traditional print or second-hand news reportage. Amateur video footage of the funeral of Hamza Ali al-Khateeb, a 13-year-old boy who was allegedly tortured and killed by Syrian security forces after being detained in a protest in his native Dera`a, spawned a wave of outrage in Syria and around the world that helped embolden the already simmering opposition against the Ba`athist regime.

At this juncture, it is impossible to determine the precise effect social media is having on shaping the course of developments in Syria. It is clear, however, that the virtual arena has emerged as a crucial battlefield for the warring factions, political and violent, operating on Syrian soil and outside of its borders. At the very least, the sheer volume of social media platforms operating independently and in unison by all sides suggests an interest to secure both tactical and strategic gains through victories in the virtual battlefield.

Table of Contents

In Twist, Chinese Company Keeps Syria on Internet

By Jaikumar Vijayan, ComputerWorld, 22 Aug 2012

August 22, 2012 06:00 AM ET. .Computerworld - In a somewhat ironic turn of events, a telecom company based in China, a country famous for Internet censorship, has become the primary means of Internet access for people looking to get information out of war-torn Syria.

An analysis of Internet traffic flowing into and out of Syria over the past few days, shows that a major portion of it is being routed through Hong Kong-based PCCW, according to Internet monitoring firm Renesys.

Turk Telecom, which used to be the biggest provider of Internet connectivity services to Syria has completely dropped out of the picture since August 12 while other smaller providers like Telecom Italia appear to be fading away as well, the company said.

That has left PCCW carrying a lion's share of the Internet traffic to and from Syria, Renesys analyst Doug Madory said today.

What's unclear yet is if the situation is the result of the tightening economic sanctions against Syria or whether it stems from infrastructure damages inside the country as a result of the ongoing conflict, he said.

"While U.S. firms are barred by sanctions, it is China, a country that bans YouTube via the Great Firewall, that is largely responsible for the free flow of information out of Syria," Renesys general manager Earl Zmijewski added.

The Internet has played a big role in the civilian uprisings in the Middle East over the past two years. The huge protests in Egypt, Tunisia and Iran were fueled to an extent by social media networks such as Twitter and Facebook.

Though the governments in each of those countries attempted to throttle access to social networks by cutting off access to Internet services many still managed to find their way around such efforts thanks in large part to support from companies and organizations in countries friendly to their cause.

The escalating conflict in Syria has already resulted in several major Internet outages over the past six weeks, Madory said. Syria's only Internet provider, the Syria Telecommunications Establishment (STE) briefly withdrew all 61 of the country's networks from the global routing table last Friday. It did the same thing intermittently with about 20 networks on Saturday.

"When there's a big outage we see routes to different networks being withdrawn from the global routing table," which is what has been happening in Syria for the past several weeks.

In addition to these outages, Renesys has also observed a fairly dramatic shift in the service to Syria being provided by the different telecommunications companies in the region, Madory said. Turk Telecom, which was by far the biggest provider of services to the STE, briefly disappeared for a while on August 3rd before dropping out of sight entirely on August 12.

The change in service levels could be the result of physical infrastructure damage or because of configuration changes made by the company to exclude traffic flowing in and out of Syria. The result is that all 61 of Syria's networks are now directing traffic through PCCW's networks.

What's interesting is that major U.S. telecommunications companies such as Level 3 and Cogent currently provide Internet services to Syria's neighbors such as Lebanon, but are prohibited from providing the same services in Syria.

"With the diminishing role of western carriers, PCCW is left as a primary means for the Syrian people to document the ongoing conflict, such as via timely YouTube videos, Madory wrote in a blog post on Tuesday. ”Ultimately, telecommunications bans could prove counterproductive if they end up placing barriers to the free flow of information," he said.

Table of Contents

Inside the Ring: Taliban Infiltrate Social Media

By Bill Gertz, Washington Times, 23 August 2012

Taliban insurgents are using Facebook, YouTube and more recently Twitter to try to recruit terrorists and incite terrorist attacks, U.S. military officials say.

The increasing use of the Internet and cellular telephones with access to the Web is a relatively new feature of life in Afghanistan, and military officials say the Taliban are exploiting the new social-media platforms for their Islamist aims.

"Overall, it's probably too early to talk about trends, but I would say the Taliban, just like the rest of the world, are trying to use social media to achieve their aims," said Lt. Col. T.G. Taylor, a U.S. Central Command spokesman. "How effective they are remains to be seen."

