Information Operations Newsletter

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

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

ARSTRAT IO Newsletter Online

Table of Contents

Vol. 14, no. 01 (October – December 2013)

How to Fight Cyber War? Estonia Shows the Way

By Indrani Bagchi, TNN, Oct 17, 2013

NEW DELHI: Estonia is the Hiroshima of cyber war.

In April 2007, the new government decided to move a Soviet-era war memorial to a location outside the capital, Talinn. Pro-Soviet elements came out on the streets to protest. Then, the cyber attacks started. Within hours, the attackers brought down the tiny country's banks, newspapers, news agencies and all government sites. The rioters raged outside.

"A cyber attack is not virtual, it's a real thing. People get scared, and governments have to respond. When the tools of modern governance are brought down, that is scary. This was the first time a cyber threat became a real national security threat," said Jaak Aaviksoo.

Aaviksoo was the defence minister and was responsible for the both the decision to move the statue, Bronze Soldier of Talinn, and the fight back against the cyber attack. In India for a conference on cyber-governance, Aaviksoo, now heading the country's education and research ministry, spoke to TOI exclusively on what a cyber war looks like and what lessons the world, particularly India, should draw from Estonia.

Today, Estonia is a global leader in cyber defence, not to speak of the fact that it is birthplace for Skype and FastTrack and the first full e-government.

This country, which joined the EU and Nato after breaking away from the Soviet Union, is now a global leader in cyber awareness and cyber education. In the years after Estonia was hit by a cyber-tsunami, cryptography and cyber-security are all courses taught in the nation's colleges and schools. More interestingly, students between five and 15-year-olds are learning to write computer code as part of a countrywide campaign to inculcate a culture of "cyber-hygiene" in the next generation.

"It's like safe sex," Aaviksoo said. "You need to know there are certain things you should not do."

In April 2007, the attacks came in waves, but by the third week, Estonia was learning to manage. "There were a few things we learned from the cyber onslaught," he said. First, you cannot tackle this alone. Countries and societies need networked partners who can be trusted.

Second, traditional command and control structures have to be destroyed. "Cyber attacks happen in seconds. You have no time for an emergency cabinet meeting."

Trust, share, cooperation between private and public entities, Aaviksoo reasoned, "have to be done not by imposition of a law, but a more horizontal agreement among government, private sector, civil society." The first responders to an attack may not be official since it could well be civilian because most critical infrastructure is in private hands.

Significantly, public awareness and education is imperative. "The attack started with one person plugging a USB drive into an infected computer. A cyber threat is neither abstract nor remote. You are vulnerable and you have to behave responsibly."

What are the evolving cyber threats? "The cyberspace is not a threat per se. It is important to understand the interests and motivations behind an attack," Aaviksoo said. "In strategic terms, it is almost impossible to bring down a nation through the cyberspace. But it's possible to destabilize a country."

For instance, rumours, disinformation are weapons in this new-age war.

In 2012, there was a panic exodus of north-easterners from south India in a tell-tale sign of a cyber attack. "Responses have to be in the same medium, instant, and not top-down."

Table of Contents

Utilizing Social Media during Major Events

Product of the Research & Information Support Center (RISC), *OSAC Website*, downloaded 17 Oct 2013

The following report is based on open source reporting.

Executive Summary

Social media monitoring is a useful way to gain real-time, actionable insight into activities surrounding major events that could impact the way an organization operates or responds in times of crisis or heightened security risk. Successful social media monitoring during major events depends on the ability to collate, filter, and consume information flowing through digital channels quickly and succinctly. Success depends on understanding and using a suite of monitoring tools and techniques and a willingness to be creative and flexible.

The Event

Successful social media monitoring during a major event means quick adaptation and acclimation to the conversations, the players, and the methods of communication. During the upcoming Sochi Olympics, for example, there will be innumerable conversations on Facebook, Twitter, the Russian social media site VKontakt (VK), message boards, or other social media platforms.

While a certain degree of preparation is possible -- i.e. learning what social networks are commonly used in a given country or region -- discussions about a major event will include its own targets, lingo/terminology, threats and players. Therefore, a degree of learning spontaneously should be expected.

Before the Major Event

Social media planning should occur before a major event takes place. First steps might include:

- Researching key social media platforms
- Locating relevant conversation threads and hashtags
- Locating relevant Facebook pages (if applicable)
- Identifying websites, Twitter feeds, MeetUp, and other social media sites with anti-event ideology
- Research open source news on past events' disruptions
- Determining influential social media users
- Setting up Google News/Google Alerts to track media reporting and media surrounding social media

During the Major Event

During a major event actively monitor social media:

- Discard abandoned hashtags: Once the conversation stops, do not look for it to start up again. Social media, like conversations, are ephemeral.
- Constantly search for new influencers: The list is not static. As conversations grow and change, so will the conversation drivers.
- Use social media as a starting point for further research. Often, social media users send each other links to relevant stories, photos, or videos. Follow links to other media in conversations.

Best Practices for Processing Information from Social Media

In order to best track incidents, such as widespread protests that may occur during major events, break each protest down and tailor social media searches to specific, key words ("fill in the blanks") on a particular event. It is important to determine the "who, what, where, when, why, and how."

- Search actively for key words or phrases indicative of a protest. This includes words or phrases relating to the event, geography around the location of an event, events covered in the news surrounding the event, partner organizations supporting the event, or stakeholders involved in planning or executing the event.
- Learn the influencers. See who is tweeting, posting to Facebook, or using other social media platforms on matters related to your event.
- On Twitter or other microblogs: Follow hashtags. Many protests use specific tags tied to events to identify genuine information. For example, #feb20 was used widely in the Arab Spring by Egyptians in Tahrir Square.
- On Facebook or similar "profile"-based systems: Search for groups, users or "fan" pages that contain keywords derived from your searches, relate to your events, or are followed by influencers you are monitoring.
- On message boards: search for message boards relating to the upcoming event. It is not likely that protests will be discussed as openly on messageboards, but with careful investigation, it may be possible to associate a Facebook or Twitter account with a message board user. They may use a similar alias on either platform.

When monitoring social media for private sector interests:

- Incorporate keyword searches relevant to the private sector interest or OSAC constituent in the strategy.
- Target searches by location as closely as possible – if partner X is in Chennai, search for key locative terms in that city or surrounding region.
- Work with private sector stakeholder communications teams to gain insight into their process, high-level influencers, common hashtags, important message boards, or other relevant social media concerns.

- When monitoring logistics, transportation breakdowns, road closures, traffic, crime, or police activity, follow local law enforcement accounts.

When monitoring social media for threats, it is important to assess the veracity of the threat and the reliability of the social media account on which the information was posted.

- To that end, social media monitoring must be done in concert with other aspects of intelligence gathering to provide additional information. On social media, it is very easy to hide an identity.
- Consider, also, that social media can be a platform to blow off steam, so while text may appear threatening, it may be used as a social medium for airing grievances and garnering sympathy or support.
- Further, as with other types of threats, attention must be paid to determine locative or intentional clues – common keywords used, for instance.

After the Major Event

After the major event, take time to note any lessons learned on the social media front and make adjustments to social media strategies and best practices for future events.

Monitoring Tools and Techniques

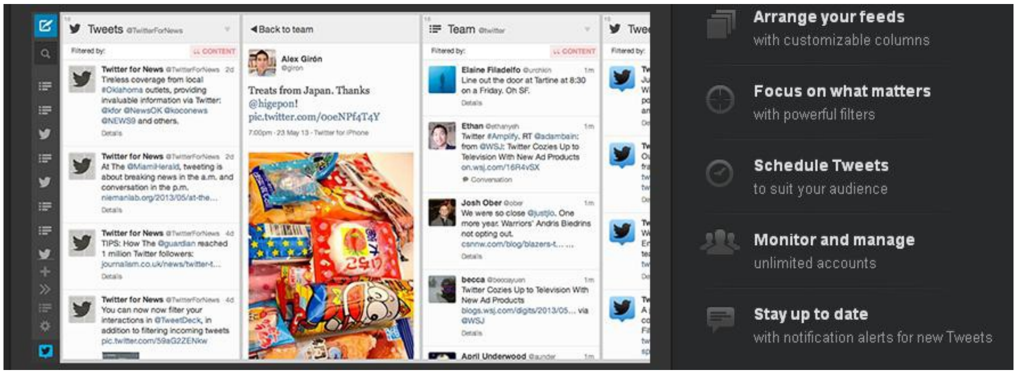
A major event often will fuel a significant amount of discussion on social media outlets. Topics range from the event itself -- i.e. specific participants in the Olympic Games, results of recent events, or even the experience of spectators at the events. Knowing how to target social media research in order to focus on the most relevant information is key. This means actively monitoring social media, a process that can be very time and resource intensive. Therefore, consider these suggestions on how to filter, process, and consume large amounts of information. These processes and tools will be discussed in greater detail in subsequent sections.

- Keep updated and granular keyword or hashtag searches running in a social media aggregator tool, like HootSuite or TweetDeck. These services allow users to implement multiple streams per social media platform. Create a new one for each search term whenever possible.
- Journal instances where keyword search or hashtag led to a new influencer or ongoing, relevant conversation. Map connections using mapping tool.
- Monitor hashtag or keyword search traffic actively. If a conversation stops, stop monitoring it.
- Whenever possible, use mapping software – both relationship mapping and, if applicable, a "pinning" tool like Google Maps to track spread of tweets or of events discussed in tweets.

Social media content is, by design, fast-moving and ephemeral. Conversations on social media progress quickly, almost in real-time. If you are not archiving them or taking notes closely, you may lose track of them. In order to get the most out of social media monitoring, one must be monitoring it constantly and be ready to record significant conversations.

Various tools are available online to help users expand the number of social feeds that can be observed at any given time. Two commonly-used tools include TweetDeck and HootSuite.

TweetDeck



Tweets @TwitterForNews

Filtered by: CONTENT

Twitter for News @TwitterForNews · 2d
Tireless coverage from local #Oklahoma outlets, providing invaluable information via Twitter: @kfor @NewsOK @koconews @NEWS9 and others.
Details

Twitter for News @TwitterForNews · 2d
At The @MiamiHerald, tweeting is about breaking news in the a.m. and conversation in the p.m. niemanlab.org/2013/05/at-the...
Details

Twitter for News @TwitterForNews · 4d
TIPS: How The @guardian reached 1 million Twitter followers: journalism.co.uk/news/twitter-t...
Details

Twitter for News @TwitterForNews · 4d
You can now now filter your interactions in @TweetDeck, in addition to filtering incoming tweets pic.twitter.com/59aG2ZENkw

Back to team

Alex Girón @giron
Treats from Japan. Thanks @higepon! pic.twitter.com/ooeNPf4T4Y
7:00pm · 23 May 13 · Twitter for iPhone

Team @twitter

Filtered by: CONTENT

Elaine Filadelfo @urchin · 1m
Line out the door at Tartine at 8:30 on a Friday. Oh SF.
Details

Ethan @ethanyeh · 1m
Twitter #Amplify. RT @adambain: from @WSJ: Twitter Cozies Up to Television With New Ad Products on.wsj.com/16R4vSX
Conversation

Josh Ober @ober · 1m
We were so close @justjo. One more year. Warriors' Andris Biedrins not opting out. csnnw.com/blog/blazers-t... ...
Details

becca @beccayuen · 1m
Twitter Cozies Up to Television With New Ad Products blogs.wsj.com/digits/2013/05... via @WSJ
Details

April Underwood @aunder · 1m

Arrange your feeds
with customizable columns

Focus on what matters
with powerful filters

Schedule Tweets
to suit your audience

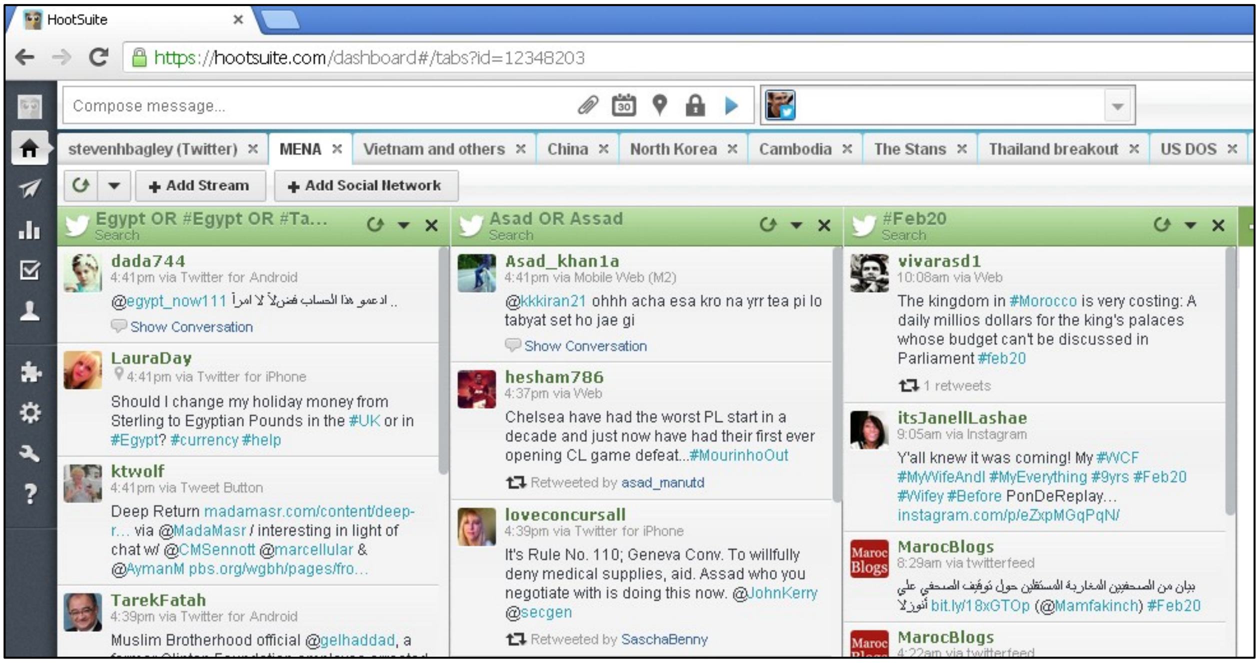
Monitor and manage
unlimited accounts

Stay up to date
with notification alerts for new Tweets

TweetDeck landing screen, www.tweetdeck.com/

TweetDeck is a free web-based platform produced by Twitter that allows a user to watch multiple streams at once, including live-updating searches for key words or phrases, popular hashtags, track messages sent to or from the user's Twitter account, and schedule tweets.

HootSuite



dada744
4:41pm via Twitter for Android
@egypt_now111 ادعمو هذا الحساب فضلاً لا امراً ..
Show Conversation

LauraDay
4:41pm via Twitter for iPhone
Should I change my holiday money from Sterling to Egyptian Pounds in the #UK or in #Egypt? #currency #help

ktwolf
4:41pm via Tweet Button
Deep Return madamasr.com/content/deep-r... via @MadaMasr / interesting in light of chat w/ @CMSennott @marcellular & @AymanM pbs.org/wgbh/pages/fro...

TarekFatah
4:39pm via Twitter for Android
Muslim Brotherhood official @gelhaddad, a

Asad_khan1a
4:41pm via Mobile Web (M2)
@kkkiran21 ohhh acha esa kro na yrr tea pi lo tabyat set ho jae gi
Show Conversation

hesham786
4:37pm via Web
Chelsea have had the worst PL start in a decade and just now have had their first ever opening CL game defeat...#MourinhoOut
Retweeted by asad_manutd

loveconcursall
4:39pm via Twitter for iPhone
It's Rule No. 110; Geneva Conv. To willfully deny medical supplies, aid. Assad who you negotiate with is doing this now. @JohnKerry @secgen
Retweeted by SaschaBenny

vivarasd1
10:08am via Web
The kingdom in #Morocco is very costing: A daily millios dollars for the king's palaces whose budget can't be discussed in Parliament #feb20
1 retweets

itsJanellLashae
9:05am via Instagram
Y'all knew it was coming! My #WCF #MyWifeAndI #MyEverything #9yrs #Feb20 #Wifey #Before PonDeReplay... instagram.com/p/eZxpMGqPqN/

MarocBlogs
8:29am via twitterfeed
بيان من الصحفيين المغاربة المستقلين حول توقيف الصحفي علي
أنوزلا bit.ly/18xGTOp (@Mamfakinch) #Feb20

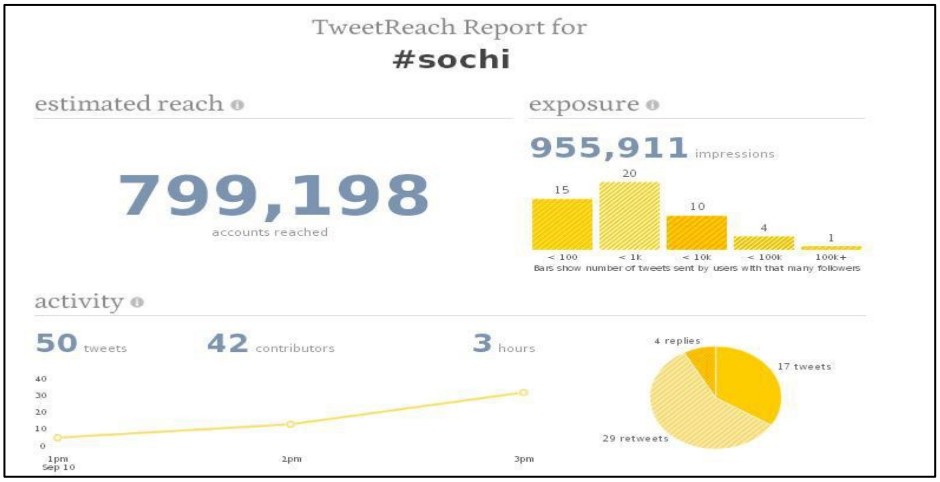
MarocBlogs
4:22am via twitterfeed

Hootsuite's free version: www.hootsuite.com

HootSuite, a more robust platform, allows synching with up to five social media accounts to enable the user to monitor not only several social networks at once but also several search terms or hashtag per each social network, all in one application. This makes it much easier to incorporate multiple platforms into a social media monitoring or engagement strategy.

TweetReach

A crucial metric to understand about social media is the "reach" of a given piece of content. TweetReach, a free service, examines the exposure a given hashtag, search term, or tweet has received by highlighting several metrics. Among other things, TweetReach shows how many Twitter accounts have seen the search term, who tends to be retweeted most, and which tweets are shared most frequently.



Topline search results on TweetReach. *www.tweetreach.com*

By breaking down tweets by their influence and highlighting whose tweets on a given topic go farthest, TweetReach is a tool for tracking the spread of conversations about an event.

Google Alerts/Google News

In addition to monitoring the social streams during major events, Google News/Google Alerts, or another news crawler, is very useful. Given the likelihood that it is already part of a suite of tools used during a major event, its inclusion on this list is to note the importance of monitoring the news media's coverage of social media, an increasingly common phenomenon. In 2011, the Arab Spring would not have spread as far and as fast as it did had the mainstream media not been covering social media activity. Using Google News/Alerts to monitor reporting of social media content will help to identify key social media influencers, topics of discussions, and hashtags.

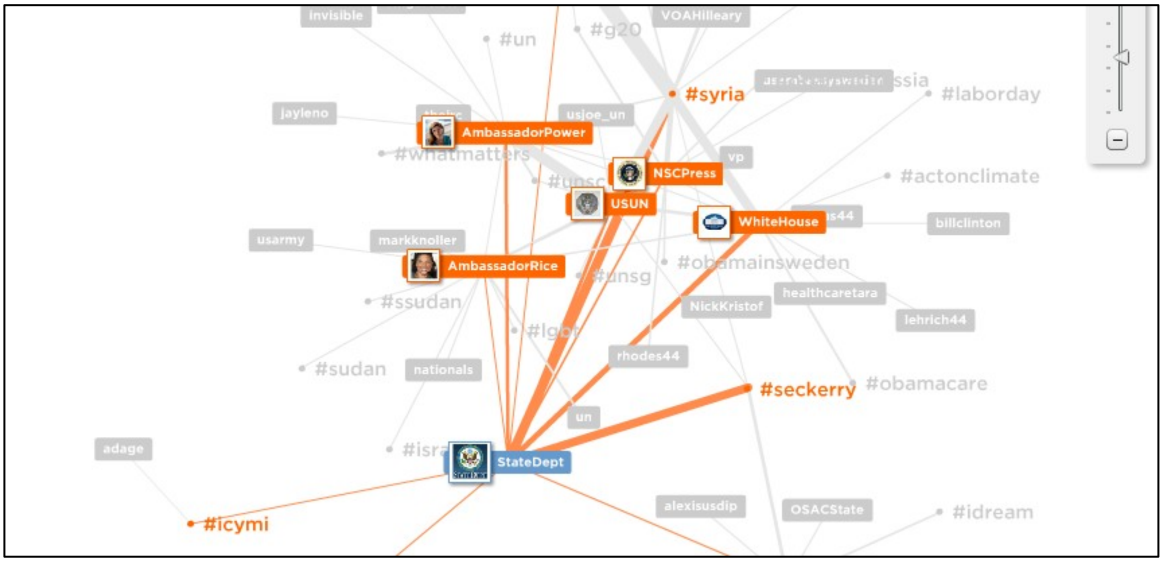
Mapping Influence

A good way to think of social media monitoring is to pay attention to several conversations, often about several topics, in several places at the same time. At first, it is overwhelming, but with training, it becomes easier to find relevant pieces of information and threads to follow. "Spending time on the ground" means getting to know the relevant aspects of social media exchanges. By delving into a particular conversational ecosystem, it becomes evident which influencers and hashtags to follow.

