Information Operations Newsletter

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

ARSTRAT IO Newsletter Online

Table of Contents

Vol. 14, no. 02 (January –February 2014)

Psychological Warfare Meets Hallmark: Colombia's Christmas Ads Target Guerrillas

By Jim Wyss, Miami Herald, Dec. 24, 2013

BOGOTA -- BOGOTA-During Colombia's 50-year civil conflict with armed guerrillas, the military has developed a powerful weapon: Christmas.

For the last four years, the Ministry of Defense, in conjunction with the Lowe SSP3 ad agency, has rolled out holiday campaigns to encourage rebels to defect at a time when they're homesick and vulnerable.

It's psychological warfare with a Hallmark twist.

In 2010, when the campaign was first launched, commandos put Christmas trees deep in the heart of guerrilla territory, complete with lights and a message: "If Christmas can make it into the jungle, you can make it home."

Defections jumped 30 percent that year versus the previous December - although there's no evidence that the uptick was directly related to the ploy.

"Our campaigns are based on the same basic insight - even if you are an armed guerrilla living in the jungle, you're human, with dreams and desires," said Juan Pablo Garcia, who manages the Ministry of Defense account with Lowe SSP3. "And the holidays are a time when you're most homesick and alone."

These are unique times in Colombia. The government and the country's largest guerrilla group, the Revolutionary Armed Forces of Colombia, or FARC, have been holding meetings in Havana for more than a year trying to hammer out a peace deal.

They've gotten through two of the six points on the peace agenda - land reform and the guerrillas' political future - and are discussing ways the FARC can exit the drug-trafficking business.

President Juan Manuel Santos says similar negotiations could begin soon with the country's second-largest group, the National Liberation Army.

Many in this once war-torn country are hopeful that a lasting peace might be in the works. Even so, the government is maintaining military pressure on the guerrillas and defections are still taking place.

From January through October, 1,064 guerrillas abandoned the ranks, according to government figures. Minister of Defense Juan Carlos Pinzon says more than 100 more have put down their arms since then and that defections are up 19 percent versus 2012.

Each year the Christmas campaign gets tweaked amid the shifting reality of the conflict.

In 2010 and 2011, when the majority of the guerrillas were thought to be in isolated rural areas, the military took the message to them.

The year after the Christmas tree stunt, Lowe SSP3 created a campaign called Rivers of Light in which family members put messages and small gifts in 7,000 LED-illuminated capsules sent floating down rivers the guerrillas were known to frequent.

That campaign won prestigious awards and the trade journal Ad Age named Lowe the 2013 International Ad Agency of the Year.

Last year, amid military intelligence reports that the FARC was moving troops around to keep them disoriented and to discourage them from defecting over the holidays, the agency created Operation Bethlehem - setting up searchlights in small villages.

"It was like a beacon so that they would know where to go to turn themselves in," Garcia explained.

This year's campaign is equal parts Madison Avenue and guerrilla-marketing.

The FARC recently declared a 30-day unilateral ceasefire that runs through Jan. 15. That means that guerrilla soldiers will likely spend more time in populated areas, blending in with civilians and exposed to traditional media, the agency said.

Working with the mothers of recruits, the company has blown up baby photos of rebel fighters and emblazoned them with the message: "Before you were a guerrilla you were my child - This Christmas I'll wait for you at home."

Those posters are being plastered on village walls and hung in the jungle. At the same time, the campaign includes television spots and a web page, featuring real mothers.

"There's nothing more powerful than a message from a mother," Garcia explained.

Francisco, who joined the FARC when he was 15 and spent almost two decades with the group before defecting earlier this year, said the holidays are particularly trying for guerrillas, many of whom are young.

"When you're in the hills all you can think about is how much fun your family and friends might be having," said Francisco, who asked for anonymity to minimize the threat of FARC reprisals since defection is a capital crime. "And you feel like you're just up there waiting for a bomb to drop on you."

While he was never directly exposed to any of the Lowe SSP3 campaigns, he met others who had seen him.

"Yes they're effective," he said of the ads. "When you're in the mountains you get obsessed with your loved ones this time of the year. There's a lot of psychological pressure."

As he rolled out the latest ad campaign in the guerrilla stronghold of San Vicente de Caguan in central Colombia, Minister of Defense Pinzan said it was a simple call to reunite with family.

"Come home now, come home for this Christmas," he told guerrillas who might be listening to the local media. "It makes no sense for you to be out there...Start your life now; there's no need to wait for negotiations."

Like all good ad agencies, Garcia and his team run focus groups with ex-guerrillas to see what works. Through those meetings they know, for example, that the Christmas tree campaign "created a lot of buzz in the guerrilla rumor mill."

But despite their cutting-edge delivery, Garcia said the message is as traditional as the holiday.

"During Christmas anything is possible," he said, echoing a line from the campaign. "It's a time when everyone believes that change is truly possible. That's not just for guerrillas. That's for everyone."