A defense official said U.S. intelligence agencies that monitor the Internet for terrorist activity in the past have detected Taliban insurgents and other violent extremists using social media. When that happens, Central Command is notified, and, in the past, the command has contacted outlets like Facebook and Twitter, urging them to halt terrorist recruitment or inciting violent attacks noting that it violates their terms of service.

Facebook has been the most responsive, deleting some accounts of Taliban insurgents or those posing as Taliban.

In Afghanistan, the use of Facebook is the most prevalent form of social media among many Afghans who use the service to contact family members and associates, to share Internet links and to post status reports, photos, videos and comments.

Along with the general population, Afghan insurgents and jihadists now are using social media such as Facebook and more recently Twitter, officials said.

The International Security Assistance Force in Afghanistan, the military command that is in charge of information operations against the Taliban, has been very concerned about the terrorists' use of social media.

Military officials say the Taliban have proven to be an adaptable enemy and are now using cyberspace as a new battlefield.

In addition to recruitment, the Taliban use social media to provide information, including false and misleading "disinformation," to various audiences both domestically and internationally.

In some cases, the Taliban's use of social media has outpaced that of NATO and U.S. forces, which have been struggling to wage effective information-warfare campaigns against the Islamist insurgents.

The military is trying to balance the need to gather intelligence from such media and cellphones with efforts to prevent the enemy from recruiting more fighters or influencing populations, a defense official said.

"A balance has to be struck, not just with Twitter, but especially with cellphones," said the official. "If we hear Bad Guy A talking to Bad Guy B, do we let them have the conversation and listen, or do we shut it down and not let them talk?"

Table of Contents

North Korean Jamming of GPS Shows System’s Weakness

By Shaun Waterman, Washington Times, August 23, 2012

U.S. and South Korean military commanders will be on the lookout for North Korean efforts to jam GPS signals as they take part in exercises on the divided peninsula this week and next.

North Korea repeatedly has jammed GPS signals in South Korea, which has “very serious implications” because U.S. and South Korean military system rely on the navigation system, said Bruce Bennett, a North Korea scholar for the California think tank Rand Corp.

The jamming also underscores the vulnerability of a satellite-based tool on which civilian systems from car navigation to air traffic control rely upon.

North Koreans have used Russian-made, truck-mounted jamming gear near the border to disrupt low-power GPS signals in large swaths of South Korea. By broadcasting powerful radio signals on the same frequencies as the satellites, the jammers drown out the GPS signals.

Mr. Bennett said the jamming has occurred three times in the past two years and has coincided with joint U.S.-South Korean military exercises.

The timing strongly suggests the jamming was “an experiment … a test … to let [the North Koreans] see what effect it would have and maybe disrupt the exercises,” he said.

Defense officials declined to comment on the jamming, or discuss what measures U.S. forces are taking to guard against further incidents during this week’s exercises, which end Aug. 31 and involve more than 80,000 troops from the United States and South Korea, plus observers from seven other countries.

“The U.S. Department of Defense takes all jamming seriously,” said Air ForceLt. Col. Damien Pickart, a spokesman for U.S. Pacific Command.

For North Korea, the jamming is an attempt to turn the tables on the more technologically advanced U.S. and South Korean forces.

“Neutralizing those [technological] advantages could have big psychological benefits in peacetime and major military benefits in war,” Mr. Bennett said.

He added that the jamming equipment is easy to locate because of the powerful signals it broadcasts. “If you use this kind of weapon, you must assume that sooner or later, the other guy is going to destroy them,” he said.

Determining how North Korea might use the jamming as a weapon is difficult because its military does not produce publications, unlike China’s, which publishes academic journals and policy documents, Mr. Bennett said.

“The way we try to understand North Korean [military] doctrine is watching how they train and exercise,” he said.

In September, there were reports that North Koreans were developing their own, more-powerful jamming technology. Mr. Bennett said it appears that this new equipment was being tested in the most recent jamming incidents in March and April.

The incident in April caused the most significant disruption, even though the jammers were switched on only intermittently. The South Korean capital, Seoul, is only a few miles from the border, and its airport, Incheon International, was badly affected by the jamming. Aircraft had to rely on alternative navigation aids, and even cars in the city’s northern suburbs found their GPS equipment affected.