- Influencers: Twitter/Facebook/VK users whose tweets/content are widely disseminated, replied to, retweeted, or commented on.
- Hashtags: searchable indexing functions (i.e. #sochi) that demarcate conversational threads. When #sochi is added to a tweet, the tweet will be displayed among Twitter's search results relating to the upcoming Olympic Games in Russia.

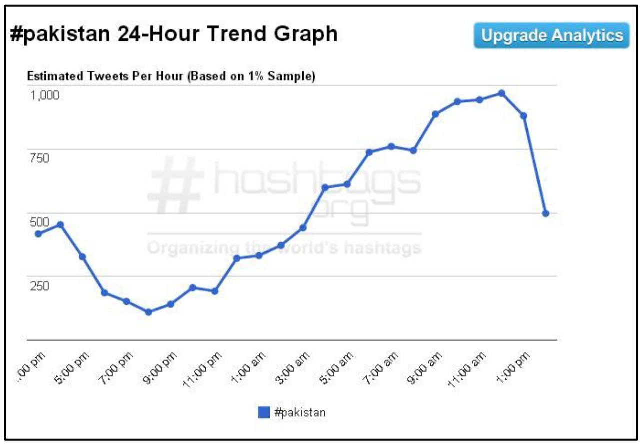
In addition to "spending time on the ground," there are tools available to track the spread of conversations and the relationships between influencers.

The free web-based platform MentionMapp is able to draw a map tracing relationships between social media influencers and key conversation topics. As shown below, Twitter influencers tend to retweet each others' content. Take, for instance, the Department of State's official Twitter account's map of influence:



A visual way of tracking relationships between influencers on Twitter. www.mentionmapp.com

On this map, the number of engagements between Twitter feeds is indicated by the thickness of the line between influencer and influencer or influencer and hashtag. This tool displays the volume of a hashtag's mentions in the preceding 24 hours. For example, clicking on #pakistan generates this graph, at hashtags.org:



#hashtag activity in last 24 hours. *www.hashtags.org/.*

From within MentionMapp, it is possible to track a hashtag’s engagement among Twitter influencers, as well. Mapping data – including a map of influencers’ communications and a map of the hashtags associated with a certain conversation topic – will demonstrate how influencers and conversation topics relate to each other.

Mapping events is also an important aspect of social media monitoring. With Google Maps, an open, free platform, it is possible to “pin” data points on a geographic map, indicating where events occurred. This is a useful tool in situations where events are described on social media: with a tweet’s timestamp and geo-location information, it is possible (and recommended) to track the spread of a tweet across the globe or to track tweets about a particular event in a location associated with a major event.

Influence

The social media users in Tahrir Square outpaced the mainstream media and created a situation whereby traditional influencers were subverted by social media users on the ground. That is why it is important to see whose content is connected to whose via a mapping service like MentionMapp; it is equally important to determine where social media users are physically located. That way, in situation-specific events, such as the upcoming Olympic Games, the additional variable of geography may help to determine how much weight to give a social media user. If two users’ tweets on #sochi are widely shared, but one user is based near the Games, that user’s tweets may be more accurate. That user’s information may also be more widely disseminated by other influencers, including reporters.

Conclusion

Social media is an invaluable tool to monitor the digital conversation surrounding a major event. Not only is social media a strong view into sentiment surrounding the event, it may also provide insight into planned security risks or attempts to cause damage or disruption during the event. In addition to monitoring and tracking social media content, tools like TweetReach or Mention Mapp can help to qualify and quantify social media users’ engagement and connections. Understanding the tools and techniques that are available will improve efforts to account for social media content during a major event.

Table of Contents

Google Launches Project Shield Cybersecurity Initiative for 'Free Expression'

From Reuters, October 22, 2013

Google Inc will begin to shield news organizations and human rights groups from cyberattacks as part of a new package of services designed to support "free expression" on the Web, the internet giant said Monday.

At a presentation in New York, the company also unveiled a new technology called uProxy that allows citizens under some regimes to bypass government censorship or surveillance software to surf the Web. The software will be available for Google's Chrome browser and Firefox but not for rival Microsoft Corp's Internet Explorer, at least initially.

The world's No. 1 search engine presented the two services - as well as a new map that highlights cyberattacks taking place around the world in real time - as some of the most significant software products to emerge from Google Ideas, a think-tank established by the company in 2010.

Known for its "Don't Be Evil" corporate motto, Google has a well-established reputation for resisting authorities around the world who seek to censor its Web properties, including YouTube and Blogger.

But the formation of the Ideas group, which the company advertises as a "think/do tank" headed by Jared Cohen, a former U.S. State Department official, has raised the possibility of the company playing a more active role in furthering U.S. policy.

Under its "Project Shield" initiative, Google said it would host sites that frequently came under politically-motivated distributed denial-of-service attacks. Because of the size and sophistication of its technical infrastructure, Google is far more able to withstand such attacks compared to websites hosted independently.

The product remains in testing, Google said. A promotional video made by Google featured an endorsement from Balatarin, a popular Persian-language news website that has already tested the digital shield program. Google has also worked to protect an election monitoring website in Kenya, according to Forbes.

The uProxy software, funded by Google but developed by the University of Washington and nonprofit group Brave New Software, will allow users in countries like China to access the Internet as it is seen by a friend in a different, uncensored country.

The software creates an encrypted connection between two users in a way that resembles a virtual private network - a method that savvy Chinese netizens currently use to circumvent the government's Great Firewall, which blocks many social media sites.

Google said uProxy also remained in testing.

Table of Contents

U.S.-Style Personal Data Gathering Is Spreading Worldwide

By Adam Tanner, Forbes, 16 Oct 2013

Data brokers are gathering ever more personal data about people worldwide, including, perhaps, these women at Ipanema beach in Rio de Janeiro, Brazil. Data brokers have gathered hundreds of millions of dossiers in Brazil, and billions worldwide. (Image credit: AFP/Getty Images via @daylife)

U.S. firms and marketers are often portrayed as especially rapacious and aggressive in their collection and use of our personal data. Yet the trend of gathering as much information about potential and existing clients as possible is spreading fast worldwide.

Pick a target group in a far off land and data brokers can often produce a list of people with addresses, emails and a list of consumer characteristics. “For example, you might be interested in female, affluent consumers in China, Hong Kong and Singapore,” the California data broker Infocore advertises in its international data catalog. “From that we’ll access our repository and send you a custom data summary.”

Infocore has access to 6.5 billion personal records worldwide: 1.9 billion personal records in Asia, 1.65 billion in Europe and 1.2 billion in Latin America, with Brazil far ahead of other Latin America countries. Africa and the Middle East lag behind in personal data collection, which means Infocore has access to just 55 million records. By next year, Infocore expects to have access to 10 billion records worldwide (yes, that is more files than there are people in the world as companies have multiple data records on some people and none on others).

Such personal data files are built on public records, warranty card information, contest applications, online forms, smartphones and other sources.

Kitty Kolding, Infocore’s president and CEO, says her clients marketing to individuals abroad include some of the world’s best-known multinational companies such as Cisco, IBM, Dell, Netflix, Disney, Kimberly-Clark and big auto manufacturers. Major U.S. data brokers such as Acxiom and Merkle are also major clients of Infocore, she says.

Infocore sold 150 million records over the past year. Consumer data files typically cost $80 to $450 per 1,000 names, and some clients buy millions of dollars worth of foreign personal data files a year. “The economy is healthier than it was. Marketers are far more willing to spend then six or 12 months ago,” she says.

At the annual Direct Marketing Association conference this week in Chicago, an increasing number of firms are looking to take advantage of the spread of U.S.-style data gathering abroad. “More organizations are asking for multicountry/global solutions,” Experian, a major U.S. data broker, wrote in a recent report.

In some countries, commercial collection of consumer files dates back for decades, in other places such files are relatively new. “Turkey is very prominent right now. The data industry is very nascent right now,” Kolding says. “But there is a lot of long term profit to be had.”

Some countries are more restrictive in what personal data can be gathered, with Europe a prime example. But even within Europe, some countries allow access to personal data that would be considered intrusive by American standards. For example, in Sweden, marketers who obtain a person’s social security number, which might come from signing up for a loyalty program, can then access government files on that person including tax revenue information, says Peter Trap, director of international business development at Bisnode, a European data broker with annual sales of 450 million euros. The Netherlands has super precise postal codes, to the extent that some buildings have different codes for different parts of the building, so knowing the ZIP code tells a marketer a lot.

Spain, by contrast, is especially restrictive, and does not allow the merging of different records, meaning that if one store knows your phone number and the other your email address, they cannot create one master file.

In the big picture, with every passing day, marketers are collecting ever more information worldwide. “The trend is there to collect more, and more powerful data,” says Trap, whose company has access to 350 million personal data dossiers in 19 European countries. Their largest client is consumer goods company Procter & Gamble.

As companies worldwide have begun to realize the value of personal data, some have taken shortcuts in putting together marketing lists of people who would not expect that their data would be commercially sold. “There is a lot of data which is very questionably obtained,” said Kolding. “In China there is way more data than you would think. Some of it is dodgy.”

Some of these practices date back a long time. One example emerged soon after the collapse of the Soviet Union. Someone obtained all of the home phone numbers in Moscow, including unlisted ones, and published them on a CD selling for a dollar or two at local markets. Among those whose home number was included was the former president, Mikhail Gorbachev.

Table of Contents

How They Think: PME in the Modern PLA

By John D. McRae, Small Wars Journal, October 22, 2013

Background

The People’s Liberation Army (PLA) can be thought of first and foremost as the tool by which the Communist Party of China (CPC) retains power. As Mao Zedong succinctly put it, “Our principle is that the Party commands the gun, and the gun will never be allowed to command the Party.” (Jan, 1999, p. 1241) As potentially broad as this “protection’ mission is, it defines the framework of how the Party and the PLA understand one another, and in turn how the PLA operates. In conjunction with this core function, the PLA serves the familiar purpose of most modern armies, the defense of its borders, be they maritime, aerial, or land. The PLA also finds itself in the midst of a new evolution in combat, the so-called “Cyber domain”. Given this broad and evolving mission set, the accession, training, and educational system of the PLA must adapt to develop the leaders necessary to counter a variety of threats in the service of the CPC. Although its track record has historically been spotty with regard to modernity, the PLA has undergone a transformation in the past decade aimed at keeping pace with peers; an effort that has yielded clear dividends.

In the wake of the Cultural Revolution, CPC leaders sought to decentralize control of the PLA to an extent in an effort to avoid future interference in political-civil relations. Used as both an agent of implementation and order during the Cultural Revolution with arguably disastrous results, the PLA stood as an impotent force both internally and externally in the early 1970’s.

This de-fanging came about via the carefully orchestrated rotation of PLA units and their leaders and the exodus of PLA members from leadership roles within the CPC. (Whiting, 1974, p. 2) Of course, this effort also had the destabilizing effect of diminishing unit cohesion and effectiveness given the traditionally localized nature of PLA units. The destabilizing effects of this initiative were readily apparent in the lackluster Chinese showing in the Sino-Vietnamese War of 1979. (Saghal, 2011)

A New Way Forward

The modernization of the Chinese military subsequent to the Sino-Vietnamese War was predicated on a new set of assumptions, namely that the nature of warfare that the Chinese would be most likely to face was now a “local, limited war” rather than the “early, major, and nuclear war” that Mao foresaw. (Blasko, 2005, p.68) The decline and breakup of the Soviet empire was one significant factor enabling the Chinese to develop a PLA more focused on quality than sheer volume of troops. As a part of that effort, the PLA overhauled many facets of the force in an effort to further professionalize, strengthen, and streamline the organization, an effort that is still ongoing. Among these efforts were:

- Reduction in force size.
- Changes in force structure.
- Reform of the structure and missions of the reserves and militia.
- Changes in the personnel system.
- An influx of new equipment.
- Doctrinal revision to prepare the PLA to fight and win Local Wars Under Modern High-Technology Conditions or Local Wars Under Informationalization (sic) Conditions.
- Improvements in the frequency, content, and methods of military training, with emphasis on joint operations.
- Transformation of the PLA logistics system.
- Enhancement of all soldiers' standard of living, pay, and lifestyle.
- Modification of the professional military education system.

This last effort is among the most significant. The PLA's officer training program had virtually ceased to exist in the 1970's. (Dreyer, 1996, p. 318) New standards implemented in the 1980's dictated that PLA officers must now be graduates of military academies. (ibid) Rather than conduct a wholesale purge of currently serving officers, however, the PLA elected to gradually bring around serving officers to new educational standards by conducting part-time courses that would enable them in theory to have the benefit of the same professional education that newly accessed officers were privy to. By raising the standard for all, the PLA hoped to ensure that the widespread and detrimental lack of formal education among its officer corps could be eradicated, and in its place a tri-tier educational system could be implemented on a permanent basis. (ibid)

First among these military schools were regional academies meant to develop a junior officer corps with a common set of military and civilian skills. The most apt comparison with the US military's educational system would be the handful of all-cadet Reserve Officer Training Corps, or ROTC schools such as the Virginia Military Academy or The Citadel. The regional military academies were similarly fashioned to provide a college education simultaneous with military training, ensuring that new officers would in fact be better trained and educated than the troops they were charged to lead. Although a common concept in Western militaries, this was a fairly transformative step for the PLA and did much to professionalize and standardize the military almost immediately. One factor helping the regional military academies attract promising candidates was the fact that these academies did not charge tuition like their highly competitive civilian counterparts. (ibid, p. 320)

The next tier of military education implemented in the PLA was for mid-career officers at the rank of captain and major. This course, known as the command college, prepared select officers for positions of increased responsibility, such as the command of a regiment. (ibid) This course serves both as an educational milestone for PLA officers and as a weeding apparatus that separates those promising few on the "command track" from those destined to remain at the lower rungs of the PLA until separation or retirement. The course is also available in different parochial "flavors" that allowed specialized officers such as engineers the chance to hone their unique skills. (ibid)

The upper tier of military education implemented in the PLA during its period of modernization was the National Defense University (NDU), a program analogous to the various War Colleges found in the US branches of the armed services. A yearlong course designed for only a select few officers being groomed for top positions, the NDU was formed in 1985 from the three extant senior military schools known as the Military Academy, the Political Academy, and the Logistics Academy. (ibid) A separate two-year course at the NDU prepared officers for divisional command, and a one-year course prepared the very upper tier of PLA flag officers for command of corps and armies.

Interestingly, the final, culminating course taught at NDU known as the Capstone is not based entirely on merit. An effort is made to diversify the rolls of the course along regional lines. "A balance among the military regions and service headquarters is sought, with regional commanders and headquarters deciding who will represent their commands in the class. Participants are not necessarily selected for their past performance or promotion potential, nor do they necessarily have any particular insights about their regions' or headquarters' responsibilities." (ibid) Despite the efforts of the PLA to strengthen its officer corps from the bottom up, the pervasive influence of Chinese politics and regionalism persists. Perhaps in a country comprised of such disparate economic, ethnic, and geographic populations, some effort to artificially create a heterogeneous pool of senior officers is to be expected. After all, they typically return to their regional headquarters following formal schooling, and are then expected to assimilate back into the "stovepipe" reality of their regions, wherein the economic, security, and party politics of the area play the dominant role.

Curriculum

The structure of the PME system in the PLA is no doubt a significant step forward in the creation of a professional officer corps. The other significant consideration in the overhaul of PME in the PLA is the curriculum by which leaders are taught both "what" and "how" to think. This aspect of Chinese PME gives us true insight into how the Chinese military views itself, its mission, and its array of perceived threats in the world at large. By carefully examining the content and structure of the curriculum of the military academies, command college, and National Defense University, it is readily apparent that the PLA is quite serious about creating a modern, sophisticated, and agile organization led by knowledgeable officers capable of countering the myriad threats facing the world's fastest growing economy.

To understand the driving factors shaping the curriculum of the junior officer education system, it is useful to understand the strategic guidance that the academies are using to develop their material. Announced by President Jiang Zemen in 1995, the so-called "Two Transformations" of the Chinese military: a force built on quality rather than quantity, and a mindset focused on modern, high-tech conditions, are the broad strategic underpinnings that drive education at all levels, beginning with newly minted company-level officers. (Snakenberg, 2011, p. 105) One new focus area for the PLA is the education of its non-commissioned officer force (NCOs). Traditionally known as the backbone of any military, the NCOs are the executors of the orders issued by commissioned officers. Thus, it is striking that the PLA allowed NCO education to take a backseat to officer education for generations.

The change in attitude toward the NCO corps of the PLA is a recent one, with the traditional role of the NCO understood to be one of "leader in rank only", and a weak educational system to support that end. Training was focused at the most basic level: "literacy, basic tactics, and political instruction." (ibid) Most crucially, the aspects of leadership training so vital to a professional NCO corps were entirely lacking. "The army expended little effort in educating NCOs beyond minimum functional requirements, and did not intend for them to perform any meaningful leadership role." (ibid) This lack of leader training at the NCO level is unthinkable from a Western perspective, and essentially created a pool of followers at all echelons below commissioned officers. As most leaders would attest, it is a more efficient and effective model to create leaders at multiple levels, thereby distributing supervisory and oversight roles in a multi-tiered way that supports accountability.

The PLA has recently turned the corner with respect to the education of its NCOs and now mandates certain educational requirements simply to become one. In 2005 for example, "It established a goal of raising all junior NCOs' education levels to high school equivalency, and all senior NCOs to the level of 3-year college (the Chinese equivalent of technical school) graduates by 2008. That year, the PLA added the requirement to possess a relevant certificate of professional qualification for all types and levels of NCO." (ibid) This basic threshold system has yielded dividends not only by creating a presumably brighter class of NCOs, but by creating a more aspirational culture in the PLA. Whereas before it was commonly understood that "anyone" could rise to NCO rank, with recent changes it is now apparent to officer and soldier alike that there are indeed baseline thresholds both professional and educational that one must meet in order to take on the additional responsibilities of an NCO. This is truly a landmark event in the professionalization of the PLA.

One drawback in the evolution of NCO PME is the seeming lack of standards common to all members of the NCO corps. Trained and educated in varying degrees, physical locations, standards, and doctrine, the PLA's NCOs are truly all over the map. Although the baseline educational requirement to become an NCO persists, the method and means of education is left up to the individual, thereby producing a wide spectrum of learning among NCOs. This is true with respect to both civilian and military education. Shockingly, this is due to the ostensible lack of standards common to all entrants to the NCO corps, as "'no single Chinese source [outlines] the totality of the training system for conscripts and NCOs." (ibid, p. 106) Despite the challenge inherent in a lack of doctrinal standards for NCO education, the simple fact that the PLA has acknowledged the need for a more professional NCO class is itself a significant and positive step in the modernization of the PLA at the tactical level.

Similarly, junior officer education in the PLA has undergone a significant shift of late, with the Two Transformations readily apparent in this effort. With respect to the first Transformation, the focus on quality rather than quantity has led to a number of reforms over the last few decades, with the PLA desiring to create a smaller number of more well-rounded officers rather than a vast cadre of specialized officers. For example, the previous method of education at the company grade level would have called for technical officers to go off into the void of educational specialization, never to return to the parallel billets of their peers on the command track. In the mid 1980's, however, these tracks were merged in an effort to create more generalized officers capable of succeeding in a broader range of assignments.