“GPS signals are not difficult to jam because they are weak in the first place and a very, very long way away,” said Todd Humphreys of the Radionavigation Laboratory at the University of Texas in Austin.

Global positioning satellites hovering 22,000 miles above the planet produce the signals that ground-based detectors use to triangulate locations on Earth’s surface.

Even military GPS signals, which are 10 times stronger than civilian ones, can be jammed easily, at least in small areas, with cheap commercially available equipment, Mr. Humphreys said.

He noted that Chinese-made jammers are advertised for sale on the Internet — pocket-sized devices that block GPS signals from several feet to more than 100 feet away.

And it is not just rogue nations such as North Korea that are interested in jamming GPS signals.

In Britain, a clandestine government-sponsored network of 20 roadside GPS monitoring posts this year found dozens of incidents of jamming with small-scale devices. Most were caused by truckers trying to defeat the electronic surveillance devices that tell their employers how long they drive and how fast, and when they stop for mandatory rest breaks.

But some of the jamming appeared to be caused by thieves seeking to disable security tracking devices in commercial vehicles, according to Charles Curry, whose company Chronos Technology Ltd. set up the network.

Table of Contents

Army Increases Leader Training on Cyber Threats

By C. Todd Lopez, FT. Leavenworth Lamp, Aug 23, 2012

Baltimore — An increased focus on training and leader development can help commanders at all levels better understand the threat to America posed by adversaries in the cyber domain, said the commander of Army Cyber Command, during the Armed Forces Communications and Electronics Association TechNet Land Forces East conference Aug. 16 in Baltimore.

"There is still more that can be done that causes leaders at all levels to understand and appreciate what it is going to take to operate and be able to conduct operations in land and cyber," said Lt. Gen. Rhett Hernandez, commander of ARCYBER. "I put a lot of energy into our exercise program."

Hernandez said ARCYBER has already participated in three brigade combat team-level training rotations at the National Training Center at Fort Irwin, Calif., and is working now to expand opportunities where commanders can really see the impact that the cyber threat has on operations. Included in that effort is expansion to the Joint Readiness Training Center level and also into Europe at the Combat Maneuver Training Center.

"Once commanders are allowed to see and understand what it takes to plan for and integrate, and we unleash a world-class cyber (opposing force) on them, they now have the ability to recognize what they have to protect, what they can take risk in, and where we might have gaps in our training, or in our capabilities," Hernandez said. "That will improve our ability to conduct operations at those levels."

Hernandez said that commanders who operate "all the way to the tactical edge" must learn the importance of the network, and the impact that threats to the network have on land operations.

"Every day at the tactical edge there is an absolute requirement to conduct operations that ensure that you are defending your network so you maintain the freedom to operate," Hernandez said. "That's not going to go away. What I believe will happen over time is we will have more convergence. We will train more as one team, and we will be able to bring cyberspace operations effects at all echelons, through all three lines of operations."

Those lines of operations, Hernandez said, include "operate, defend, and when directed, conduct offensive operations."

Mirroring the words of the Army's chief of staff, Gen. Ray Odierno, Hernandez presented to AFCEA conference attendees the roles of ARCYBER, in the cyber domain, in terms of the three roles that the chief has spelled out for the Army: prevent, shape and win.

Hernandez said that the network, mobile networks and the social media networks have the ability to both shape the battle space and to prevent conflict in the first place, and that commanders must come to understand the influence of those networks on operations.

"It is the social media that we all have a lot of work to do, and understand and appreciate it, because it is key to not only preventing but also shaping," Hernandez said. "We have seen from activities from around the world, particularly with the 'Arab Spring,' that it plays a significant role in winning."

The general said the Army has a lot of work to do in determining how to include social media as an operational issue and not just as a public affairs issue, and must determine what needs to be done to "prepare ourselves for that social media environment that will be a part of, I believe, any future contests."

With budget cuts on every Army commander's mind, Hernandez said the Army must be smart in how it prioritizes the threat in the cyber domain, and how it allocates limited funding to combat those threats.

"What's on us is to ensure that we clearly articulate the most significant gaps and the requirements that need to be addressed — are prioritized in a way that give us the biggest effect for the least amount of cost," Hernandez said.

Hernandez said that DoD's plans for the "Joint Information Environment," which includes consolidated data centers, consolidated operations and management of network infrastructure, consolidated end-user services like e-mail, migration to cloud services, and standardization of hardware and software platform, are essential. Until the Joint Information Environment comes to fruition, he said the Army must focus on the essentials.

“Absolutely essential to this is our ability to bridge the gap between now and then with only those things we have to absolutely invest in to mitigate the most significant vulnerabilities and risk to the network,” Hernandez said.

Additionally, he said, the Army must remain focused on research and development to stay abreast of rapidly changing technologies.

The Army, he said, must “remain committed to identifying and articulating the most significant science and technology requirements we need for the future, so that they are not surprises, but we are ahead of the threat and we are investing in the right (research and development) capability that will be there before we need it and not too late.”

Table of Contents

ANSF Takes the Lead in Information Fight

By U.S. Army Sgt. William Begley, 11th Public Affairs Detachment, May 21, 2012

LOGAR PROVINCE, Afghanistan— Afghan National Security Forces are working hard to ‘take point’ in the information fight as the withdrawal of U.S. Forces in Afghanistan draws closer.

“The ANA guys are really on point here,” said U.S. Army Sgt. Kevin Kumlin, a team leader with the Tactical Military Information Support Operations Det. 1355, and Minneapolis native. “They have their finger on the pulse of the area and know what method of delivering information will work best.”

The ANSF are working closely with their coalition partners to learn various methods of communication to earn trust and build credibility with local populations.

U.S. Army Capt. Brian Gorre, a native of Mancato, Minn. and Tactical MISO Det. 1355 commander, said some of those methods are distribution of paper products, face-to-face engagements with key leaders, rapport building, and the use of radio broadcasts.

The broadcasts are one of the most effective methods because for years, free hand-crank radios, or “radios in a box”, have been distributed to local Afghan communities.

Afghan National Army commanders in partnership with U.S. Forces utilize RIAB to send messages, such as unexploded ordnance and improvised explosive device information, out to the populace. Radio is the primary method Afghans use in Logar Province to get news and other information since there are few or no TV stations, Gorre said.

“What we’ve done along with the ANSF is to get on the RIAB and have call in shows,” he said. “So when the locals call in to the station number they can get answers for most of their questions by local officials.”

Mohammad Masoom, a disc jockey for Radio Unity 94.9 FM, based in the Logar Province, has been doing his job for seven months.

“I can help the people through the radio shows,” said Masoom. “If the people have questions they can call in, and I give them answers.”

Masoom said he hopes for peace and a brighter future for Afghanistan.

“I enjoy my job because it gives me the opportunity to serve my people,” said Masoom. “I can also help bring prosperity to Afghanistan and to my people by doing my job. I can support my family because I make money here.”

Through the RIAB, ANA Col. Rahim Jan, officer in charge of recruiting in Logar province, has noticed an increase in recruitment for May.

“Last year in May we had 47 recruits,” said Jan. “But this year because of the help from our coalition friends and the rapport building item distribution we have 106 new recruits, and the month is not over. We are hoping to sign at least eight more for a total of 114.”

The broadcast detailed standards for Afghan citizens to join the ANSF, causing recruitment to skyrocket as a result of a simple message.

Rapport building items, or RBI, have been a huge bonus in Afghanistan, Gorre said. It takes time to build relationships and gain trust. The ANSF are responsible for distributing items to the local populace such as blankets to keep them warm during the cold winters and hand crank radios with rechargeable batteries to help them to receive radio broadcasts.

Besides building rapport with the local populace and using information operations to increase recruitment, the ANSF has also been effective at using messaging to counter enemy propaganda.

One of the methods insurgents use to instil fear in the heart of the Logar population is called a night letter. At night, when the villagers are asleep, letters are posted in villages with negative messages about the government and the ANSF.

U.S. Army 1st Sgt. Mark Malott, senior enlisted leader for the 340th Tactical MISO Co. and a native of Williamsburg, Ohio, credits the ANA for coming up with a solution to counteract these.

“The ANA came up with an idea called a confidence letter. It’s basically a letter that says while you were sleeping we were here to protect you,” said Malott. “So the locals see that they are being protected, and it gives them a feeling of security.”

Confidence letters, along with flyers informing the population about the dangers of UXO and IED’s are some of the ways paper products are used to provide the Logar population with information that can make their lives along with the lives of ANSF and U.S. Soldiers safer.