Another effort aimed at professionalizing education at the junior officer level is the leveraging of Chinese civilian institutions to train future leaders. Despite the best efforts of the PLA, the curriculum at its junior officer military academies is still seen as somewhat less rigorous when compared with the higher education environment at large. As such, many new PLA officers are being trained at both, receiving a traditional civilian university education followed by a tenure at the military academies wherein basic tactics and troop leading are taught. (ibid, p. 107) This approach is particularly attractive in molding a well-rounded officer corps able to coalesce information from a variety of sources. Additionally, the esteem with which PLA officers are increasingly seen (as the professionalization of the military improves) in turn yields dividends in recruiting desirable candidates for service. Interestingly, this bifurcated educational model is itself a good means of implementing a "quality over quantity" officer corps, as many modern PLA lieutenants and captains are required to succeed in mastering both civilian and military educational curriculums before ever taking charge of their first platoon.

The twin effort Zemen called for in the "Two Transformations", the ability to counter an increasingly modern and technical array of threats, has manifested itself in a number of areas, not least of which is the Cyber domain. By most accounts, China has a fairly robust Cyber capability able to conduct both offensive and defensive operations. Although little is known about the specific structure of the Cyber apparatus inside the PLA, it is clear that new PLA officers are being selected and trained in this domain in an effort to prepare for the seemingly inevitable clashes among state and non-state actors in the 21st Century. The predominant organization new Chinese Cyber warriors are flowing to is known as the 3/PLA, the Signals Intelligence Agency of the People's Liberation Army. Interestingly, this was a conventional Signal unit until recently, when it expanded its focus beyond Chinese borders. "Until the advent of the Internet, 3/PLA operated as a conventional military signals intelligence agency with various collection platforms within China, but with no apparent collection capabilities overseas to match those of the United States and the United Kingdom." (Inkster, 2013, p. 49) It seems likely that the PLA will continue to hone the external Cyber capability of 3/PLA, as it is a relatively low-cost alternative to conventional kinetic warfare. As such, it will require a significant throughput of officers trained in Cyber skills not traditionally taught in the military academies. It remains to be seen what alterations to the Chinese PME system will be required to support this expanding mission set.

At the command college level, Chinese officers are given intermediate level instruction at the operational level of war. This instruction is broadly based given the myriad of domains in which so-called "new-type officers" may be called upon to operate. "Educating 'new-type military talent' is necessary for the PLA mainly because effective preparation for warfare in the information age requires synthetical integration of diverse knowledge, technologies, command and control, weapons platforms, logistics, and operational units." (Kamphausen, 2008, p. 296) This curriculum has expanded and intensified in recent years. As recently as 1997, the command college intermediate level curriculum was based around a single platform, specifically the utilization in combat of mechanized vehicles such as tanks. This myopia precluded much of the art and theory of military instruction from ever intruding into the classroom. The inevitable byproduct of this type of instruction was a detrimental focus on the tactical level of war; fine if educating lieutenants and NCOs, but frighteningly insufficient when preparing the field grade officer corps of the nation to "think bigger."

Among the new topics taught at the command college level are those formerly the domain of flag officers alone, such as joint operations, high technology operations, and command and control theory. (ibid, p. 297) Interestingly, the modern Chinese system of educating its promising crop of midlevel officers incorporates a heavy focus on the lessons learned by the US Army in locations like Iraq and Afghanistan. (ibid, p. 300) The utilization of case-based study has enabled Chinese officers to take on the roles of their American counterparts in an effort to better understand the complexities of modern conflict, particularly the challenges of asymmetric warfare on a large and unwieldy Army. These lessons are arguably far more relevant for the future course of Chinese operations than are the erstwhile lectures on tank operations that now seem like a Cold War relic. The seriousness with which students' academic progress is handled has undergone a similarly impressive transformation. One example is the handling of theses submitted by command college students. Whereas before a student's thesis was graded by the same professor the student had for the duration of the course, potentially leading to positive bias, the current system calls for a pair of anonymous reviewers to grade the thesis, with both having to sign off on its acceptability for satisfaction of degree requirements. (ibid, p. 302)

Additionally, the faculty themselves have undergone an impressive positive transformation. Whereas before the educators of the command college were culled from the "available", the current crop of teachers boast backgrounds from the highest levels of the military, diplomatic corps, Communist Party of China, and the sciences. Furthermore, they are expected to continue their learning via study abroad programs, partnerships with Chinese universities, and regular participation in exercises alongside their past and future students. Finally, instructors are “embedded” in active units in an observational role in order to glean insight into their daily operations. (ibid) The cumulative effect is a far more effective and knowledgeable bench of educators with whom students can exchange ideas, engage in wargaming, and share past experiences; truly a living manifestation of the principles of the “Two Transformations”.

At the National Defense University level, the curriculum is increasingly focused on joint operations, those consisting of two or more elements of land, sea, and air power. Whereas before the two latter elements were seen as of lesser importance compared to ground forces, modern Chinese doctrine calls for the combined might of all three. To that end, the NDU seeks to educate officers headed to senior level commands on the finer points of employing the troops and technology of all services to achieve strategic objectives, though they themselves are not taught to be true “strategists”. (ibid, p. 318) The mission sets for which these senior officers are prepared are evolving in recent years: “China’s armed forces, however, prepare for missions in addition to major combat operations, and these are becoming ever more salient as years pass. Among them are anti-terrorism, rescue and relief operations, post disaster reconstruction, and possibly noncombatant evacuation operations (NEO), all of which require the attention of senior officers.” (ibid, p. 319) Undoubtedly, it is increasingly important for the PLA to invest “early” via the education and cultivation of agile thinkers capable of steering these diverse mission sets with ease.

The relief operations mission is an increasingly attractive one for the PLA and its leaders. By conducting high profile relief missions, the PLA is seen in a favorable light, with positive humanitarian notices in global media, and the opportunity to showcase its expeditionary capacity and materiel systems. In April, the PLA was able to do both when an earthquake struck the city of Ya’an. Within hours, the PLA was fully engaged in the relief effort. As the Washington Times noted, “what was presumed to be an earthquake relief operation led by civilians quickly became an all-out campaign by the People’s Liberation Army to show off its mobilization capability and high-tech weapons with an over-the-top propaganda theme — “The PLA Loves The People.” (Yu, 2013, p. A1) Never one to shy away from positive publicity, PLA leaders of the various branches were soon jockeying for position in front of cameras and reporters, all eager to give a positive face to their particular piece of the operation. (ibid) Despite the somewhat over the top nature of this particular incident, the underlying theme is an important one: the PLA of 2013 possesses the type of leadership, equipment, and acumen to conduct complex operations with quickness and relative ease. This newfound capacity begins with the education of the officers of the PLA.

The “finishing school” of the PLA that prepares its newly minted generals and admirals for their newfound responsibilities is the Capstone course. Modeled on the US program of the same name, Capstone is intended to serve as a master class in executive level decision making in times of crisis. (Kamphausen, 2008, p. 322) In the Chinese version of the course, implemented in 1986, the method of instruction was a combination of lecture, writing, role playing, intercultural study, and site visits. This hybrid method of instruction was likely considered unorthodox to a group of Chinese officers more accustomed to rote memorization and regurgitation than holistic study and reflection. Undoubtedly, however, this course was yet another manifestation of the upside of the “Two Transformations” concept, creating a new generation of more seasoned and well-rounded flag officers capable of orienting themselves quickly to unfamiliar scenarios. A scan of the future assignments of Capstone graduates reveals that this training is seen as especially valuable for PLA leaders charged with important and complex jobs, from the Director of the General Logistics Department to the Deputy Commanding General of the People’s Liberation Army Air Force. (ibid, p. 339)

Implications for the Future

The professionalization of leader education in the PLA has no doubt yielded dividends in the overall readiness, sophistication, agility, and capacity of the organization. At all levels of the organization, officers are charged with increasingly diverse and complex tasks. The technological capacity of the PLA, despite lagging behind the US significantly, is on the rise. As such, Chinese reliance on sophisticated weapons systems is likely to increase as well. The leaders charged with employing these weapons must be well versed in both the operational and tactical arts and the technological aspects of these systems. There is no longer any separation between the two: “The effective use of advanced weapons depends on a range of ‘soft’ components that are no less important than hardware in preparing an army to fight. These include training, officer and noncommissioned officer education, organization, logistics, information technology application, and political indoctrination. To the improvement of each the Chinese have devoted a great deal of attention and effort in the last few years.” (ibid, p. 383-384)

Despite the marked increase in attention to technology, the core mission sets of the PLA remain the same: defense at home (and by extension ensuring the Party's preeminence), enabling outward economic expansion, and reacting to worldwide contingencies. Interestingly, the first mission, particularly as it relates to ensuring the Party remains in power, may have a detrimental effect on the final two. As stated in the Washington Quarterly, "The PLA's top mission and highest priority for China's communist leaders -listed first in the New Historic Missions- is to serve as the ultimate backup for other security forces to protect the ruling regime against domestic challenges. This responsibility constitutes a 'domestic drag' in that it inhibits the PLA's ability to concentrate on external missions." (Scobell, 2012, p. 137) In essence, the perpetual Party paranoia restricts the ability of the PLA and its new breed of leaders to respond to the true array of global threats facing China. This constraint is unlikely to be viewed favorably by a class of military officers equipped with a greater deal of independent thinking and sophistication than their forebears of the Mao generation. It remains to be seen how this potential divergence of priorities between the CPC and the PLA will play out.

In a similar vein, the looming Taiwan situation is never far from the thoughts of the Chinese military class. Long a stated objective of the PRC, the return of Taiwan to Chinese sovereignty is unlikely to shift to the backburner in the near future. The effects of a more educated and skilled Chinese force are of course not clearly quantifiable or qualifiable in any potential martial scenario, but it is likely that the Chinese Army of 2013 would be far more capable than the Chinese Army of 1969 to overtake Taiwan, all other things being equal. With a core nucleus of NCOs with at least a high school diploma and significant leadership and skill training, a junior officer corps with finely tuned civilian and military skill sets, a midlevel group of officers with a sophisticated understanding of the operational requirements of a large scale amphibious landing, and a senior group of colonels and generals ready to lead a complex joint operation, the PLA is a formidable force indeed.

The joint, combined-arms expertise of the Chinese officer corps is particularly well suited to the Taiwan contingency. The scenario China is likely to face is multi-faceted given the always-complex nature of maritime operations and the host of "area-denial" defenses sure to await any advancing force: "facing these obstacles, if it must attack Taiwan, the PLA has prepared itself to use a mixture of elements from three generic campaign options: a blockade of the island, missile attacks, and an amphibious landing." (ibid, p. 141) The whole host of PLA capability would be put to the test in a Taiwan scenario, albeit with joint commanders running the show. Given their newfound capacity for joint operations, PLA officers at midlevel and senior ranks would no doubt prove quite effective in this operational scenario. Clearly the curriculum developed for China's 21st Century officers' professional military development is rooted not only in a desire to "professionalize", but to prepare for perceived real world needs. As such, the officers of the PLA seem better suited now than at any point since Taiwan's move to independence to engage in the long-simmering conflict.

Perhaps the most telling aspect of any military's orientation is its doctrine, the set of rules, parameters, techniques, and procedures by which it aims to operate. By reviewing both the warfighting (Kamphausen, 2008, p. 376) components of PLA doctrine, one is able to glean significant insight into the way the PLA would seek to counter threats. The first broad area encapsulated in Chinese doctrine is the method by which it would repel a large scale ground invasion. The fact that the PLA spends time and energy preparing its force for such a seemingly unlikely scenario is indicative of the lingering paranoia with which the Chinese view their neighbors. It is also frighteningly optimistic in nature, as if designed more as a form of propaganda than as a legitimate military playbook. "Although this [invasion] scenario is apocalyptic and completely unrealistic, it gives the Chinese confidence that they cannot be subdued or conquered." (ibid, p. 378) When contrasted with the very real strides made in the military education domain, it is disheartening to see such a fundamental disconnect with reality in another area fundamental to a professional military: its doctrine

The PLA set out on a journey toward a professional military ethic more than 25 years ago. In that time it has not had to fight in a major conventional war. It has also avoided the type of small localized conflicts that have by default defined the modern American military. As such, it has had a great deal of time for reflection. It is clear that the PLA of today is far more poised to engage in a broad spectrum of potential conflicts than any time in its history. It is also clear that a premium has been placed on learning like never before. Although the PLA may have a few more strides to make before being able to call itself a truly "modern and professional army", it has already taken the most important step possible: investing in the minds of those charged with leading it.

Bibliography

Blasko, D. J. (2005). Chinese Army Modernization: An Overview. Military Review, 85(5), 68.

Dreyer, J. (1996). The New Officer Corps: Implications for the Future. The China Quarterly, (146), 315. doi:10.2307/655471

George P. Jan (1999) The Military and Democratization in China in the Post Cold War Era, International Journal of Public Administration, 22:8, 1241-1268

Inkster, N. (n.d). Chinese Intelligence in the Cyber Age. Survival, 55(1), 45-66.

Kamphausen, R., Scobell, A., & Tanner, T. (2008). The "people" in the PLA [electronic resource] : recruitment, training, and education in China's military / Roy Kamphausen, Andrew Scobell and Travis Tanner editors. [Carlisle, PA] : Strategic Studies Institute, [2008].

Sahgal, B. (2011). Emerging Trends in the PLA Army. Maritime Affairs: Journal Of The National Maritime Foundation Of India, 7(2), 14-32. doi:10.1080/09733159.2011.641383

Scobell, A., & Nathan, A. J. (2012). China's Overstretched Military. Washington Quarterly, 35(4), 135-148. doi:10.1080/0163660X.2012.726438

Snakenberg, M. K. (2011). Implications for the Future. JFQ: Joint Force Quarterly, (62), 104-109.

Yu, Miles. "Inside China." The Washington Times 26 Apr. 2013: 1. Print.

Table of Contents

CNO Says Navy Needs Ground Forces’ Help On Cyber, Electronic Warfare

By Sydney J. Freedberg Jr., Breaking Defense, October 29, 2013

WASHINGTON: Rivalries between the services are a favorite topic in this town, especially when budgets tighten. But when it comes to cyberwarfare, electronic warfare, and the wireless world where they intersect, the Navy’s top man in uniform is more than happy to get help from the Army.

Admittedly, Adm. Jonathan Greenert is mostly focused on working with the Air Force on cyber/EW under the Air-Sea Battle concept and on reforming the Navy itself. He’s challenging the culture of “straight stick” naval aviators to admit that electronic warfare aircraft like the EA-18G Growler and E-2D Hawkeye are often more important than the strike fighters they support: The strike planes have to make through enemy air defenses to their targets, he noted, and — in a reflection of the Navy’s doubts about “low observable” technology — “all the stealth in the world ain’t gonna penetrate everything,” he told the audience at the 50th annual conference of the Association of Old Crows, a group named after a slang term for electronic warfare operators. Often, he added, a cyber attack or jamming can take down an enemy command network or stop an incoming missile far more effectively than any physical attack.

Greenert’s also jamming cyber and EW content into every training program from the Naval Academy to the Naval Postgraduate School. “Establishing a better awareness is number one,” he said. The CNO also pushed for Cyber Command, currently a part of Strategic Command and co-located with the National Security Agency at Fort Meade, be elevated to an independent “unified combatant command with global reach.” But when I asked Greenert about the Army and Marine Corps’ role on his way out, he made clear the ground forces can bring some things the Navy lacks.

“They have apertures that we haven’t yet developed yet,” Greenert stopped to tell me as his aides desperately tried to chivvy him along to his next appointment. “A ground node is very powerful.” Some radar, sensor, and electronic warfare systems are physically too big and power-hungry to fit on a ship, for example, and it’s hard to imagine taking a cluster of supercomputers like the one at Fort Meade and getting it to float. On the other hand, those megafacilities are, by definition, static. “A ship can move, but it doesn’t have the aperture and the bandwidth” of those big ground-based systems, Greenert said.

On the flipside, what the Navy brings that the Army doesn’t is strategic mobility. “If you’re an afloat unit, you can relocate anywhere around the world,” he told me. “It’s the site, the node that we’re moving around.”

True, the Army and Marines have plenty of smaller electronic warfare systems that can fit in a truck, and the Army in particular is fielding high-bandwidth networks. But those give up the raw power of permanent ground installations without gaining the mobility of shipboard systems. Ground forces may be tactically mobile, but strategically they’re merely deployable, requiring ships and planes to put them into position. A ship, by contrast, is the largest possible platform that can still move.

(The ability to move much larger things through the water than would be possible over land is a matter of physics that applies across the board: The largest marine mammals, blue whales, are much bigger than the largest land mammals, elephants.)

Greenert is hopeful that new technologies can bring the cyber/EW power of ships closer to that of permanent ground installations. (He didn’t mention specifics, but one is probably replacing today’s turbine engines with an all-electric drive). “When we get a shop that gets that tremendous amount of power [--] that’s in the future — and we miniaturize more, we’ll be that much more agile,” Greenert told me.

For a long time to come, however, ground units and installations will play a crucial role in supporting naval forces in an area of warfare that the CNO identifies as their highest priority.

Table of Contents

The Nairobi Attack and Al-Shabab’s Media Strategy

By Christopher Anzalone, CTC Sentinel, October 2013, pages 1-6

After carrying out a bold attack inside the upscale Westgate Mall in Nairobi in September 2013, the Somali militant group al-Shabab succeeded in recapturing the media spotlight. This was in large part due to the nature of the attack, its duration, the difficulty in resecuring the mall, the number of casualties, and al-Shabab’s aggressive media campaign during and immediately after the attack.[1]

From al-Shabab’s perspective, the attack on Westgate Mall was a media triumph, particularly coming in the midst of a growing rift among jihadists both inside and outside Somalia regarding the consolidation of power by the group’s amir, Ahmed “Mukhtar Abu al-Zubayr” Godane. The attack also followed a year in which al-Shabab lost control of significant amounts of territory in Somalia, most importantly major urban and economic centers such as the cities of Baidoa and Kismayo.

This article examines al-Shabab’s media strategy during and immediately after the Westgate Mall attack, both via micro-blogging on Twitter through its various accounts as well as more traditional media formats such as audio statements from the group’s leadership. The article also puts the group’s media operations for the Westgate attack in historical context by comparing and contrasting them to al-Shabab’s past media campaigns. Finally, the article concludes with an assessment of al-Shabab’s current state of health and the potential for more spectacular acts of violence, in large part as political and media spectacles designed to capture public attention.[2] It finds that al-Shabab, despite facing increased political and military setbacks, remains adept at executing audacious attacks designed to attract the maximum amount of media attention. Its media operatives are still able to skillfully exploit its enemies’ mistakes on the battlefield and in the information operations war, as well as manipulating the news cycle by inserting sensationalist claims.[3] It also finds that al-Shabab has maintained a great deal of continuity with its messaging toward foreign state actors active in Somalia, despite the insurgents’ shifting fortunes on the ground.[4]

The Westgate Attack

Al-Shabab’s complex assault on the Westgate Mall began just after noon on Saturday, September 21, 2013, when an undetermined number of gunmen entered the facility and began throwing grenades and shooting indiscriminately.[5] Eyewitness accounts from the early stages of the attack suggested that the first response from Kenyan security forces was, at best, disorganized, which likely was one of the reasons that the militants were able to prolong the attack over several days.[6] After the initial failed attempts to stop them, the attackers proceeded to pick out targets from among those trapped inside the mall, in some places separating Muslims from non-Muslims.[7] Kenyan authorities remained unsure as to developments inside the mall nearly an hour into the attack, and the first army units arrived in the late afternoon, although confusion continued due to the lack of clear command-and-control between the Kenyan military and police.[8] The Kenyan military and police—reportedly aided by foreign advisers from the United States, United Kingdom, and Israel—helped hundreds of trapped shoppers escape the mall throughout the siege.[9]

The standoff between the al-Shabab fighters and Kenyan security forces continued through the weekend. At 1:28 p.m. Kenyan time on September 22, however, the Kenyan military’s official Twitter account said that most of those trapped inside had been rescued and “most parts” of the mall complex were under control.[10] The claim that the attack was nearly over was disproved in the early morning of September 23 when an explosion rocked the Westlands district of Nairobi where the Westgate Mall is located. More large explosions followed in the early afternoon. Confusion reportedly continued with regards to the exact chain-of-command among the Kenyan military and police, with differences emerging between commanders and the office of Kenyan President Uhuru Kenyatta.[11] Fighting continued into the evening of Tuesday, September 24, and President Kenyatta only declared a formal end to the siege late in the evening on the same day.[12] The following day, shopkeepers and restaurateurs were able to return to their businesses inside the mall, where some discovered evidence of theft and looting by some Kenyan soldiers.[13] The number of casualties currently stands at 72, including five of the attackers and six Kenyan soldiers.[14] As of October 15, the Red Cross reported that 23 people were still missing after the attack, although the Kenyan government claims all those missing have been accounted for.[15]

Kenyan authorities initially believed that there were 10 to 15 attackers, but have since revised their estimate to as low as four to six.[16] They have named four individuals they believe participated in the attack: Abu Bara’ al-Sudani (“the Sudanese”), Omar al-Nabhan, Khattab al-Kini (“the Kenyan”), and an individual named Umayr.[17] All four were reportedly members of al-Hijra, al-Shabab’s chief Kenyan ally, which was formerly known as the Muslim Youth Center.[18] If the attack was indeed carried out largely by fighters from al-Hijra, it would be yet another sign of the increasing importance to al-Shabab of its Kenyan allies and support networks, which have steadily increased since 2010.[19]

Al-Shabab’s Media Operations During the Siege

The start of al-Shabab’s use of Twitter as a propaganda tool began on December 7, 2011, following the entrance of the Kenyan military into southern Somalia in October 2011.[20] Since then, it has attracted significant attention from journalists.[21] Since its debut on Twitter, al-Shabab has made great use of the micro-blogging format to deliver its counternarrative to events occurring inside Somalia, running commentary on a host of political, social, and religious issues, and taunting its enemies, such as the African Union Mission in Somalia (AMISOM) force inside Somalia, the Somali federal government, and the United States.[22]

The insurgent group’s media department provided a continuous stream of “updates” and commentary throughout the assault on Westgate Mall.[23] This reveals that the group recognizes the value of tweeting, particularly in English, in attracting the attention of the world’s news media. Prior to launching their assault, the attackers may have set up a “command-and-control center” in an unidentified vehicle positioned earlier in the day on September 21.[24] Intelligence intercepts suggested that some of the Twitter updates posted by al-Shabab’s HSM Press (Harakat al-Shabab al-Mujahidin) account were sent from there.[25]

The tweets posted to the account during the assault attempted to deliver al-Shabab’s message in a number of different areas. First, there was the promotion of the insurgents’ counternarrative, which painted the attack on Westgate Mall as a response to the greater suffering endured by those inside Somalia. Some example tweets included: “The attack at #WestgateMall is just a very tiny fraction of what Muslims in Somalia experience at the hands of Kenyan invaders. #Wetsgate [sic]”; “What Kenyans are witnessing at #Westgate is retributive justice for crimes committed by their military, albeit largely miniscule in nature”; and “The attacks are just retribution for the lives of innocent Muslims shelled by Kenyan jets in Lower Jubba [in Somalia] and in refugee camps #Westgate.”[26]

Second, al-Shabab directed renewed warnings to the Kenyan government and public, linking the latter’s security to the removal of the thousands of Kenyan military personnel from Somalia. Some example tweets included: “HSM has on numerous occasions warned the #Kenyan government that failure to remove its forces from Somalia would have severe consequences”; and “The Kenyan government, however, turned a deaf ear to our repeated warnings and continued to massacre innocent Muslims in Somalia #Westgate.”[27] They also made a direct demand for the removal of Kenyan forces from Somalia: “The message we are sending to the Kenyan govt & Public is and has always been just one: remove all your forces from our country #Westgate.”[28]

Third, and most importantly for the use of its Twitter messaging as a propaganda tool designed to attract media attention, the HSM Press account purportedly posted “updates” on the ongoing siege at a time when conflicting reports abounded. These included tweets announcing the attack on the “Kenyan Kuffar [unbelievers] inside their own turf,” denying the cessation of fighting between “the mujahidin” and the Kenyan military and police, alleging that the Kenyan government was “pleading” with the attackers inside the mall to negotiate, and reports of the calmness of the attackers despite being under siege by Kenyan security forces.[29] Al-Shabab also claimed via Twitter that it had “singled out” only “unbelievers” in the attack and had “escorted out” Muslims before the attack began, announcing that the defense of Muslim lands “is one of the foremost obligations after faith & defending against the aggressive enemy is our right as Muslims.”[30]

Al-Shabab’s discourse via more traditional channels—such as press statements broadcast on the radio and distributed online via pro-Shabab news websites—delivered similar messages. In an audio statement on September 21, al-Shabab’s senior spokesman, Ali Mohamed Rage (also known as Ali Dheere), said that the Westgate Mall attack was in response to the attack by “Christian Kenya” on Somalia via the southern region of Jubba.[31] The Kenyans, he alleged, committed massacres of Somali civilians, including women and children, with fighter aircraft and heavy weapons.[32] The Kenyan government, Rage said, continues to ignore the insurgents’ warnings to withdraw from its “illegal” occupation of parts of Somalia or face the consequences at home.[33] Rage painted the attack as an “eye for an eye,” citing the second half of a Qur’anic verse, which reads, “And the one who attacks you, attack him in a manner similar to that which he attacked you.”[34] Rage said that the attack was carried out by a specially trained squad of fighters who were “defending” their religion and avenging the innocents killed by the Kenyan military.[35]

Insurgent Media as an Alternative News Source

Since it emerged in 2007-2008 as the premier insurgent movement fighting the then-Transitional Federal Government (TFG) in Somalia, al-Shabab has expressed an interest in “correcting false news” about itself.[36] The latest stage in the evolution of the group’s media operations was the rebranding of a part of its media department as the “al-Kataib News Channel,” a source of news about “the mujahidin” that was unbiased and brought “the truth directly from the battlefield.”[37] Through this rebranding effort, al-Shabab promoted its propaganda videos as “documentaries” and a form of “insurgent journalism” that revealed the “truth” in the midst of the falsehoods supposedly being spread by the Western media about the group.[38]

Advancing its counternarrative is a key part of al-Shabab's media strategy, as is evident by the group's handling of the Westgate Mall story. By claiming to be in close contact with the militants inside the mall, its media operatives garnered a great deal of attention from news media outlets around the world. It is suspected that al-Shabab succeeded multiple times in circumventing attempts to prevent them from micro-blogging by creating a new account each time a Twitter suspension went into effect.[39] Al-Shabab also tailored its different Twitter feeds to their different audiences, focusing on more domestic issues via its Somali language Twitter account.[40] The confused handling of the crisis by the Kenyan government benefited al-Shabab's efforts to manipulate the reporting of the attack, on which it was quick to capitalize. Al-Shabab has undermined its enemies' claims previously as well, releasing photographs showing dead AMISOM soldiers, including close-ups of their identification cards and captured weapons and equipment, following AMISOM denials of suffering casualties in attacks in Somalia.[41]

After Westgate: Continuity in Media Operations

On the last day of the attack, al-Shabab's HSM Press Twitter account was still busy disseminating the group's messages and attempting to influence the news cycle. In the early hours of September 24, the group continued to deny reports that the siege had ended, callously noting that "countless dead bodies" were scattered throughout the mall as the attackers continued to hold out.[42] A still image from closed circuit television from inside the mall showing two of the attackers was also released.[43] In a tweet clearly demonstrating that the group's media operatives were well aware of events impacting Muslims outside of Somalia, HSM Press quoted and heralded "mujahid" Michael Adebolajo, one of two young British men charged with murdering off-duty soldier Private Lee Rigby on May 22, 2013, in London. Shortly after Rigby's murder, Adebolajo said that it was an "eye for an eye" response to British aggression against Muslims.[44] In the tweet, al-Shabab said, "His [attack] was #Woolwich [in London], #Westgate ours!"[45]

The insurgents, via Twitter, also alleged that the Kenyan government had used "chemical agents" in Westgate Mall in a desperate attempt to end the siege.[46] To cover "their crime," the HSM Press feed continued, the Kenyan government destroyed the building, burying scores beneath the rubble.[47] Al-Shabab also commented on Western media speculation that the so-called "White Widow" (British militant Samantha Lewthwaite) was involved in the attack.[48] The group denied that "any woman" was involved, stating, "We have an adequate number of young men who are fully committed & we do not employ our sisters in such military operations."[49] The insurgents, perhaps aware of potentially damaging public relations, also denied targeting women and children in the attack, saying that they provided them "safe passage," a claim belied by the evidence.[50]

Al-Shabab repeated its earlier demands to the Kenyan public to pressure their government to withdraw its military forces from Somalia. In exchange, al-Shabab would allow Kenyans to live in peace: "Kenyans, look how fear has gripped your nation…You can put on a brave face but you're shaken. Your spirit is on the wane &your leaders lack the moral fibre to do the right thing…You could have avoided all this and lived your lives with relative safety. Remove your forces from our country and peace will come."[51]

There is a precedent for al-Shabab's use of this type of media strategy. The group employed a similar strategy with Uganda and Burundi in 2010 before and after al-Shabab carried out two "martyrdom operations" in Kampala in June of that year.[52] Before carrying out those attacks, al-Shabab's al-Kataib Media Foundation released a video in which the unidentified narrator, who spoke impeccable English with a British accent and whose face was not shown, warned the Ugandan and, to a lesser extent, the Burundian people to pressure their governments to withdraw their forces from Somalia, where both militaries formed the backbone of the AMISOM force propping up the weak Somali TFG.[53]

Following the Kampala attacks, the insurgents released a follow-up video prominently featuring scenes from those attacks. What sounded like the same English-speaking narrator warned the Ugandan public that if the "lessons being taught" against their military forces inside Mogadishu were not clear enough, then perhaps only "lessons a little closer to home" would be the "only solution…You [the Ugandan public] will then pay a hefty price."[54] An audio message from al-Shabab leader Godane in the same video portrayed the Kampala attacks as revenge for innocent Somali women, children, and elderly killed by AMISOM in Somalia.[55] In October 2011, Rage warned the Kenyan public to "consider carefully" the path their government was taking them down by intervening militarily in Somalia, a point he has since reiterated in audio statements regarding the Westgate Mall attack.[56]

Aware of the media frenzy surrounding the Westgate Mall attack, the HSM Press feed began advertising in advance a forthcoming audio statement from Godane on the afternoon of September 24.[57] Godane's statement was released the next day and distributed on pro-Shabab Somali news websites, jihadist forums, and on Twitter, first with a Somali language tweet and, soon after, two English language tweets with links to official English written and audio translations of the statement.[58] The audio translation was read by what sounded like the same individual, speaking with a British accent, who debuted in al-Shabab's English language video productions during the summer of 2010. The release of written and audio English translations of Godane's statement within hours of the release of the original demonstrated the group's media savvy in capitalizing on and even feeding the worldwide media attention surrounding the attack.[59]

Dubbing the attack the "Badr Nairobi" in reference to the Prophet Muhammad's first major battle in 624 AD, Godane eulogized the "martyrdom-seekers" who carried out the attack and stated that the operation was in response to Kenya's military intervention inside Somalia.[60] The "success" of the attack, he said, once again showed the "power of faith, which "nothing can stand against," revealing weaknesses in the Kenyan government, military, and police.[61] As he did to the Ugandan public following the Kampala bombings in 2010, Godane addressed the Kenyan public by telling them to leave Somalia. "You have entered into a war that is not yours and is against your national interests…you have voluntarily given up your security and economy and have lost many of your sons," he said, arguing that because they elected their politicians, they bear the responsibility of "the massacres that are being perpetrated by your military in Kismayo and the neighboring regions."[62]

Conclusion

The Westgate Mall attack has returned the beleaguered al-Shabab militant group into worldwide headlines. Wracked by internal divisions—most notably the public spat between al-Shabab's senior leadership under Godane and dissidents such as Omar Hammami as well as former senior leaders within the group itself—al-Shabab was in need of relief. The attack on Westgate Mall provided the group with a media triumph that catapulted it back onto the public stage.

The long-term military significance of the attack is unknown at this time. While it is unlikely that it will result in significant military gains for al-Shabab on the ground in Somalia, it may lead to strategic gains for the group in the short-term, particularly if there is a heavy-handed response from the Kenyan government that targets the hundreds of thousands of Somalis living in Kenya.[63] The increased media attention may also prove to be a mixed blessing for al-Shabab. On the one hand, it renews its relevance in the eyes of potential supporters at home and abroad. On the other hand, it will intensify the drive by powerful international actors such as the African Union, the United States, and the United Kingdom to target al-Shabab's leadership in the hopes of eliminating it as an international threat.

The attack may not lead to a Kenyan military withdrawal from Somalia, but it could be a harbinger of a continuing shift by al-Shabab back to asymmetric warfare. The group might carry out more attacks on soft targets, such as civilian centers and non-military sites, to bleed the fledgling Somali federal government and its African Union backers. Indeed, the insurgents began shifting back to their guerrilla roots in August 2011 when they withdrew from Mogadishu in the face of a mounting offensive by AMISOM, the TFG, and allied Somali militias. This followed al-Shabab's failure to drive out AMISOM and the TFG from Mogadishu.

As al-Shabab's battlefield capabilities continue to deteriorate, the strategic benefits of low-cost acts of terrorism and asymmetric warfare increase, and the group is likely to turn to such actions in a bid to remain a relevant force both inside and outside Somalia.

Christopher Anzalone is a Ph.D. student in the Institute of Islamic Studies at McGill University where he studies modern Muslim sociopolitical movements, contemporary jihadist movements, Shi`a Islam, and Islamist visual cultures. He is also an adjunct research fellow at the Ali Vural Ak Center for Global Islamic Studies at George Mason University.

Notes

[1] Roopa Gogineni, "Nairobi Mall Death Toll Expected to Rise," Voice of America, September 25, 2013.

[2] For more on the "spectacle" aspect of terrorism/anti-civilian violence, see Gerard Chaliand, Terrorism: From Popular Struggle to Media Spectacle (London: Saqi Books, 2001); Steven Livingston, The Terrorism Spectacle (Boulder, CO: Westview Press, 1994). The media spectacle of violence is discussed in Douglas Kellner, "Media Propaganda and Spectacle in the War on Iraq: A Critique of U.S. Broadcasting Networks," Cultural Studies: Critical Methodologies 4:3 (2004): pp. 329-338; Cynthia Carter, Violence and the Media (New York: Open University Press, 2003); Matthew Robert Kerbel, If It Bleeds, It Leads: An Anatomy of Television News (Boulder, CO: Westview Press, 2001). For a theoretical discussion of the "political spectacle," see Murray Edelman, Constructing the Political Spectacle (Chicago: University of Chicago Press, 1988); Arie S. Soesilo and Philo S. Wasburn, "Constructing a Political Spectacle: American and Indonesian Media Accounts of the 'Crisis in the Gulf,'" Sociological Quarterly 35:2 (1994): pp. 367-381.

[3] These include making allegations that Kenyan forces used chemical weapons during the siege and later blew up sections of the mall, burying scores of people, to hide their act.

[4] Looking at al-Shabab's media operations from a historical perspective allows for a more detailed and contextualized analysis of continuities, shifts, and trends in its messaging, which is not possible if the group's statements are examined in a vacuum.

[5] The Kenyan government has said that there were between 10 and 15 attackers, but the exact number remains unclear. See "Nairobi Attack: Kenya Forces Comb Westgate Site," BBC, September 24, 2013.

[6] Daniel Howden, "Terror in Nairobi: The Full Story Behind al-Shabaab's Mall Attack," Guardian, October 4, 2013.

[7] Ibid.

[8] Ibid.

[9] Peter Walker, "Kenyan Forces Begin 'Major Assault' to End Nairobi Mall Siege – as it Happened," Guardian, September 23, 2013; Richard Norton-Taylor and Vikram Dodd, "Nairobi Attack: Israel Takes Lead Role in Advising Kenyan Forces," Guardian, September 23, 2013; Geoffrey Mosoku, "Kenya Denies Involvement of Foreign Military," The Standard [Nairobi], September 23, 2013.

[10] Kenya Defense Forces, tweet, September 22, 2013, available at www.twitter.com/kdfinfo/statuses/381877655227731968.

[11] Howden.

[12] Ibid. Stefan Smith and Peter Martell, "Kenyan President Announces End to Mall Bloodbath," Agence France-Presse, September 25, 2013.

[13] Howden; Geoffrey York, "Kenyan Military Seeks Soldiers Who Looted Stores During Mall Attack," Globe and Mail, October 3, 2013; Margaret Wahito, "Lenku Admits Looting at Westgate, Probe Continues," Capital FM Radio [Nairobi], September 29, 2013; John Campbell, "Nairobi's Westgate Mall Attack: Unanswered Questions," Council on Foreign Relations, October 8, 2013.

[14] Gogineni; "Kenyan Mall Attack: 39 Still Missing, Says Red Cross," Associated Press, September 30, 2013.

[15] Ramadhan Rajab, "23 People Still Missing Almost a Month after Westgate Attack," The Star [Nairobi], October 15, 2013.

[16] "Kenya Military Names Westgate Mall Attack Suspects," BBC, October 5, 2013.

[17] Ibid. Omar al-Nabhan was the nephew of the late Saleh al-Nabhan, an al-Qa`ida operative in East Africa who served as a military trainer for al-Shabab and was killed in a U.S. military raid in September 2009. For background information on Saleh al-Nabhan, see "Profile: Saleh Ali Saleh Nabhan," BBC, September 15, 2009.

[18] "Abu Baara al-Sudani, Omar Nabhan, Khattab al-Kene, and Umayr Identified as Kenya Mall Attackers," news.com.au, October 6, 2013. The Muslim Youth Center's (MYC) reported name change appeared in the latest report from the UN Monitoring Group on Somalia and Eritrea, although the entire section on the MYC is redacted and listed as "strictly confidential." Twitter and Tumblr accounts believed to be linked to the MYC, and which release statements in its name, still use the old name, not al-Hijra.

[19] Christopher Anzalone, "Kenya's Muslim Youth Center and Al-Shabab's East African Recruitment," CTC Sentinel 5:10 (2012).

[20] Christopher Anzalone, "Harakat al-Shabab al-Mujahideen's Press Office Opens Twitter Account," al-Wasat blog, December 8, 2011. Al-Shabab's original English language Twitter account has since been closed, but the group's media department appeared to open new accounts as previous ones were suspended by Twitter for "violations of service." See, for example, Feisal Omar, "Al Shabaab's Twitter Account Down after Hostage Threat," Reuters, January 25, 2013.

[21] See, for example, Michelle Shepherd, "Tweeting War: Somalia's Al Shabab Joins Twitter," Toronto Star, December 8, 2011; Spencer Ackerman, "Somali Terrorists Join Twitter #Propaganda," Wired, December 7, 2011; David Smith, "Al-Shabaab in War of Words with Kenyan Army on Twitter," Guardian, December 13, 2011; Geoffrey York, "Al-Shabab Goes to War with Kenyan Army on Twitter," Globe and Mail, January 11, 2012.

[22] The al-Shabab media operatives who run the "HSM Press" account spend a great deal of time and energy, measurable to some degree in a comparative analysis of the numbers of tweets on the subject, pushing forward their counternarrative to that of the Somali government, African Union, the United States, and other international actors. See the analytical data in Alexander Meleagrou-Hitchens, Shiraz Maher, and James Sheehan, Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy (London: The International Centre for the Study of Radicalisation, 2012), pp. 31-35.

[23] Propaganda messaging in English, a language more readily accessible to many in the Western news media, has in the past led to the inflation of the importance of some jihadist publications, such as Inspire magazine, and, some argue, personalities, such as the late radical Yemeni-American preacher Anwar al-`Awlaqi. See J.M. Berger, "Inspiration Inflation," Foreign Policy, April 23, 2013; Erik Stier, "Is Anwar al-Awlaki's Importance to Al Qaeda Overstated?" Christian Science Monitor, May 10, 2011; Gregory D. Johnsen, "A False Target in Yemen," New York Times, November 19, 2010; Thomas Hegghammer, "The Case for Chasing al-Awlaki," Foreign Policy, November 24, 2010.

[24] Howden.

[25] Ibid.

[26] These tweets were posted by the now-defunct @HSM_Press Twitter account, September 21-24, 2013. The text of the tweets has been saved by the author.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ali Mohamed Rage, "Mujaahidiintu Duulaan Aargoosi ah Ayay Ku qaadeen Kenya," al-Shabab, September 21, 2013.

[32] Ibid.

[33] Ibid.

[34] See Qur'an 2:194.

[35] Rage, "Mujaahidiintu Duulaan Aargoosi ah Ayay Ku qaadeen Kenya."

[36] "An Important Clarification regarding the Promotion by Al-Jazeera of False News about the Movement [al-Shabab]," al-Shabab, November 24, 2008.