“Another huge problem within our area of operations is IED’s. The locals know what they look like; they know to stay away from them,” said Gorre. “However, young children still like to investigate, and kids will be kids. The ANSF has made sure the message gets out that it’s not only the business of CF to make sure that not only are we looking out for those dangerous items, but they are as well.”

And as the children grow older, and the 2014 withdrawal date nears, they will need to know more about their country than staying away from IEDs, and the ANSF, trained and mentored by their coalition partners, will be right there to help them.

Table of Contents

US General: We Hacked the Enemy in Afghanistan

By Raphael Satter, AP, 24 August 2012

The U.S. military has been launching cyberattacks against its opponents in Afghanistan, a senior officer said last week, making an unusually explicit acknowledgment of the oft-hidden world of electronic warfare.

Marine Lt. Gen. Richard P. Mills' comments came at a conference in Baltimore during which he explained how U.S. commanders considered cyberweapons an important part of their arsenal.

"I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact," Mills said. "I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."

Mills, now a deputy commandant with the Marine Corps, was in charge of international forces in southwestern Afghanistan between 2010 and 2011, according to his official biography. He didn't go into any further detail as to the nature or scope of his forces' attacks, but experts said that such a public admission that they were being carried out was itself striking.

"This is news," said James Lewis, a cybersecurity analyst with the Washington-based Center for Strategic and International Studies. He said that while it was generally known in defense circles that cyberattacks had been carried out by U.S. forces in Afghanistan, he had never seen a senior officer take credit for them in such a way.

"It's not secret," Lewis said in a telephone interview, but he added: "I haven't seen as explicit a statement on this as the one" Mills made.

The Pentagon did not immediately respond to an email seeking comment on Mills' speech.

U.S. defense planners have spent the past few years wondering aloud about how and under what circumstances the Pentagon would launch a cyberattack against its enemies, but it's only recently become apparent that a sophisticated program of U.S.-backed cyberattacks is already under way.

A book by The New York Times reporter David Sanger recently recounted how President Barack Obama ordered a wave of electronic incursions aimed at physically sabotaging Iran's disputed atomic energy program. Subsequent reports have linked the program to a virus dubbed Flame, which prompted a temporary Internet blackout across Iran's oil industry in April, and another virus called Gauss, which appeared to have been aimed at stealing information from customers of Lebanese banks. An earlier report alleged that U.S. forces in Iraq had hacked into a terrorist group's computer there to lure its members into an ambush.

Herbert Lin, a cyber expert at the National Research Council, agreed that Mills' comments were unusual in terms of the fact that they were made publicly. But Lin said that the United States was, little by little, opening up about the fact that its military was launching attacks across the Internet.

"The U.S. military is starting to talk more and more in terms of what it's doing and how it's doing it," he said. "A couple of years ago it was hard to get them to acknowledge that they were doing offense at all — even as a matter of policy, let alone in specific theaters or specific operations."

Mills' brief comments about cyberattacks in Afghanistan were delivered to the TechNet Land Forces East conference in Baltimore on Aug. 16, but they did not appear to have attracted much attention at the time. Footage of the speech was only recently posted to the Internet by conference organizers.

Table of Contents

Facespook: Russian Spies Order $1mln Software to Influence Social Networks

From RT, 27 August, 2012, 13:13

Russia's Foreign Intelligence Service (SVR) has ordered three systems worth about US$1 million that will automatically spread information on the Internet.

The systems were ordered in a three separate tenders and the official client's name is Military Unit 54939, but Kommersant Daily newspaper, which broke the news, writes that according to its sources this military unit belongs to the Foreign Intelligence Service's structure.

The first system is called Dispute and is responsible for overall monitoring of the blogosphere and social networks in order to single out the centers where the information is created and the ways by which it is spread among the virtual society. It also looks at factors that affect the popularity of various reports among internet users.

The second system, Monitor-3, will develop the methods of organization and management of a "virtual community of attracted experts" – setting of tasks, control over work and regular reports on chosen issues.

The third, and probably most important, of the systems is Storm-12 – its task is to automatically spread the necessary information through the blogosphere, as well as "information support of operations with pre-prepared scenarios of influence on mass audience in social networks."

The first two systems are to be ready by the end of 2012 and the third by 2013.