[37] "Al-Kata'ib News Channel," al-Shabab, July 27, 2010.

[38] The Burundian Bloodbath: Battle of Dayniile, al-Shabab, November 12, 2011; Under the Shade of Shari'ah, al-Shabab, July 1, 2012; Christopher Anzalone, "The Rapid Evolution of Al-Shabab's Media and Insurgent 'Journalism,'" Open Democracy, November 16, 2011.

[39] "Al-Shabab Showed Gruesome Social Media Savvy During Attack," CBS News, September 24, 2013.

[40] Ibid. Cedric Barnes, a Somalia expert working for the International Crisis Group, noted this difference between al-Shabab's English and Somali language media messaging regarding its assault on the Westgate Mall, but the story does not provide any specific examples of these differences.

[41] The Burundian Bloodbath: Battle of Dayniile; Mogadishu: Crusaders' Graveyard, al-Shabab, July 30, 2010; Christopher Anzalone, "Harakat al-Shabab al-Mujahideen Releases Statement & Information on Burundian AMISOM Soldiers Slain at Battle of Dayniile," al-Wasat blog, December 12, 2011.

[42] HSM Press tweet, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author.

[43] Ibid.

[44] Tom Whitehead, David Barrett, and Steven Swinford, "Woolwich Attack: Suspect Michael 'Mujahid' Adebolajo Led Away in Handcuffs at Fanatic's Trial," Telegraph, May 23, 2013.

[45] HSM Press tweet, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author. On October 17, al-Shabab's media department released a new propaganda film, Woolwich Attack: It's an Eye for an Eye, in Arabic and English versions, heralding Adebolajo and other "lone wolf mujahidin" who, when unable to become foreign fighters in places such as Somalia, have "fulfilled their duty of jihad" in their home countries.

[46] HSM Press tweets, September 25, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author. Also see Umberto Bacchi, "Nairobi Westgate Mall Siege: Al-Shabaab Accuses Kenyan Troops of Chemical Weapon Use," International Business Times, September 25, 2013.

[47] HSM Press tweet, September 25, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author. Also see Afua Hirsch, "Kenya Mall Attack: Dozens More Bodies Believed Buried Under Rubble," Guardian, September 26, 2013.

[48] Mike Pflanz, "Britain's Shadowy 'White Widow' Linked to SEAL Team Target in Somalia," Christian Science Monitor, October 8, 2013.

[49] HSM Press tweets, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author.

[50] HSM Press tweets, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author. Stating that they have “no interest” in harming women and children, the group claimed that it did everything “practically possible” to remove women and children from the mall.

[51] HSM Press tweets, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author.

[52] Anzalone, “The Rapid Evolution of Al-Shabab’s Media and Insurgent ‘Journalism.’”

[53] The African Crusaders: Fighting the West’s War, al-Shabab, June 27, 2010.

[54] Mogadishu: Crusaders’ Graveyard.

[55] Ibid.

[56] Rage, “Mujaahidiintu Duulaan Aargoosi ah Ayay Ku qaadeen Kenya,” al-Shabab, October 2011; Ali Mohamed Rage, “Statement of Shaykh Ali Dheere [Rage],” al-Shabab, September 24, 2013; Ali Mohamed Rage, “Mujaahidiintu Way Ufasaxanyihiin,” al-Shabab, September 22, 2013. The second statement, which is in Arabic, was advertised on the HSM Press Twitter account, first with an Arabic and then an English tweet.

[57] HSM Press tweet, September 24, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author.

[58] HSM Press tweets, September 25, 2013. This account has since been suspended by Twitter. The text of the tweets referenced has been saved by the author.

[59] It is possible that al-Shabab decided to produce an English audio translation of Godane’s statement to make it easier for television and radio outlets to play excerpts in their broadcasts.

[60] Ahmed Godane, “Badr Nairobi,” al-Shabab, September 25, 2013.

[61] Ibid.

[62] Ibid.

[63] “Westgate Attack: MPs to Call for Refugee Camps to Close,” BBC, September 30, 2013; “Number of Somali Refugees in Horn of Africa Passes 1 Million Mark,” United Nations Refugee Agency, July 17, 2012.

Table of Contents

Army Pursues Development of Soldiers’ Cybersecurity Skills < >

By Valerie Insinna, National Defense Magazine, 24 Oct 2013

Cyber-initiatives often conjure up images of network infrastructure or lines of computer code. But to win a war in cyberspace, the human element is even more important than hardware and software, a panel of military and industry experts said.

Not only is the Army on the hunt for talented “cyberwarriors” to carry out offensive and defensive operations, officials want normalize network security across the entire service.

“People are the key to gain and maintain a competitive advantage, and building a cyberforce is critical,” Lt. Gen. Edward Cardon, commanding general of the Army’s Cyberspace Command, said Oct. 23 at the Association of the U.S. Army annual conference. “Cyberspace is too big. No one entity has all the answers. No one knows all hardware. No one knows all code. No one has a monopoly on good ideas, so our team has to include the best minds in industry, government and academia.”

Finding and grooming the right personnel will be key, agreed Jim Young, Google’s Army account executive.

“When it comes to software coding, one superstar is as good as 1,000 general purpose coders. In cyber, the ratio is actually higher. They simply see things that others do not,” he said.

The Army’s 780th Military Intelligence Brigade is the Army’s premier cyberoperations unit and is at the center of the service’s recruitment, training and operations, said its commander, Col. Jennifer Buckner.

The unit strives to have a Google-like culture of innovation, she said. Some of the unit’s most competent cyberwarriors started the job with no formal intelligence training or technical education.

“Rank and position mean very, very little, but the skill sets that you bring to a mission will be rewarded, and you will be rewarded accordingly,” she said. “We have specialists that are performing missions today of national and strategic significance because they’re very good at what they do.”

Though the Army is ramping up activities in cyberspace, it is still sometimes frustrating that some parts of the force do not understand how to employ its capabilities, said Brig. Gen. George Franz III, director of current operations for the Cyber National Mission Forces.

Cybersecurity operations are “not enabling operations, they're not network operations, they are not just security, and they are just not intel. It is a full spectrum,” he said.

The battlespace cannot be thought of as a separate domain that operates apart from the rest of the force, agreed Lt. Gen. Dave Perkins, commanding general of the Command Arms Center. The Army eventually will incorporate cyber-events as a part of training exercises.

U.S. Training and Doctrine Command must decide what cyber skill sets need to be taught across the entire Army and “not just the people that know what control +alt + F8 does,” Perkins said. “And I have no idea what that does, so don't go home and do it," he continued, laughing.

This doesn’t mean that there will be cybersecurity experts at every level. Perkins compared possible use of such personnel to the Army’s air assets. There are no F-16 pilots organic to an infantry platoon, but soldiers can easily call up air support, he said.

Unlike with kinetic or electronic warfare, a commander in the cyberdomain may not be able to respond to an attack without receiving permission, Cardon said. That will change over time, as trust is established between cyber-officials and the rest of the Army.

“The problem in cyber is once you use [a weapon]... you can't get it back. It's out there, and often it gets reversed engineer right away. Before you know it, it can be used on you within a couple days,” he said.

Not only does the Army need to hire cybersecurity experts and train its existing force, the service must protect its infrastructure from malicious entities already inside its networks. Concerns about insider threats to the military reached a fever pitch after Edward Snowden, a former defense contractor with Booz Allen Hamilton, disclosed classified information on National Security Administration initiatives.

One way the service is tackling this problem is the development of “Army Network 2020, “ which will incorporate behavior-based analytics that can help identify possible anomalies, said Maj. Gen. Alan R. Lynn, vice director of the Defense Information Systems Agency.

“It will follow your pattern and how you operate. If you go to X number of website, it logs it. If you put out so many emails, it logs it. If you now change your behavior and so something completely different, you go to a separate site or an inside site and you start downloading a whole lot of information,” the network will send a red flag to security personnel, he said.

Not only may the system be able to identify when an individual is acting out of the norm, it could help determine when a computer has been taken over by a malevolent entity, he added.

Individuals are most likely to disclose government or company information shortly after they are hired or before they leave that organization. It’s impossible to monitor all the data streaming through a network, but the Army and defense contractors could increase monitoring of new and outgoing employees, said Charles Croom, Lockheed Martin's vice president of cybersecurity solutions.

Insider threats may also be less of a problem as the military trains its own personnel. The Army is decreasing its dependence on cybersecurity contractors, Buckner said. Civilian hires are still needed, but mostly for niche capabilities.

Table of Contents

South Korea Says North Korea Developing Electromagnetic Pulse Weapons

By Agency France Presse, November 4, 2013

The National Intelligence Service (NIS) said in a report to parliament that the North had purchased Russian electromagnetic pulse (EMP) weaponry to develop its own versions.

EMP weapons are used to damage to electronic equipment. At higher energy levels, an EMP event can cause more widespread damage including to aircraft structures and other objects.

The spy agency also said the North’s leader Kim Jong-Un sees cyber attacks as an all-purpose weapon along with nuclear weapons and missiles, according to lawmakers briefed by the NIS. The North is trying to hack into smartphones and lure South Koreans into becoming informants, it said.

It has collected information on where South Korea stores chemical substances and oil reserves as well as details about subways, tunnels and train networks in major cities, it said.

The spy agency also said North Korean spies were operating in China and Japan to distribute pro-Pyongyang propaganda.

North Korea is believed to run an elite cyber warfare unit of 3,000 personnel.

A South Korean lawmaker, citing government data, said last month that the North had staged thousands of cyber attacks against the South in recent years, causing financial losses of around $805 million.

In addition to military institutions, the North’s recent high-profile cyber attacks have targeted commercial banks, government agencies, TV broadcasters and media websites.

North Korea has denied any involvement in cyber attacks and accused Seoul of fabricating them to fan cross-border tension.

Table of Contents

Research Alliance Looks to Guide US Army's Cyberwarfare Future

By Joe Gould, Defense News, Oct. 21, 2013

The Army is concerned that near-peer adversaries will one day use cyber attacks to target soldiers' laptops, radios or other small computers that surround them in vehicles and weapon systems on the battlefield. The enemy might insert malicious software to steal, destroy or fake information, or to misdirect a flying drone, send a soldier spoofed orders or detonate some ordnance prematurely.

To fight back, the Army Research Laboratory is exploring how soldiers one day might calculate risk, detect intrusions and make networks agile to evade attacks as part of a newly formed consortium of academic institutions, the defense industry and the Army Communications- Electronics Research, Development and Engineering Center. It's also researching the psychosocial perspective on attackers, defenders and the soldiers who use the networks.

It could inform future acquisitions, training, doctrine and tactical decisions, according to Alexander Kott, associate director for science and technology for the lab's Computational and Information Sciences Directorate.

The collaborative research alliance, launched Sept. 20, is set to run for five years, with an optional five-year renewal at $3.3 million to $5.2 million annually.

It is led by Penn State University, and includes Carnegie Mellon University, Indiana University and the University of California-Davis and Riverside.

The first area, "risk research," seeks to develop theories and more fluid models for risk assessment.

"We need to have much better abilities to change our ways on the fly, depending on what we observe the enemy doing," Kott said.

The next, "detection research," would shape cyber threat detection and recognition capabilities. "The faster we can detect the enemy, the faster we can change our tactics to become less vulnerable to them," Kott said. "Malware is the enemy on our networks, and if we can't see it, it will stay on our networks and keep harming us."

The last, "agility research," supports planning and control of cyber maneuvers, ways to rapidly adjust Army networks and defenses to defeat or mitigate cyber threats and effects. As a frequency-hopping radio adjusts to evade would-be eavesdroppers, networks can be made more dynamic to shake off intrusive malware.

One of the most unique research areas is psychosocial or human factors on the network, which includes not only how to out-think and anticipate the enemy but better protect soldiers and civilians. Why do soldiers and civilians who, in defiance of their training, create weak passwords

and click on suspicious links, and how can that be improved? The research will explore how to psychologically prepare a soldier for a sophisticated cyber attack."I think we'll have to get more sophisticated," Kott said. "Just like... [with improvised explosive devices], I think there's a little bit of an analogy here."

Table of Contents

Saudi Experts Boost Their Skills in Electronic Warfare

By Saeed Al Khotani, Saudi Gazette, 13 Nov 2013

RIYADH – Saudi experts have acquired wide expertise in the field of electronic warfare (EW) and the Kingdom are going ahead in enhancing their capabilities in this field, said Deputy President of King Abdulaziz City for Science and Technology, Prince Turki Bin Saud Bin Mohammed Al Saud, at his opening address in the 3rd Saudi symposium of EW at KACST headquarters in Riyadh on Tuesday.

"This was because EW has become an important element in today's world occupying outstanding position in the civil and military activities and as well has become a concern to the majority of the countries including us," the Prince said.

"KACST has established an specialized center for censors and defensive electronics as part of its structures with the aim of conducting scientific researches for application purposes and technology transfer to serve our armed forces and build competent national capabilities in EW to secure self-reliance to the nation in this field," he added.

The symposium was opened by Prince Turki and the Chief of the General Staff of the Armed Forces, Field Marshal Husein Al Gubayyel, in the presence of a large audience of top military and civil officials along with researchers and experts.

A group of Saudi senior military experts in EW were honored for their distinguished efforts and contribution in developing the field of EW and building capabilities in the Kingdom.

Also American Lt Gen Robert J. Elder, Jr., the President of the Association of Old Crows (AOC), was honored at the event organized by KACST, Ministry of Defense, and the Saudi chapter of AOC.

AOC is a not-for-profit international professional association with over 13,500 members and 180 organizations engaged in the science and practice of EW, Information Operations, and related disciplines.

Its name "Old Crows" emerged from the first large-scale use of Electronic Warfare during the WWII Battle of Britain and the US and allied bombing raids over Europe. The Allied Radar Countermeasure operators used the codename "Ravens" and employed receivers and transmitters to monitor and jam threat frequencies. Military jargon later changed "Ravens" to "Crows". The Saudi chapter of AOC was established 2008, but did not get official recognition until this year during the fiftieth anniversary of the association in USA.

Both Prince Turki and Al Gubayyel opened and toured the exhibition organized alongside the symposium. Around 30 exhibitors participated in the exhibition from 14 countries displaying the latest products in EW.

Table of Contents

Fighting On the Cyber Battlefield: Weak States and Nonstate Actors Pose Threats

By James Jay Carafano, Ph.D., Heritage Foundation, 8 Nov 2013

America is already fighting in cyberspace. Look for more, not fewer, engagements in the years ahead. But the Pentagon should worry less about a cyber Pearl Harbor and more about losing the daily slog in the cyber-trenches.

The cyber threat is a serious national security issue. Indeed, it's a virtual jungle out there. Our online enemies are legion, but they are not created equal. Among the ranks of our cyber competitors, China and Russia stand out as superpowers.

This is not to say that even very weak states pose no danger. History is filled with examples of Davids laying low the most powerful Goliaths. Don't believe for a moment that states like Iran or Syria can't pull off the cyber equivalent of a stone to the temple.

Indeed, both have already loosed cyber-raiding parties. Most recently, as President Obama was threatening punitive strikes against Syria, media reports reveal that the Syrian Electronic Army successfully hacked the New York Times, Twitter and the U.S. Marine Corps website.

Nor are all threats state-sponsored. Some countries do a terrible job of policing bad actors in their cyberspace. Pakistan, for example, is emerging as a hub of cybercrime. This can magnify international tensions. For example, Pakistani hacker groups attacked Indian websites during the height of the 2011 Kashmir crisis.

Nonstate actors are serious players in cyberspace — for good and ill. So far, most of the malicious activity from private-sector hackers has been geared to accumulate wealth, not to wage war on America. Even terrorist groups use the Internet primarily to facilitate communications and financing rather than to slaughter innocents directly.

Obviously, the United States has some very big cyber guns at its disposal. Just how big remains largely classified. But revelations from the likes of Pfc. Bradley Manning and former National Security Agency contractor Edward Snowden give us some idea. An unclassified, inside summary of our cyber capabilities would sound like: "The U.S. can do things nobody else in the world can do." The unfortunate corollary is: "And we can't defend against everything we can do."

Still, it's premature to head to the bunker. There's a "mutual assured destruction" aspect to the Internet: If it were taken down, all sides would lose.

Further, the Web is likely to endure most any cyber conflict (absent taking out the underlying physical infrastructure including the power grid and undersea cables). It has already proved far more resilient than commonly assumed. Think of 2009's Green Revolution in Iran. Despite that nation's limited infrastructure, spirited denial-of-service attacks from both sides, and an insatiable global demand for information, the Internet held up well. Or go back further, to Sept. 11. A National Academies study concluded that the Web proved fairly resilient despite the destruction to telecommunications in Manhattan and a tsunami-like surge in Internet traffic.

But the military must also worry about cyber conflict at the sharp end of war. Today's military commander must have an understanding of his cyber footprint that is every bit as sophisticated as his knowledge of the terrain, the forces at his disposal and the makeup of the enemy.

Maintaining "retail" cyber is much more difficult in military operations than in civilian life. War zones seldom offer Starbucks with Wi-Fi. Nor are cyber operations just an extension of traditional electronic warfare (like jamming). A commander, for example, might be supporting a humanitarian operation where the tasks are quite different from, say, taking an enemy offline.

Moreover, the military can't just buy secure, classified systems for every need. For starters, that's too expensive. And, it would limit engagement with nonsecure folks in their area of operation. Plus, if a very expensive "secure" network becomes comprised, the fallout is usually far worse because the communications have been less guarded.

Of course, off-the-shelf commercial technology can't provide a competitive advantage. The bad guys can buy iPhones too.

What all the services need on the front end is software that provides "visualization" of the enemy's cyber footprints, analytical tools that help them identify the most critical information gathered, and people skilled at interpreting and acting on the information.

In today's White House, the only answer to "How much is enough for defense?" is "less." That leaves the services wondering how they can possibly build the infrastructure and amass the human capital needed to give our side a real edge on the cyber battlefields of the future.

The slower we move ahead in this arena, the faster our competitors can catch and surpass us. Our military may not face an online Pearl Harbor, but it could well have a couple of electronic Alamos.

Table of Contents

US Governmental Information Operations and Strategic Communications: A Discredited Tool or User Failure? Implications for Future Conflict

By Dr. Steve Tatham, US Army War College Strategic Studies Institute, 3 Dec 2013

Through the prism of operations in Afghanistan, the author examines how the U.S. Government's Strategic Communication (SC) and, in particular, the Department of Defense's (DoD) Information Operations (IO) and Military Information Support to Operations (MISO) programs, have contributed to U.S. strategic and foreign policy objectives. It assesses whether current practice, which is largely predicated on ideas of positively shaping audiences perceptions and attitudes towards the United States, is actually fit for purpose. Indeed, it finds that the United States has for many years now been encouraged by large contractors to approach communications objectives through techniques heavily influenced by civilian advertising and marketing, which attempt to change hostile attitudes to the United States and its foreign policy in the belief that this will subsequently reduce hostile behavior. While an attitudinal approach may work in convincing U.S. citizens to buy consumer products, it does not easily translate to the conflict- and crisis-riven societies to which it has been routinely applied since September 11, 2001.

Download link: http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1182 3Mb; 99 pages

Table of Contents

US Senators Warn On Huawei Deal with South Korea

By Richard McGregor, CNBC, 3 Dec 2013

A deal signed in South Korea by Huawei Technologies, the Chinese telecommunications giant, could undermine Washington's defense ties with Seoul, according to two powerful U.S. senators.

Dianne Feinstein and Robert Menendez, respectively the chairs of the Senate's intelligence and foreign affairs committees, said in a letter that "maintaining the integrity of telecommunications infrastructure" was critical to the alliance.

Congress has long objected to Huawei expanding its business in the U.S. but the letter is a rare example of political leaders in the country making an issue of the Chinese company's investments offshore.

U.S. suspicions about Huawei could also rebound on American technology companies abroad in the wake of documents leaked by former intelligence contractor Edward Snowden outlining their co-operation with Washington's spy agencies.

The letter, sent in late November, was addressed to John Kerry, the secretary of state, Chuck Hagel, the defense secretary, and James Clapper, the director of national intelligence.

The letter's timing dovetails with a planned trip by Joe Biden, U.S. vice-president, to China and South Korea, a visit taking place in the shadow of Beijing's announcement last week of an extension of Chinese-regulated air space.

Beijing's move, primarily aimed at chief regional rival Japan, also impinged on the so-called air defense identification zone of South Korea. Mr Biden is in China on Wednesday.

The letter from Senators Feinstein and Menendez expresses concerns about Huawei's selection to build a broadband network for a subsidiary of South Korea's LG Corporation.

"An essential feature of our alliance are the numerous steps our militaries and our intelligence agencies are taking together to advance training and information sharing," it says.

The Huawei deal, the letter goes on, "raises serious questions and potential security concerns" and asks its recipients to assess any possible threat.

In recent years, U.S. lawmakers have objected to Huawei's acquisition of patents from 3 Leaf, a small U.S. company, and forced Japan's SoftBank to limit the use of the Chinese company's technology as a condition for buying a U.S. carrier.

But Washington's hardline could provoke a backlash against U.S. companies offshore. Documents leaked by Mr Snowden revealed U.S. intelligence has forced U.S. telecommunications carriers to hand over phone records and also tried to infiltrate their systems to gain access to their private records.

"Hounding Huawei really sets a precedent that will eventually be used against U.S. companies abroad," said Christopher Soghoian, principal technologist of the American Civil Liberties Union. "All the things that Huawei has been accused of, U.S. companies do."

Huawei has long considered exiting the U.S. market altogether because of the political barriers to doing business there.

In a rare interview with the western media this week, Ren Zhengfei, the Huawei founder and chief executive, said if the company got caught in the middle of U.S.-China tensions, "it's not worth it".

He added: "Therefore, we have decided to exit the U.S. market, and not stay in the middle," without elaborating.

Huawei is a private company and insists its close ties with China's ruling communist party do not affect its commercial decisions.

Both the UK and Australia, intelligence partners of the U.S., have restricted Huawei's business in their countries or subjected them to greater oversight.

Table of Contents

Cyberspace Warriors Graduate With Army's Newest Military Occupational Specialty

By Wilson A. Rivera, Fort Gordon Public Affairs Office, December 6, 2013

FORT GORDON, Ga. (Nov. 27, 2013) - The network is under attack! Cyber attacks are a daily reality and are growing in sophistication and complexity. How does the Army keep pace with this evolving threat and defend its network?

Fifteen Soldiers made history when they were awarded the newest Army military occupational specialty, 25D, cyber network defender, during a graduation ceremony Nov. 27, held in Alexander Hall at Fort Gordon, Ga.

Soldiers completed a 14-week course, considered rigorous for its curriculum, to learn the skills needed to meet the demand for cyber warfare.

"Cyberspace is composed of hundreds of thousands interconnecting computers, servers, routers, switches, fiber optic cables which allow our critical infrastructure to work," said Command Sgt. Maj. Ronald S. Pflieger, regimental sergeant major for the U.S. Army Signal Center of Excellence and Fort Gordon, guest speaker for the first-ever graduating class for the Cyber Network Defender course. "A functional and healthy cyberspace is essential to our economy and national security."

"With the need for educated individuals to defend our network, so does the need to engage cyberspace," Pflieger said.

Through the establishment of the new cyber network defender, 25D military occupational specialty, known as an MOS, there were changes made to the classification and structure among the 25 career management field series for communications and information systems operation with other MOS revisions of information technology specialist, 25B; radio operator-maintainer, 25C; and telecommunications operator chief, 25W.

Significant changes to the 25 career management field identify the positions and personnel to perform duties with cyber network defense, and selected functions for cyber network defender MOS positions transferred from previous MOS positions associated with cyber network defense.

Major duties a cyber network defender will perform include protecting, monitoring, detecting, analyzing, and responding to unauthorized cyberspace domain actions; deployment and administration of computer network defense infrastructures such as firewalls, intrusion detection systems and more. Soldiers are also tasked to take action to modify information systems, computer network configurations in regard to computer network threats and collect data to analyze events and warn of attacks. Cyber network defenders will be trained to perform assessments of threats and vulnerabilities within the network environment, conduct network damage assessments, and develop response actions.

Increases in cyberspace operations training continue in key Army leader education programs.

"A gap was identified within the non-commissioned officers' career field," Pflieger said. "The next step was to identify the right Soldiers."

Staff sergeants interested in becoming a cyber network defender must meet the requirements, such as having a minimum of four years information technology experience, an Armed Services Vocational Aptitude Battery of 105 in both General Technical and Skilled Technical scores. They must be a U.S. citizen, complete an in-service screening, and have a recommendation from their battalion or higher.

Table of Contents

China Spins New Lesson from Soviet Union's Fall

By Jeremy Page, Wall Street Journal, Dec. 10, 2013

BEIJING—The Communist Party boss in eastern China's Jiangsu province summoned local officials recently to a compulsory study session. Their task was to watch a six-part documentary on the Soviet Union's collapse.

The film begins with images of the Soviet Union in its heyday, but quickly cuts to graphic footage of unrest in China's northern neighbor in the 1990s, set to ominous music and punctuated by Russian communists lamenting their nation's fate.

When the screening in Jiangsu ended, state media reported, local party chief Luo Zhijun exhorted the assembled officials to "correctly understand the lessons of history." The film's message: The Soviet Union didn't fall apart because of the communist system itself, but because of individuals who betrayed it, especially Mikhail Gorbachev.

The film is part of an ideological campaign launched by China's new leader, Xi Jinping, to re-energize the party and enforce discipline among its members. It has been shown at dozens of political meetings since September.

The frequent showings suggest Mr. Xi believes China needs to reinforce its Leninist political system rather than limit the party's powers. Party insiders and academics say it is part of an effort to combat what is portrayed as an American conspiracy to overthrow the party through "peaceful evolution"—the spread of Western ideas via media, academia and popular culture.

The office in charge of Mr. Xi's campaign didn't respond to questions about the film, called "20th Anniversary of the Death of the Soviet Party and State: As the Russians Relate," but said the campaign drew on experiences from China and the rest of the world.

The film, which was produced by a retired Chinese major general, has drawn criticism from some Chinese scholars of Soviet history, including some within the party. They argue that Moscow's mistake was to overlook deep flaws in the Soviet political and economic systems that emerged long before Mr. Gorbachev.

The film "lacks rational analysis, is mainly aimed at defending the Stalinist system and is illogical in many places," wrote Zuo Fengrong, an expert on Soviet history at the Central Party School, a party think tank and training academy, in a recent review. "As a film for educating party members, it can only play a misleading role." She declined to comment, but several other Chinese scholars echoed her views.

The debate over Soviet history is playing out amid a broader one about China's future. Mr. Xi, who took power last November, is moving to establish himself as the most individually powerful Chinese leader since Deng Xiaoping.

At a meeting in November, the Central Committee—the party's top 376 leaders—endorsed a package of reforms proposed by Mr. Xi, designed to open the economy further to market forces and to boost the spending power of farmers and migrant workers.

On the political front, Mr. Xi is heading in the opposite direction, reaching into the past to reinforce Leninist orthodoxy and silence those who advocate using the constitution to restrict party power.

After the meeting, China announced the establishment of a new "national security committee" that Chinese analysts say will give Mr. Xi greater powers to oversee domestic security, foreign policy and the military. The committee's name uses the same Chinese characters as those used to translate the names of the U.S. National Security Council and for the Soviet KGB.

Some Chinese academics who advocate liberal political reforms are drawing parallels between Mr. Xi's political program and that of Yuri Andropov, the former KGB chief who launched campaigns against corruption and dissent after he took over as Soviet leader in 1982.

Modern-day China is vastly different from the Soviet Union. The Chinese economy is larger, faster-growing and more closely integrated with the rest of the world than the Soviet one ever was. China's political system now allows greater personal freedoms than the Soviet Union did, and it has established retirement norms for its leaders, also something the Soviets never managed.

In other ways, China's party remains rooted in the past, with its decision-making mechanisms, household-registration system and policies toward ethnic minorities based on the old Soviet model.

"When the leadership gets up in the morning and goes to bed at night, it is the Soviet collapse that haunts them, only augmented by fears deriving from the Central Asian 'color revolutions' and Arab Spring," says David Shambaugh, an expert on Chinese politics at George Washington University. "Observers don't realize just how similar the Chinese system is to the Soviet system. The former is cloned from the latter."

In essence, Mr. Xi is gambling that China's version of one-party rule can succeed where the Soviet Union's failed, with respect to policing itself and managing a changing society, party insiders say. Part of that strategy is reasserting an official narrative of history.

In a speech in December, Mr. Xi blamed Mr. Gorbachev for losing control of the Soviet military and allowing "historical nihilism" to question the achievements of Lenin and Stalin, according to people who have read a transcript.

In April, the party issued an edict, known as Document No. 9, which warned officials to resist the spread of Western values and "incorrect thinking," especially attempts to reassess history.

Mr. Xi has publicly said that Mao's achievements should be considered equal in importance to the country's progress since economic reforms were introduced in 1978.

Some of Mr. Xi's admirers argue that he is taking a conservative stand early to ensure political support as he tackles resistance to his promised economic changes.

There is a growing sense within the party, however, that Mr. Xi is aligned more closely than his two predecessors were with party conservatives and some military leaders who feel China must resist Westernization at all costs.

Another film circulating in the party and available online, "Silent Contest," contends the U.S. is trying to weaken China through nongovernmental organizations and military-to-military exchanges, among other things. It was produced in conjunction with the National Defense University—China's equivalent of West Point—under the auspices of Gen. Liu Yazhou, its political commissar and the son-in-law of a former president, who is considered close to Mr. Xi.

Gen. Liu had been considered a reformist voice within the military after he wrote an article in 2010 warning that China would face the same fate as the Soviet Union if it didn't democratize. "The Soviet Union's problems were all systemic problems," he wrote back then.

In "Silent Contest," however, he is shown warning that the U.S. is trying to contain and weaken China through the projection of Western values—or "peaceful evolution."

The man behind the film on the Soviet collapse also features in "Silent Contest." He is Li Shenming, a retired major general. He has served as vice head of the Chinese Academy of Social Sciences, or CASS, and as personal secretary to the late Wang Zhen, a revolutionary leader who strongly supported the military crackdown on pro-democracy protests in 1989.

Mr. Li is an outspoken admirer of Stalin and Mao. He didn't respond to requests for comment.

People who know Mr. Li describe him as the leader of a small group of ultraconservative thinkers, many of them attached to the CASS Center for World Socialism Research, which produced the film.

In a recent article in Red Flag Manuscript, a party magazine, he wrote that hostile Western forces had deliberately exaggerated estimates that Stalin and Mao were each responsible for the deaths of 30 million people.

"I don't think many people listen to him in the scholarly world, but in the party leadership, people apparently listen to him," says Hua-yu Li, a political-science professor of at Oregon State University who has written about Soviet influence on China.

The film is based on just one of dozens of studies of the Soviet collapse that Chinese academics have undertaken since 1991. Many of those studies reached different conclusions about what triggered the collapse: an ossified political system, corruption in the elite, chauvinistic policies toward ethnic minorities and fundamental flaws in its economic model.

Those issues are pertinent to China today as it grapples with official graft, an overly powerful state sector and unrest in its far western regions of Tibet and Xinjiang, Chinese scholars say.

The Soviet collapse remains a sensitive topic in China because Chinese communist leaders have long looked to Moscow for guidance—both positive and negative—about their own future.

Until the late 1950s, the Soviet Union provided them with inspiration, advice and aid. After an ideological rift in 1959, Beijing saw Moscow as a rival for leadership of the communist world.

In the 1980s, reformist Chinese leaders watched Mr. Gorbachev's perestroika and glasnost reforms with growing interest—until those leaders were sidelined following the military crackdown on pro-democracy protests around Tiananmen Square in 1989.

Since the Soviet collapse in 1991, Chinese leaders have been preoccupied with understanding its root causes and avoiding a similar fate.

Many early Chinese studies concluded that the Soviet collapse was caused either by Mr. Gorbachev or by the U.S. strategy of "peaceful evolution." In the mid-1990s, Chinese scholars began exploring other factors, often concluding that its roots lay in a lack of reform under Leonid Brezhnev, who ruled from 1964 to 1982.

Jiang Zemin, China's party chief from 1989 to 2002, encouraged many of the studies, according to several Chinese scholars.

In 2004, China's leadership reached an internal decision that the Soviet collapse was caused by Moscow abandoning core Marxist principles, but Chinese leaders before Mr. Xi rarely spoke about it.

The debate has continued within the party and academia, fueled by more studies of alternative theories, many conducted at the Central Party School. The school's official newspaper published an essay this week blaming the Soviet collapse mainly on the collectivization of agriculture under Stalin, and warning of the dangers of failing to reform.

Mr. Li and his colleagues at the CASS World Socialism Research Center have consistently rejected such arguments and promoted the blame-Gorbachev theory.

Mr. Li produced an early version of his film in 2006, followed by a book in 2008. Both were circulated only within the party. He then released an updated version of the film in 2011.

It became compulsory viewing for party officials, with widespread coverage in state media, after it was adopted as part of a "mass line" campaign launched by President Xi.

Some Chinese scholars of Soviet history say they believe Mr. Li and the other filmmakers, sensing Mr. Xi's conservative political outlook, used their political connections to have their work included in the campaign. Wu Enyuan, a Russia expert and vice head of the CASS World Socialism Research Center who was involved in making the film, denies it was chosen because of political connections.

The updated film was based in large part on recent Russian research, he says, and Chinese scholars who criticized it mostly lacked Russian language skills and the experience of visiting the Soviet Union or post-Soviet Russia.

"There is one central issue," he says. "Did the Soviet Union collapse because of historic systemic problems—problems with the Stalinist model—or because of Gorbachev's mistakes? Our view is the latter. It is consistent with the leadership's."

Table of Contents

Drawing Lessons from Zimbabwe's War of Liberation: Efficacious Use of Propaganda and Violence

By Jephias Andrew Dzimbanhete, Small Wars Journal, 10 Dec 2013

Abstract

The article seeks to examine aspects of Zimbabwe's liberation war from which today's politics can draw lessons. The aspects are propaganda and violence that were deployed by the Rhodesian Front-led government and the liberation movements. The basis of colonial propaganda during the war of independence was the misconception that the rural people were passive, unsophisticated and gullible. On the other hand the liberation movements, who were cognisant of the significant role of the subaltern group, the peasants, with

whom they collaborated, did not propagate delusive propaganda. The liberation forces deployed propaganda that was bound up with the fight for freedom. The white minority regime unleashed indiscriminate violence against the civilian population. The intention was to glean information about the freedom fighters and punish the rural population for cooperating with the liberation fighters. Such random violence rebounded and did not produce the desired results. The liberation forces used violence against members of the rural population who collaborated with the Rhodesian regime and security forces. Guerrilla violence was selective and generally did not alienate the liberation guerrilla fighters from the rural populace. This article derives from the author's doctoral study on the Zimbabwe African National Union (ZANU)'s guerrilla war.*

Introduction

Zimbabwe attained its independence in 1980 after a war that pitted the colonial forces of Rhodesia against the Zimbabwean liberation guerrilla forces. The war assumed a guerrilla warfare character and drew the warring parties into a contest that was both military and political. The goal of either side in the political rivalry was to control the African population that resided in the countryside which was the war's theatre of operation. The Rhodesian security forces needed to win the ‘hearts and minds' of the rural populace so that they could secure information about the activities of the nationalist guerrilla forces. The colonial forces thus desired the co-operation of the rural African people in their agenda of fighting what they labeled ‘terrorism'. On the other hand it was imperative for the liberation forces to secure political control of the rural population. This entailed securing their sympathy and support. The profit of political control of the rural population for the liberation fighters was the availability of food, clothing, intelligence and other logistical support. Controlling access to the civilian population was the key to defeating one's opponent in the liberation war. The contending forces got embroiled in a situation that demanded the deployment of propaganda and violence to achieve the goal of exerting political control over the civilian population. I do not however intend to catalogue lessons that could be drawn from the Zimbabwe's war of liberation war in the manner of saying lesson number 1, lesson 2 and so on. I simply examine and revisit the nature of war-time violence and propaganda and present a critical expose which has been lacking in much of the documented narratives of the war of national liberation. In this article I subscribe to Sturges's definition of propaganda. He writes that propaganda is the practice of distributing material that is untrue or if it is true, it is actually not relevant and applicable. The aim of propaganda is to confuse and deceive those that receive it.[1]

Wartime Propaganda

Propaganda dissemination by the war's rival players involved a process of projecting information about oneself in a positive manner and of the adversary in a negative style. For the contesting players propaganda thus served as either an instrument of offence or defence. Whilst the Rhodesian colonial regime was able to mobilise massive propaganda machinery the Zimbabwean liberation movement had to make do with an inferior but effective propaganda apparatus.

The Propaganda Tool of the Rhodesian Government

The colonial government churned out propaganda which largely demonised the liberation fighters. The intention was to alienate the liberation fighters from the rural populace and to elicit the loyalty of the residents of the rural areas, the war's theatre of operation. The basis of this propaganda was that the rural population was unsophisticated, gullible and passive. Such colonial stereotype and bigotry found expression in intimations of the following nature: ‘The typical ZANLA fighter was unsophisticated, but the impoverished peasants among whom he operated were usually illiterate and even more unsophisticated'.[2] Newspapers and magazines which included The Rhodesian Herald, The Sunday Mail, The African Times, The Bulawayo Chronicle, The Police Outpost, The Parrot and others were awash with reports on the glowing and successful military successes of the Rhodesian army forces. These reports compiled by white Rhodesian journalists exaggerated the numbers of liberation fighters that were killed in encounters between the warring parties and also understated the figures of the Rhodesian soldiers who died in the same encounters. The hope was that the black population of Rhodesia, especially those who resided in the rural areas, would realise that it was futile to back a losing side. This would drive them away from co-operating with the liberation fighters. The rural populace were also bombarded with war communiqués that came through the radio services of the Rhodesian Broadcasting Corporation (RBC). These communiqués not only inflated the number of the freedom fighters that the Rhodesian armed forces killed but also understated the figures of members of the Rhodesian forces who died at the hands of the nationalist fighters.

The same propaganda machinery of the Rhodesian regime demonised the liberation fighters and stressed the cruelty and brutality of the freedom fighters. Besides exaggerating guerrilla violence this propaganda fingered the liberation fighters for atrocities they probably did not commit. Instead the Rhodesian Selous Scouts, a pseudo-guerrilla unit of the colonial armed forces, committed atrocities disguised as the liberation guerrilla fighters. These atrocities included the murder of missionaries at rural mission stations and use of chemical weapons. Writing in 2006, Parker, a former Rhodesian serviceman, revealed that the Selous Scouts were responsible for the murder of Father Killian Huesser, a Roman Catholic priest based at Berejena Mission in February 1980.[3] The Rhodesian media had rushed to blame the Zimbabwe African National Liberation Army (ZANLA), one of the two liberation armies of Zimbabwe's war of independence. The cold-blooded murder of seven white missionaries at St. Pauls' Musami on 7 February 1977 was also blamed on the liberation fighters. Writing in 1999, Reid-Daly echoed Rhodesian regime propaganda when he indicated that the white missionaries at Musami Catholic Mission were slaughtered without mercy by Robert Mugabe's ZANLA forces.[4] The balance of probability points to the Rhodesian Selous Scouts as being responsible for the murder. It was very likely that the Rhodesian Selous Scouts were responsible for the murder of white missionaries at rural outposts and rural African businessmen.[5] The Rhodesian regime made capital of these murders and used them as propaganda material to discredit the forces of liberation. This was in the vain hope that this would erode the support that the rural population rendered to the liberation forces. The Rhodesian Ministry of Information produced, and distributed pamphlets that told gory stories of guerrilla violence on the civilian population. The African people were however not turned away from the liberation fighters but instead they became glued to the nationalist guerrilla fighters and the cause for freedom.

The weakness of Rhodesian propaganda was it lacked essential preoccupation with the truth. The rural population who were the target of the propaganda was aware of its factual deficiency and found it ludicrous. For example part of the Rhodesian propaganda that reached the African people insinuated that the freedom fighters willy-nilly raped married women. But peasants never experienced these scenarios in the war zones. The Rhodesian regime also propagated that the armed wings of the liberation movements were ‘terrorists' who murdered civilians indiscriminately and for no reason. The rural people witnessed a totally different picture. The nature of Rhodesian propaganda stemmed from the faulty colonial view that the African mind was a container that could be emptied and refilled. Contrary to this view, the rural African people were awake to the fact that the atrocities that were attributed to the freedom fighters by Rhodesian propaganda were committed by Rhodesian army units especially the Rhodesian Selous Scouts.