According to Kommersant, all three tenders were won by the company Iteranet, headed by a former deputy head of the Russian Cryptography Institute, Igor Matskevich, who previously worked on top secret state orders.

The newspaper claims that the tenders were held in a top secret mode and does not specify how the information was obtained or the reasons for deciding to disclose it.

Experts were cautious in their assessments of the new initiative. Russia's leading startup manager of internet projects Anton Nossik said that imbedded spam filters will resist the automated opinion-making systems and suggested that part of the budget must be spent on means to overcome this.

Another expert who preferred not to be named told Kommersant that the system can only be effective if its activities go beyond the legal sphere – like hacking the administrators' rights on social networks, mass messaging or even infecting the users' computers with automatic "bot" programs.

The head of the Russian association Center for Safe Internet, Urvan Parfentyev, said that the news was a natural development of conventional propaganda means, like the Voice of America and RFE RL radio stations, only on the internet.

Table of Contents

Software Company Denies Spy Agency Collaboration

By Mikhail Fomichev, RIA Novosti, 27/08/2012

MOSCOW, August 27 (RIA Novosti)

A Russian IT company denied on Monday any involvement in a project to develop software to monitor social networks and influence public opinion for the country's intelligence services.

Kommersant daily reported earlier in the day that the Iteranet company had a contract with the Foreign Intelligence Service (SVR) of the General Staff of the Russian Armed Forces. The daily calimed that the SVR has ordered three systems worth about US$1 million.

"We are not in the business of developing systems to monitor blogs and plant information in the blogosphere," Iteranet CEO Igor Matskevich told RIA Novosti.

“There have been no contracts of the type Kommersant claims. We do not engage in such activity.”

He declined to elaborate.

Kommersant said Iteranet’s SVR contract included systems to monitor and control the blogosphere and shape public opinion by spreading “special information” in social networks.

Table of Contents

Pentagon Fighting Taliban on Social Media Front

By Jim Michaels, USA Today, August 30, 2012

WASHINGTON — The U.S. military is ramping up efforts to counter the Taliban's growing presence on social media sites by aggressively responding to falsehoods and reporting violations of the sites' guidelines on violent threats, experts say.

Twitter accounts or websites associated with militant groups typically take responsibility for attacks whether or not they had anything to do with them.

But most of the information they provide is either exaggerated or false, said Army Lt. Col. T.G. Taylor, a spokesman for U.S. Central Command.

The Pentagon has become quicker and more effective at issuing rebuttals through Twitter and other venues, said Christopher Paul, an information operations analyst at RAND Corp.

"Insurgents have always wanted to make themselves look like winners," Paul said. "The Internet makes it a whole lot easier."

Winning the information war is particularly important in insurgencies, where shaping public opinion can count as much as what happens on the battlefield.

The Taliban and other militant groups issue statements and video to create a perception of chaos in the country and to undermine the legitimacy of the Afghan government.

Despite the Taliban's hostility to modernity, they have adapted well to social media, military officials said.

"They're all over Twitter," said Marine Lt. Col. Stewart Upton, a spokesman for Regional Command Southwest. "They're incessantly tweeting."

Internet access remains limited in Afghanistan, but increasingly people have cellphones and Taliban claims often spread from social media to satellite television and local news outlets. Militants also use a variety of languages on the Internet, including English.

The military has long struggled with how to counter enemy propaganda in Afghanistan. Insurgents post claims quickly and the military had been slow to respond, waiting to get the full story.

"We're getting better," Paul said. "There's a practical limit to how good we can get."

The military says it has reported militants when they have directly promoted violence.

Twitter could suspend an account if a user violates policies. Twitter spokeswoman Rachael Horwitz said the social networking service does not discuss specific accounts, including military requests.

Over the past year, Central Command, which oversees U.S. military operations in the Middle East, has reported about 10 social media violations by militants, Taylor said. In general, however, officers say they prefer to engage the Taliban openly rather than impede their right to free speech by trying to deny them access to the Internet.

"That would make it look like we're afraid to engage them on the moral battlefield and we're not," Upton said.

The more aggressive approach seems to be working. Increasingly, local media are seeking out the coalition for its side of the story and eying Taliban claims more skeptically than in the past, the military said.

This week the Taliban took to Twitter to deny responsibility for the recent beheadings of 17 Afghans. The Afghan government dismissed the statement, saying the Taliban was responsible.

Table of Contents