Overall the propaganda that was disseminated by the Rhodesian authorities failed to produce the desired results. The target of this propaganda (misinformation), the rural population, unfortunately, was not moved. The rural people remained committed to the forces of liberation and the cause of freedom. In reality what the rural African population persistently encountered were atrocities committed by the Rhodesian security forces. Insidious colonial injustices continued to bite the African people. The continual refusal by the colonial authorities to grant economic and political spaces to the African population, which was the root cause of the liberation struggle, made their propaganda count for nothing.

The Liberation Fighters and Their Propaganda

Pro-Rhodesian narratives have insinuated and acknowledged that the liberation fighters waged a far more effective psychological and propaganda war than the white Rhodesians.[6] This was a result of the flawed conviction of the white Rhodesians that the claim by the liberation fighters that the discontented black masses of the impending new Zimbabwe were oppressed by the Rhodesian minority government was propaganda.[7] The political mobilisation of the rural population by the liberation fighters emphasised the cruelty and brutality of the colonial forces and colonial injustice that severely gnawed the African population. This was real and could not pass as propaganda (misinformation). It was largely at pungwe (night gatherings) that the liberation guerrilla fighters conducted political mobilisation of the rural peasants. Guerrilla propaganda appeared in the military reports that the liberation fighters announced at pungwe gatherings and through the radio broadcasts of the Voice of Zimbabwe that was beamed from Dar-es-Salaam, Lusaka and Maputo during the war. These reports amplified the military successes of the liberation fighters especially the ZANLA forces. This was largely through the deliberate avoidance of stating the military setbacks and losses of the liberation forces and inflating cases of fatalities.[8] The propaganda of the nationalist liberation forces was effective because it was crafted in such a way that it fitted in with the expectations of the rural people who were yearning for the removal of the unjust colonial system. The study turns to the aspect of violence which was bilaterally deployed for diverse reasons and in different circumstances by the rival parties during Zimbabwe's war of liberation.

Wartime Violence

The contesting players in Zimbabwe's war of decolonisation resorted to violence in different contexts. The Rhodesian security forces encountered the challenge of failing to engage the Zimbabwean freedom fighters in a frontal war because the latter adopted guerrilla warfare. Consequently, the Rhodesian armed forces had to rely on a set of strategies often called counter-insurgency, whose main objective was to deprive the guerrilla fighters of civilian support. This constituted the violence that was deployed by the colonial army against the civilian population in the rural areas. Counter-insurgency entailed instituting draconian reprisals and meting out collective punishment against civilians for their collaboration with the freedom fighters. Due to their preoccupation with survival the guerrilla fighters avoided frontal military engagement of the Rhodesian security forces. Guerrilla violence visited members of the rural populace who jeopardised the lives of the freedom fighters by reporting guerrilla activities to the Rhodesian security forces. However, before the guerrillas resorted to civilian executions they warned would-be traitors or collaborators against providing the colonial forces with information on their activities.[9] Invariably, guerrilla violence was used as a last resort when members of the rural population failed to take heed of guerrilla warnings. The liberation fighters thus used violence on civilians sparingly because they could not afford to lose the priceless support they rendered them. Civilian support and co-operation was the linchpin of guerrilla survival in a war in which they faced superior forces.

The Colonial Army's Repressive Violence

The violence that was used by the Rhodesian government troops against the rural people was vastly greater than that used by the guerrillas. This was because they were the incumbent government's armed forces and consequently had superior military machinery at their disposal. Many black civilians in the war zones became victims of this violence. The regime's soldiers were motivated to commit violence against the rural peasants (the guerrillas' support base) because of their failure to glean information about the guerrilla fighters and their activities. Colonial repressive violence was also inspired by the obvious fact that the rural people provided logistical support to the guerrilla forces. In their oral testimonies civilians who participated in the war of liberation have indicated that they were subjected to forms of repression that included terror, starvation, death and destruction of their property and homes[10]. In addition to this repression the colonial authorities introduced forceful relocation of the peasants especially along the country's borders. Werbner noted the extreme measures of the Rhodesian regime from 1973 onwards of collective punishment imposed under the Emergency Powers directed against whole communities for supporting the liberation fighters.[11] The measures included imposition of dusk to dawn curfew. Members of the rural population who broke these curfew regulations were shot at. Excessive force was used in the relocation of Africans into ‘protected villages' which were introduced to deny the liberation forces' access to the rural population.

The guerrilla fighters managed to negotiate a convivial relationship with the rural juveniles, who among other wartime duties provided them with intelligence about the Rhodesian security forces. The co-operation and alliance between the freedom fighters and the juveniles (vanamujibha and vanachimbwido) was significant in the successful prosecution of the liberation war. This collaboration infuriated the Rhodesian security forces who decided to shoot dead all juveniles who were found outside homes at whatever time of the day. Entire villages, homes, granaries, and crops in the rural areas were burnt down by the Rhodesian armed forces. The Indemnity and Compensation Act that was passed by the Rhodesian government in 1975 granted the colonial regime officials and forces with the immunity against prosecution for atrocities that they committed against the civilian population.[12] This Act of Parliament officially bestowed on the Rhodesian army forces and other government officials the carte blanche to commit atrocities and murder on the rural people. Cases abound of Rhodesian security forces shooting dead civilians for no apparent reason during the war. They would make reports that they killed guerrilla fighters. In a rural area south of Masvingo, a man and his four children who were working in their field were shot dead by Rhodesian soldiers. The soldiers actually went about boasting that they had killed five guerrilla fighters.[13]

Villagers were sometimes witness to grisly incidents such as the bayoneting of a pregnant woman to death by the Rhodesian security forces. One ex-mujibha related such murder of a pregnant woman near Morgenster Mission, southeast of Masvingo. The responsible Rhodesian security forces unkindly commented that she was carrying communist weapons in her womb.[14] Terror was exercised on the rural peasants in various other forms. The imposition of a dusk to dawn curfew not only curtailed the movement of the rural people but provided the Rhodesian security forces with the excuse to shoot down people in the rural areas. Galling incidents that included tying people on army trucks and then dragging them on the ground for long distances were commonplace. Parker described how the Rhodesian soldiers how an adult man was made to sit on the bonnet of the lead army truck in the war zone hoping that he would reveal sites on the dirt roads were landmines were planted[15]. It was commonplace that peasants had parts of their bodies like noses, ears and limps dismembered by members of the colonial armies especially the Rhodesian Selous Scouts. Stories abound of rural women who were also raped by members of the Rhodesian army. The death of Rhodesian soldiers after Rhodesian army tracks detonated landmines spelt danger to the people in the vicinity. They faced the wrath of Rhodesian forces' repression. They would be subjected to terror that included severe beatings, torture and destruction of their homes and property. In his autobiography, Godwin, a white Rhodesian who worked for the British South African Police decried the failure of the Rhodesian forces to forge good relations with the rural people. Instead they went berserk in an orgy of violence and burnt rural homes in Matabeleland.[16]

The many raids of pungwe gatherings that were carried out by the colonial regime forces regrettably left many civilians dead. In May 1978 in Gutu District Rhodesian forces attacked a pungwe gathering resulting in the death of over 150 civilians and just one Zimbabwe African National Liberation Army (ZANLA) guerrilla fighter.[17] The government forces were quite aware that their raids on pungwe meetings resulted in the death of innocent civilians. That they never exercised restraint was an index of their cruelty and the propensity to commit atrocities against the rural population. These attacks which did not discriminate between combatants and non-combatants were arbitrary and non-selective in nature. Every category of people in the rural communities that fell in the war zones became targets of the repressive violence of the Rhodesian government forces. Writing on terrorism in civil wars, Kalyvas observed that indiscriminate violence is targeted at individuals on the basis of their membership in a group perceived to be connected with the opposition irrespective of their individual actions.[18] In the Rhodesian scenario indiscriminate violence was motivated by the known fact that almost every if not all members of the rural societies provided logistical support to the liberation fighters. Kalyvas also holds that random violence is also prompted by information asymmetry between warring parties in a conflict.[19]

Due to lack of the support of the rural African population the Rhodesian security forces experienced dearth of information about guerrilla activities and guerrilla positions in the war zones. The liberation fighters, on the other hand, had access to intelligence which was willingly provided by the rural peasants. Frustration resulting from unavailability of information actuated the application of arbitrary violence by the Rhodesian army forces. The Rhodesian security forces were aware that rural communities were loyal and sympathetic to the liberation fighters but sometimes had no tangible evidence to incriminate them. The unfortunate propensity to apply indiscriminate repression was the result of this shortcoming. The Rhodesian security forces also used violent and desperate means that could not discriminate between combatants and non-combatants. These measures included contamination with poison of food and clothing that was destined for guerrilla fighters.[20] Unfortunately, the rural peasants also became victims of the poisoned clothing and food.

This was the nature of the reprisals that the Rhodesian security forces applied on the African people resident in the war zones. This kind of violence exposed the Rhodesian security forces to odium. The Rhodesian regime was wary of the work of the Catholic Commission for Justice and Peace (CCJP) during the war. The CCJP set about to investigate and publicise violence committed against the civilian population by the warring parties during the war. Bishop Donal Lamont, who was the chairman of the CCJP, faced the wrath of the Rhodesian government for publishing the atrocities they committed when they used force to relocate the peasants into ‘Protected Villages'. He was deported from the country on 23 March 1977.[21] Sister Janice McLaughlin, a Catholic nun, who also worked for the CCJP was also deported from Rhodesia for her stand against Rhodesian repressive violence against the rural African people. It was evident that the Rhodesian security forces deployed wanton violence against the civilian population in its unsuccessful attempt to crush the liberation movements.

The violence that the Rhodesian colonial forces perpetrated against the rural peasants was apparently systematic and organised. It is on this score that it should be appropriately labelled ‘terrorism' and it was the Rhodesian security forces that deserved to be called ‘terrorists'. The Rhodesian regime and its forces hoped that loyalty and sympathy of the peasants would be redefined if they used terror. Resulting from the proclivity of incumbent governments to attribute ills that are rooted internally, the Rhodesian regime justified their random violence in the war zones by intimating that they were fighting against communist-trained and inspired terrorists. They stubbornly refused to accept that the liberation war was not externally motivated but was largely a result of their unjust policies and practises. The Rhodesian regime recoiled from ever attempting to ‘win the hearts and minds' of the rural African population. Such a policy would have implied addressing grievances of the black population in Rhodesia. Officially these grievances did not exist. According to the Rhodesian government and the security force commanders, the way to eliminate terrorism was to kill ‘terrorists', deny them physical access to the black population and punish those who collaborated with them.[22]

Guerrilla ‘Violence for Freedom'

The perpetration of violence by the guerrilla movement against the rural population was no doubt an undeniable feature of the liberation war. However, pro-Rhodesian narratives of the war, which are unfriendly to the liberation fighters, have exaggerated the occurrence of incidents of and the character of guerrilla violence. The narratives have erroneously contended that guerrilla violence was part of the manner and method that the liberation movements employed to secure the co-operation of the rural population. Such narratives have given the impression that the liberation fighters applied violence against specific groups of the rural community. Kriger and Sachikonye suggest that chiefs, headmen, kraal heads, church leaders, shopkeepers and government agricultural demonstrators were obvious targets of guerrilla violence.[23]

Sachikonye makes the contention that: ‘There was also a great deal of violence exercised by guerrillas against collaborators of regime forces as well as against civilians amongst the African rural population'.[24] Sachikonye errs in making a distinction between collaborators and civilians. Collaborators definitely emerged from the civilian population in the rural areas. Villagers who participated in the war have revealed that sell outs or traitors (vatengesi) that collaborated with the Rhodesian army forces were from all categories of the rural population. The sub-scholarly literature produced by ex-Rhodesian servicemen has largely exaggerated guerrilla violence. Chris Lotter, a former Rhodesian soldier manifested this hyperbole when he wrote:

The terrorist
Is excused
His rape and frenzied pillage
May mutilate and burn
For freedom has no crime
Hear the muted agony
Of crippled men and boy [25]

Lotter gives the impression that the freedom fighters exercised violence that included rape, mutilation and cutting off the limps of the civilians. Reid-Daly, the commander of the Rhodesian Selous Scouts during the war, lamented lack of press mention of guerrilla atrocities. He pointed out that these included cases in which wives were forced to eat flesh cut from their murdered husbands' bodies, whole villages razed to the ground and all the villagers slaughtered or burnt to death while locked in their huts.[26] Parker writes that the liberation guerrilla fighters raped, murdered and ruthlessly brutalised the villagers to keep them living in fear.[27] These assertions found in narratives written by ex-Rhodesian servicemen were drawn from and were generally part of the propaganda of the Rhodesian regime. These narratives were not only serious exaggeration but largely untrue. The narrative that provided this hyperbole was also deficient in analysis and failed to realise that guerrilla violence was selective. The liberation fighters did not hesitate to execute and administer thorough beatings on members of the rural communities who sold out information about their activities to the Rhodesian security forces.

In my doctoral study I documented examples of collaborators who were executed by the liberation fighters around Morgenster and Bondolfi Missions.[28] I however indicated that these killings were not part of the programme of the freedom fighters. The nationalist fighters were at pains to avoid estranging themselves from the rural population. Executions were dictated by the need to survive since civilian collaboration with the colonial army forces put the lives of the freedom fighters and the peasants at risk. It was clear that guerrilla violence that visited the rural folk was discriminate. It was used against only those elements of the rural population, who against the express advice of the liberation forces collaborated with the Rhodesian security forces. It was possible that the liberation fighters executed innocent people who were incorrectly judged to be traitors. These were exceptions rather than the rule. The rural people easily avoided guerrilla violence by refraining from flirting with the Rhodesian security forces as per advice of the liberation fighters. It is significant to note that guerrilla violence during Zimbabwe war of liberation was effective because it was combined with an agenda to promote peasant interests. Moreover, the Zimbabwean nationalist guerrillas largely practised justice rather than vengeance when they applied violence against elements of the rural population. The application of selective violence by the freedom fighters induced the rural population to be loyal and avail resources to the nationalist freedom fighters. What made guerrilla violence selective? This was largely because the Zimbabwean liberation fighters were careful not to offend the rural people who were the bedrock of their survival by supplying them with intelligence, food and other necessary material. Again, the guerrilla fighters who were freedom fighters purported to be socialist and thus were guided by a moral vision of a better world, which precluded terrorist actions as inconsistent with such a vision.

Guerrilla violence was used in a highly controlled, ancillary and selective fashion within the overall plan of ideological and organisational restructuring in the war's theatre of operation. The liberation movement, especially the Zimbabwe African National Union (ZANU), and its armed wing, ZANLA, crafted a code of conduct that among other issues regulated the relations between the guerrillas and the peasants. The nature of guerrilla violence was influenced by these rules. Among these were the ‘Three Rules' and the ‘Eight Points for Attention.'[29] The code of conduct provided clear-cut censure procedures against commission of unwarranted atrocities by ZANLA forces. ZANLA regulations stipulated that the decision to execute collaborators or sell outs (vatengesi) was the prerogative of senior ZANLA field commanders from detachment leadership and above.[30] This ensured adherence to the process that had to be followed before any killing of such persons took place. The process entailed trials that constituted verification of the allegations that someone had ‘sold out' information which compromised the cause for freedom. It was these important and necessary trial sessions that anti-liberation literature has labelled ‘kangaroo courts' or ‘centres of miscarriages of justice'. Members of ZANLA's Military High Command, which was the supreme organ of the ZANLA guerrilla fighters, based at Chimoio during the last four years of the war, made frequent visits to the war font in colonial Rhodesia. These visits, among other objectives, had the intention of investigating and resolving guerrilla indiscipline which included unnecessary guerrilla violence. In keeping with principles of their revolutionary pursuit the liberation forces wanted to maintain moral superiority over the Rhodesian security forces. An ex-guerrilla fighter, Last Ndega, pointed out that liberation fighters endeavoured to depict that they were disciplined freedom fighters.[31] The ZANLA forces compiled reports of their activities at the war front. These reports were sent to the ZANLA military headquarters at Chimoio, in Mozambique. The exercise of writing reports was part of the training of ZANLA cadres. It was emphasised at training that ZANLA commanders had to compile accurate field reports which included activities like execution of individual enemy soldiers and collaborators. The compilation of reports precluded the liberation fighters from executing and deploying violence against innocent people in the war zones.

Conclusion

The foregoing discussion has shown that current attempts to equate and link the selective nature of violence that was deployed by the revolutionary guerrilla forces to contemporary outbreaks of violence are unfounded and devoid of academic analysis. The nonselective violence that is perpetrated by troops of an incumbent government is normally intended to stifle legitimate demand for economic and political spaces by the citizens. On the other hand the application of violence on civilians by the liberation fighters was in the interest of creating economic and political space. It would be fitting to refer to guerrilla violence as ‘freedom violence'. The rural people tolerated and accepted it because it was possible to avoid it and were nearly always in agreement to the reasons for deploying it. The Rhodesian colonial regime and its repressive military machinery failed to gain control of the civilian population. It terrorised, starved, butchered and destroyed the property of the rural people. The proper definition of such violence applied on civilians by the Rhodesian security forces would be ‘terrorism'. It was applied to defend a repugnant system and therefore backfired. There was no justification for the deployment of violence on rural people by the colonial forces of the incumbent Rhodesian government. It could not justify its continued hold to power when it failed to address the black people's demand for social justice and political self-assertion.

In its propaganda the Rhodesian colonial government deployed the rhetoric of ‘terrorism' whose goal was to de-legitimise the liberation movements' fight for independence. The colonial government also set about to criminalise the liberation war through its propaganda. These efforts failed to change the attitude of the black people whose hostility towards the white colonial regime intensified. The propaganda of the liberation fighters was effective and strengthened their bond with their fellow black population in the struggle for shaking off the manacle of the unjust colonial system.

References

Bhebe, N., ZAPU and ZANLA Guerrilla War and the Lutheran Church in Zimbabwe (Gweru: Mambo Press, 1999).

Author, ‘Zimbabwe's Liberation Struggle: A Critical Decade of the Zimbabwe African National Union (ZANU)'s Guerrilla War (PhD Thesis, Fort Hare University, 2011).

Godwin, G., Mukiwa: A White Boy in Africa (London: Macmillan, 1996).

Godwin, P., and Hancock, I., Rhodesians Never Die: The Impact of War and Political Change on White Rhodesia (Oxford: Oxford University Press, 1993).

Kalyvas, S., ‘The Paradox of Terrorism in Civil War', Journal of Ethics, 8 (2003), pp. 97-138.

Kriger, N., Zimbabwe's Guerrilla War: Peasant Voices (Cambridge: Cambridge University Press, 1992).

Lotter, C., Rhodesian Soldiers and Others who Fought (Alberton: Galago, 1984).

McLaughlin, J., On the Frontline: Catholic Missions in Zimbabwe's Liberation War (Harare: Baobab Books, 1996).

Moorcraft, P., Mugabe's War Machine (Johannesburg & Cape Town: Jonathan Ball Publishers, 2012).

Parker, J., Assignment Selous Scouts: Inside Story of a Rhodesian Special Branch Officer (Alberton: Galago, 2006).

Reid-Daly, R., Pamwe Chete: The Legend of the Selous Scouts (Weltervreden Park: Covos-Books, 1999).

Sachikonye, L., When a State Turns on its Citizens: Institutionalised Violence and Political Culture (Auckland Park: Jacana Media, 2011).

Sturges, P., ‘Information in the National Liberation Struggle: Developing a Model', Journal of Documentation, 60, 4 (2004), pp. 428-448.

Werbner, R. P., ‘In Memory: A Heritage of War in South-western Zimbabwe', in N. Bhebe & T. Ranger (eds.,), Society in Zimbabwe's Liberation War (London: James Currey, 1996).

Oral Interviews

Interview with Daniel Jerimani (ex-mujibha), Morgenster Mission, Masvingo, 10 July 2009.

Interview with Felicitas Muzembi, Morgenster Mission, Masvingo, 20 August 2009.

Interview with Alex Mataruse, Murambwi Village, Masvingo, 13 August 2009.

Interview with Last Ndega (ex-ZANLA guerrilla fighter), ZANU (PF) Headquarters, Harare, 19 January 2009.

End Notes

[1] P. Sturges, ‘Information in the National Liberation Struggle: Developing a Model', Journal of Documentation, 60, 4 (2004), p. 439.

[2] P. Moorcraft, Robert Mugabe's War Machine (Johannesburg & Cape Town: Jonathan Ball, 2012), p. 62.

[3] J. Parker, Assignment Selous Scouts: Inside Story of a Rhodesian Special Branch Officer (Alberton: Galago, 2006), p. 285.

[4] R. Reid-Daly, Pamwe Chete: The Legend of the Selous Scouts (Weltervreden Park: Covos-Books, 1999), p. 292.

[5] The Rhodesian Ministry of Information, Tourism and Immigration published a pamphlet in July 1978 in which the description of the murders is given.

[6] See P. Moorcraft, Mugabe's War Machine, p. 61.

[7] Parker, Assignment Selous Scouts, p. 187.

[8] Field commanders were obliged to compile accurate field reports. However, these internal reports took a new form when they became propaganda material. The losses of the nationalist guerrilla forces were left out.

[9] Interview with Daniel Jerimani (ex-mujibha), Morgenster Mission, Masvingo, 10 July 2009.

[10] All war zones were witness to such violence.

[11] R. P. Werbner, ‘In Memory: A Heritage of War in South-western Zimbabwe', in N. Bhebe & T. Ranger (eds.,), Society in Zimbabwe's Liberation War (London: James Currey, 1996), p. 197.

[12] N. Bhebe, ZAPU and ZANLA Guerrilla War and the Lutheran Church in Zimbabwe (Gweru: Mambo Press, 1999), p. 113.

[13] Interview with Felicitas Muzembi, Morgenster Mission, Masvingo, 20 August 2009.

[14] Interview with Alex Mataruse, Murambwi Village, Masvingo, 13 August 2009.

[15] Parker, Assignment Selous Scouts, p. 58.

[16] P. Godwin, Mukiwa: A White Boy in Africa (London: Macmillan, 1996), p. 302.

[17] J. McLaughlin, On the Frontline: Catholic Missions in Zimbabwe's Liberation War (Harare: Baobab Books, 1996), p. 196.

[18] S. Kalyvas, ‘The Paradox of Terrorism in Civil War', Journal of Ethics, 8 (2003), p. 101.

[19] Ibid, p. 101.

[20] Parker, Assignment Selous Scouts, p. 159.

[21] P. Godwin and I. Hancock, Rhodesians Never Die: The Impact of War and Political Change on White Rhodesia (Oxford: Oxford University Press, 1993), p. 186.

[22] P. Godwin and I. Hancock, Rhodesians Never Die, p. 100.

[23] N. Kriger, Zimbabwe's Guerrilla War: Peasant Voices (Cambridge: Cambridge University Press, 1992), p.104 and L. Sachikonye, When a State Turns on its Citizens: Institutionalised Violence and Political Culture (Auckland Park: Jacana Media, 2011), p. 9.

[24] Sachikonye, When a State Turns on its Citizens, p. 9

[25] C. Lotter, Rhodesian Soldiers and Others who Fought (Alberton: Galago, 1984), p. 67.

[26] Reid-Daly, Pamwe Chete, p. 292.

[27] Parker, Assignment Selous Scouts, p. 25.

[28] Author, ‘Zimbabwe's Liberation Struggle: A Critical Decade of the Zimbabwe African National Union (ZANU)'s Guerrilla War (PhD Thesis, Fort Hare University, 2011), pp. 154-155.

[29] The ‘Three Rules' and the ‘Eight Points for Attention' were regulations that ZANU adopted from Mao Tse-Tung's practice of revolution in China.

[30] From ZANLA war documents.

[31] Interview with Last Ndega (ex-ZANLA guerrilla fighter), ZANU (PF) Headquarters, Harare, 19 January 2009.

Table of Contents

Cyber Power in the Gulf

By Eneken Tikk-Ringas, International Institute for Strategic Studies, 05 December 2013

Cyber attacks – the ‘new normal’ in business, governance and conflict – are also becoming the norm in regional and international competition.

Tensions over Iranian nuclear aspirations, Assad’s regime struggle and clashes between Shia protesters and government forces in Bahrain all carry an online footprint. Cyber-capability development and deployment also reflect alliances, such as the ties between the Iranian regime and the Syrian Electronic Army, the links between GCHQ and NSA/Cyber Command – or common privacy concerns shared by Germany and Brazil in the wake of the revelations that leaders’ phones were bugged.

There is daily news of cyber attacks on government and industry radars across the globe, but the spectre of cyber conflict is particularly menacing in the Middle East. Gulf states find themselves in a turbulent cyber-security environment; witnessing cyber-weapon tests and home to inter-state and cyber proxy hostilities and to emerging military cyber powers.

In a recent study of ‘Olympic Games’ – a cyber campaign targeting Iran’s nuclear programme between 2007–2013 – the cyber-defence consultancy Langner concludes that the Islamic Republic was used as a testing ground for the sophisticated use of cyber weapons by a state actor. Through attacks against large oil companies in August 2012, the fallout from the operation encompassed Saudi Arabia and Qatar – trustees of the Syrian opposition.

Although Iran has made no secret of its ambition to control the regional security environment, its partnership with Syrian cyber groups supports the claim that Syria and Iran have used cyber capabilities to bolster each other's strategic aspirations.

In this volatile security environment, Gulf states seem to have little option but to fortify their own cyber defences along with air and missile defences.

But just as cyber activity reflects the region's conflicts, it is also aligned to the social and economic prospects of GCC countries. A cyber attack, as a short-term measure, is a combination of determination, plausible deniability and perhaps even only a moderate investment – but there is no shortcut to robust cyber defence. Carrying out a single attack is far simpler than effectively resisting, in the longer term, espionage, subversion and sabotage.

In a region with only an emerging cyber-security culture, cyber doctrines will not compensate for a lack of ICT production, sustainable talent in the field and awareness about IT security. Reliance on foreign-made devices and components (which can be easily compromised); dependence on foreign skills and competence in designing information systems; high ICT consumption and investment; opaque government and risk-management processes; and a less-developed culture of international and regional cooperation exposes the Gulf countries to economically-motivated cyber crime, and makes states in the region easy prey for local and international cyber attacks.

Moreover, the population's appetite for social media and smartphones and the deployment of state-of-the-art technologies and business models, coupled with only basic regulatory and policy regimes, contributes to the region's image as merely a 'buying' power.

Developing cyber security will present more of a challenge for the Gulf than is immediately apparent. The cyber element of strategic security is closely connected to economic and military power. Further, to have strong cyber defence, governments, companies and citizens must take equal responsible for online safety.

That said, there are some strategic shortcuts available. Instead of using manifold rewritten templates from other regions to create an information-savvy economy, and security policies and strategies, Gulf countries can take the best lessons from the European and American experiences. Applying lessons learned in the fields of telecoms and ISP regulation, consumer protection, data privacy, cyber crime and military cyber doctrine to the Gulf states' own particular concerns – as well as their advantages, such as social stability, economic continuity and strategic security – would allow the region to develop some form of common agility, cooperation and collective strategy.

The economic and political power of the region depends on common approaches to the development and use of ICT. Cyber strategies there should focus on security, rather than conflict.

Table of Contents

Inside the Ring: China targets Global Hawk drone

By Bill Gertz, Washington Times, 11 Dec 2013

China's military is planning to counter surveillance by the Pentagon's long-range Global Hawk drone, which currently is deployed on Guam and flying reconnaissance missions aimed at China.

According to a recent technical journal, China's military now has countermeasures for thwarting Global Hawk flights, saying the stealth drone is flown near China's southeast coast "continually" and thus "countermeasures against Global Hawk are considered."

Global Hawk missions are classified. But defense officials say they are worried the aircraft could become targets of China's military should its air forces try to enforce a newly established air defense identification zone over the East China Sea.

China has demanded that all aircraft entering the zone, which extends nearly 100 miles into the Pacific Ocean, file pre-flight routing plans.

The U.S. has said it does not recognize the zone, which encroaches on Japan's air zone over the Senkaku Islands.

Defense officials told Inside the Ring that one key reason for implementing the air zone was to stop U.S. military surveillance flights near China's coasts.

The report provides a detailed technical description of China's methods against Global Hawk flights, including electronic jamming of onboard spy equipment and aircraft-to-satellite signals used to remotely pilot the drones, electronic disruption of GPS signals used for navigation, and using airborne warning and control aircraft to detect the drone and guide warplanes to shoot them down.

Also, the report suggests using “smoke screens” to hide spying targets — a technique readily available in China, as dangerous levels of smog have blanketed many major cities in recent weeks.

The Chinese also are considering cyberattacks that would allow them to take over controls of Global Hawks and cause them to crash or forced to land, a technique the report suggests may have been used by Iran to down a secret RQ-170 stealth drone.

To unmask the drone’s low-radar signature, the Chinese also plan to use wide-spectrum and passive radar to locate and then direct aircraft to shoot down the drones.

“Regardless of whether it is a Global Hawk or an RQ-170 stealth [drone], it is afraid of seven things: electronics jamming; camouflage deception, being dazed by smoke screens; mid-air intercepts; airborne early warning; attack platforms and mid-air ambushes,” the report said. “If effective barrage jamming can be implemented by the opponent, then the operational effectiveness of the [drone] will be partially or totally lost.”

The Global Hawk is the Air Force’s premier long-range surveillance drone, with a range of 2,300 miles at an altitude of up to 60,000 feet. It is equipped with synthetic aperture radar, high-resolution cameras and signals intelligence equipment.

So far, an armed version has not been deployed, but the aircraft is capable of carrying up to 2,000 pounds.

The Navy version under development is called the MQ-4C Triton.

The report was published in February in the military journal “Aerospace Electronic Warfare,” a publication of the Institute 8511 of the China Aerospace Science and Industry Corp., China’s main missile manufacturer.

Table of Contents

Army Reserve Units Earn Top Places

By Capt. Addie Randolph, DVIDS, 19 Dec 2013

ADELPHI, Md. – Soldiers from the Army Reserve Information Operations Command earned first and third place amongst U.S. and International military teams in the 2013 Defense Cyber Crime Center Digital Forensic Challenge on Dec. 3, 2013.

The military category featured uniformed military and civil servants who work for Active Duty and Reserve Component military units.

The Army Reserve Information Operations Command based inside the Army Research Lab Adelphi, Md., entered two teams into the contest, the National Capital Region Information Operations Center, also based in Adelphi, and the Northeast Information Operations Center, based at Fort Devens, Mass.

"I am proud of what these teams accomplished. It is evidence of what great soldiers we have in the Army Reserve and of their exceptional technical capabilities in cyber defense," Col. Mark DiTrolio, ARIOC commander.

The NCRIOC submitted 34 digital forensics solutions during the 11-month competition and landed top honors out of 23 U.S. military teams. The NEIOC earned third place in the US military category.

The NCRIOC team “Carve This” also outscored all international military teams and placed 13th out of 317 worldwide teams among civilian, military, commercial, government, and academic categories. “The Victorizers” team representing NEIOC also scored ahead of all the international teams and placed 41st overall.

The DC3 Challenge provides digital artifacts comparable to what Soldiers might examine in a real-world cybersecurity situation. DC3 asked players to identify hidden files, perform analysis of suspicious network traffic, analyze registry entries and recover user passwords.

"I am proud of what these teams accomplished. It is evidence of what great soldiers we have in the Army Reserve and of their exceptional technical capabilities in cyber defense," said DiTrolio.

Chief Warrant Officer 2 Gary Cribbs led the team that included Sgt. 1st Class Al Williamson, Staff Sgt. Robin Brown and Maj. Mitch Wander, NCRIOC Forensics Mission Support Team leader.

Cribbs, an information services technician, provided leadership and guidance enabling the team to attempt solutions for all DC3 Challenge exercises from the basic to expert levels. DC3 identified the expert-level challenges as having “no known solution.”

“As soldiers, we prepare to deal with unexpected situations,” said Cribbs. “We train on a variety of digital media analysis tools and techniques in order to prepare for a broad range of mission requirements. The DC3 Challenge exercised our capability to solve forensic problems all over the map.”

The NCRIOC commander said he immediately saw the value of the challenge. “The Army expects our soldiers to be experts in cybersecurity, combining civilian-acquired skills with challenging, realistic training,” said Lt. Col. Michael Smith, NCRIOC commander. "Participating in the DC3 Challenge leveraged the technical expertise and creative problem solving that our soldiers apply to stateside and deployed missions.”

“The Victorizers” didn’t exist more than a year ago, so they have achieved great success in the DC3 Challenge over a short amount of time. We are very proud of them at the NEIOC,” said Lt Col. John McKee, NEIOC commander. “What’s more important here is the exposure to other teams and methodologies, both military and civilian. In cyberspace it will be this type of cross-pollination of experience and partnerships with academia and industry that will cultivate the cyber security experts the Army needs.”

Each Information Operations Center under the ARIOC is comprised of several teams with training in incident handling, computer network defense and other cybersecurity capabilities. The NCRIOC, NEIOC and three related units comprise the ARIOC. The ARIOC is part of the 76th Operational Response Command, based in Utah.

“I'm so proud of our "Carve This" and “The Victorizers” teams of Soldiers. Their devotion to their craft and willingness to work hard paid off in a spectacular showing,” said Maj. Gen. Daniel L. York, commanding general of the 76th Operational Response Command

Table of Contents

SOCOM Web Initiative on Senate Chopping Block

By Howard Altman, Tampa Tribune, December 8,

On any given day, the Al-Shorfa.com website contains dozens of stories about events in the Middle East, on topics ranging from the death toll in the Syria civil war to Tunisian women being recruited for a “sex jihad” to efforts by the government of Yemen to create a youth peace conference.

The site is part of a network of 10 websites, coordinated through an office in Tampa, that reaches millions around the world each month, providing news and information to people in hard to reach areas.

For this network, the bottom line isn't garnering advertising dollars, but changing attitudes.

Managed by U.S. Special Operations Command, the Trans Regional Web Initiative websites are operated by the Geographic Combatant Commands, who also coordinate with the State Department. They offer an alternative message to the ideology spread by al-Qaida, the Taliban and other violent extremist organizations in the cyber battlespace, say those who run the program.

“This is a cost-effective, synchronized counter-terrorism messaging effort,” says Roger Smith, the TRWI program manager, speaking in a conference room at Socom's headquarters at MacDill Air Force Base. In October, the initiative had nearly four million article reads and just under two million unique visitors. In the online world, where extremists spread their messages, gather recruits and raise money, the initiative is helping “change the narrative,” says Smith.

But the six-year-old program, criticized by some as an expensive propaganda tool for the military, is on the chopping block.

In its $620 billion defense budget bill, the Senate Armed Services Committee — including Florida Sen. Bill Nelson — voted to transfer the nearly $20 million requested to run the TRWI next year to other military support operations at Socom.

At a time when the Pentagon is looking at a potential trillion dollar spending cut over the next decade, the committee's report said that “the costs to operate the websites developed under the TRWI are excessive. The effectiveness of the websites is questionable and the performance metrics do not justify the expense.”

A classified April report by the Government Accountability Office offered other concerns, saying that the initiative “does not include country teams and is not well coordinated with other” military information support operations programs.

Despite these bleak assessments, the initiative has a fan in a high place.

President Barack Obama's administration last month issued a statement asking that money for the program be restored, calling TRWI “the only synchronized online influence effort able to challenge the spread of extremist ideology and propaganda on the Web.”

Last month, Socom issued a solicitation seeking to renew the initiative, which has been run for the past five years by General Dynamics Information Technology. But whether the command will be allowed to pursue a new contract won't be known until Congress votes on the next defense budget. The Senate is scheduled to reconvene tomorrow.

The Trans Regional Web Initiative is a small part of a larger Pentagon effort to influence foreign audiences called Military Information Support Operations. Formally known as psychological operations, MISO “are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives,” according to a 2011 Pentagon report outlining how MISO should work.

Socom leads the development, coordination, and integration of MISO capability across the Department of Defense, according to the report.

The concept for TRWI dates to 1999, says Smith, when U.S. European Command wanted to get its message into Serbia to counter the government of genocidal strongman Slobodan Milosevic.

“They set up a website that aggregated news in an attempt to expose the Serbian population to what the rest of the world was saying,” says Smith.

The website, Southeast European Times, still exists.

In 2004, Eucom teamed with Socom to create a counter-terror website focused on North Africa, where “a huge flow of foreign fighters was coming out of Morocco and Tunisia into Iraq,” says Smith. “That flow is still going into Syria.”

At the time, military leaders saw that if there were similar sites, with “common thematics and messaging, that take advantage of al-Qaida miscues, like, oops, we beheaded the wrong guy, you can truly begin to undermine some of that support,” says Smith, who wrote the initial TRWI concept in 2005 while he was still in the Army.

Al-Shorfa, Arabic for “the balcony,” came online in 2008.

The websites are presented in local languages with identical copy in English, says Smith, using British spelling and language “just to make sure that it is understood there is no intent to ever target American citizens or American readers,” says Smith.

Each one has a disclaimer announcing who runs it.

“Al-Shorfa.com is a web site sponsored by USCENTCOM to highlight movement toward greater regional stability both through bilateral and multilateral cooperative arrangements,” according to the site's “About” section. Content is provided by paid stringers indigenous to the areas they cover, says Smith. They report directly to the contractor.

“We don't want a guy getting editing assignments in Iraq from a major at Centcom,” says Smith. “We feel we would put their life at great harm by doing that. We try not to put a military linkage down to the stringer.”

In the case of Al-Shorfa and other TRWI sites in the CENTCOM region, officials at the command have frequent, daily communication managing all aspects of website operations, including coordinated editorial guidance.

Those Centcom officials also conduct frequent coordination with other offices in the command, like the public affairs office and the country desk officers, and with external agencies like the State Department's Bureau of Near Eastern Affairs, says Smith.

Not surprisingly, there are tight limits on what gets published.

Information about the situation in Syria, for instance, has strict parameters according to Centcom. Like all information on TRWI sites, it is from an allied, not U.S. perspective.

Al-Shorfa provides hard news coverage of developments on Arab League and U.N. positions on events in Syria, points out the dangers of sectarian rhetoric, outside sources exploiting the revolution, and extremists scaring off international community,

The site also encourages humanitarian efforts and takes a position that political transition in Syria should be led by the Syrian people and supported by the international community.

Two years ago, a scathing story in the journal Foreign Policy blasted the initiative for “whitewashing” abuses by the Uzbek government, a close ally that the military increasingly relies upon for transportation with the ongoing troop withdrawal from Afghanistan.

“It is not Centcom's mission to be the human rights watch,” Smith says when asked about criticism of the Central Asia Online site. “We talk about roles and missions here. This is a counter-terror website.”

Smith acknowledges that MISO efforts could become ineffective if the intended audience dismisses the sites. In doing so, he also addresses a critique of the GAO report about the coordination with the State Department. A portion of the report is available at cryptome.org, an anti-secrecy website. GAO officials confirmed that they produced a classified report but would not comment on its contents.

“We are very much concerned,” he says of the message being blunted. “That's why we coordinate very closely with the (State Department's) Bureau of Near East Affairs. That coordination is very, very intense. Ultimately, this defaults to the State Department because that is U.S. government policy.”

The State Department, says Smith, has the ultimate say in those matters.

“If the State Department says do not cover, or do not cover in this manner, then the combatant commands comply.”

Smith says TRWI's costs are not excessive and that there are metrics to support success.

”The average cost per article read is 51 cents,” says Smith. In addition, about 400 to 500 articles a month are reposted on other websites, some considered unfriendly to U.S. and allied interests, says Smith.

Another measure of success, says Smith, is that readers provided just under a half million words a month in comments across the enterprise, helping engage the audience and sparking debates.

Comprehensive reader surveys developed by Socom social scientists show that the sites are having an effect, says Smith.

More than half the readers responding to a survey about Al-Shorfa “said something they read on the website changed their attitude or perception about a particular topic,” says Smith. And 83 percent “said something they read on the website increased their knowledge and awareness of a topic.”

There also is anecdotal evidence, Smith says.

Information on the sites has caused jihadi leaders to argue among themselves, says Smith.

“They were saying, 'look, I am telling you, this extreme violence is not helping our cause,'” says Smith. “They were debating and arguing with each other. If we can get supporters questioning what and why and how they are doing things, then we are having an effect that is very, very difficult — particularly in places where we do not have anybody on the ground — to obtain.”

Nelson, who said there was no discussion about TRWI in the Senate Armed Services Committee, says he supports efforts by the military to provide facts.

“It seems to me the truth is what ought to be put out to foreign countries if they not getting the truth,” says Nelson,

In its letter to the committee, the White House said the Pentagon already “addressed many of the concerns raised in the Committee report by demonstrating that the TRWI is the most cost-effective means for reaching audiences which affect achievement of” military objectives.

The elimination of funding for TRWI would force the Department of Defense and Socom, responsible for synchronizing planning of global operations against terrorist networks, to withdraw from an important battlespace, says Smith.

“You start ceding aspects of the web to the adversary,” says Smith. “You are not there overtly challenging their message.”

Table of Contents