Table of Contents

Pentagon's Cyber Arm Poised to Expand Role

By Tony Romm, Politico, 24 Dec 2013

The U.S. military's Cyber Command is about to receive the digital equivalent of faster ships and stronger missiles — but the force, only a few years in the making, is still grappling with how far it can go in fighting adversaries in cyberspace.

As part of the defense policy bill that just passed Congress, the Pentagon's many cybersecurity initiatives together secured billions of dollars in funding as well as new resources to help train Cyber Command's programmers and prepare them to operate on the emerging digital battlefield.

But the infusion comes as CyberCom, as it's known, is still working out its fundamental rules of engagement, including thorny questions as to when it can strike back at hackers and whether it can act without getting approval from the president. It's also struggling to find and train the talent it needs to carry out its mission, partly because of Pentagon budget pressures.

And CyberCom has become ensnared in the debate over National Security Agency surveillance sparked by Edward Snowden's leaks. The cyber force shares a director and headquarters with the controversial spy agency — and some in Congress want to look at splitting the two operations.

It all points to growing pains — and more scrutiny — as CyberCom takes on a larger role in protecting the U.S. from attacks. Started chiefly to protect the Department of Defense's own networks, the organization has morphed into an operation that seeks a much broader mandate to confront digital spies and hackers.

The command's goal is to be "highly standardized, highly skilled, competent across the spectrum of conflict — high bars to prove the individual, the team, the force are trained and ready. Never been done before in cyber, but absolutely necessary," said Maj. Gen. Brett Williams, director of operations with CyberCom, during a rare interview at its headquarters in Fort Meade, Md.

Cyber Command became fully operational in November 2010 after years of lobbying by Pentagon brass, and Gen. Keith Alexander has held its reins from the start. Defense leaders early on stressed that CyberCom's role was to defend military networks "already under attack" and emphasized the goal wasn't a "militarization" of cyberspace. But the operation has since grown in size and scope to meet new threats emerging in China, Iran and beyond. Now, CyberCom boasts offensive and defensive teams and runs regular exercises to prepare for worst-case scenarios. And as it bulks up, Congress is working to give it additional tools.

For example, the annual defense bill — approved last week by the Senate after earlier passing the House — included a litany of initiatives that will benefit CyberCom, including $68 million for some of the operation's classified activities, more than $14 million for Air Force offensive cybersecurity work and a series of programs that could augment DOD's ability to strike in cyberspace.

There's $33 million set aside to help map the Internet, an effort that could allow CyberCom to better target digital foes. A project called Plan X under the military's research hub, the Defense Advanced Research Projects Agency — aimed at making cyber weaponry easier to deploy in the field — is getting a $2.5 million increase to speed up development. And CyberCom would get the nod to upgrade so-called cyber ranges, which essentially serve as private arenas for the military to train new cyber workers and test out its offensive strategies in secret.

While lawmakers look to add to CyberCom's arsenal, however, the organization is still weighing with the White House how — and under what circumstances — it can use the tools. Much of the debate revolves around what constitutes a defense, and whether the force can strike back — or strike first — at enemies who want to do the U.S. harm. Pentagon officials and the administration have been working for years on questions about when, if ever, CyberCom can act outside U.S. military networks without seeking the president's permission.

Senior defense sources tell POLITICO they envision a hardened set of cyber rules someday that would let the military make quick decisions without going to the White House — like those that allow DOD to approve a fighter pilot shooting down a suspicious aircraft that intrudes on sensitive airspace. But those sources concede CyberCom isn't there yet.

"I think there's been a three-year debate that's largely over how to do this, how the military will use cyber techniques," said Jim Lewis, senior fellow at the Center for Strategic and International Studies in Washington. A presidential directive issued in 2012 does set the outer bounds for what CyberCom can do, but the details remain murky. The public, Lewis said, would benefit from a more "open discussion" of cyber weapons, much like the one the country has had on nuclear weapons.

Recent events have brought questions about CyberCom's role into finer focus. As denial-of-service attacks incapacitated the websites of top U.S. banks earlier this year, Alexander pushed — but failed to win support — for a plan to take out the hackers' servers, The Washington Post reported. And the 2010 Stuxnet computer worm that targeted an Iranian nuclear facility — a worm developed by the U.S. and Israel, according to The New York Times — has raised broader questions about the U.S. government's use of cyberweapons.

During his tenure, Alexander has been a frequent presence on Capitol Hill, lobbying for legislation to aid CyberCom's work. He's asked Congress, for example, to protect companies from lawsuits in the event they act on government information to fight hackers, POLITICO first reported. The idea, however, has raised red flags among civil liberties groups that don't want to immunize businesses from litigation if they fail to properly shield consumer data from attacks.

Meanwhile, CyberCom continues to struggle with a more basic challenge — how to meet its own staffing targets.

Alexander, testifying before Congress earlier this year, announced a major reorganization that divided the Pentagon's cybersecurity units into three distinct forces focused on defending DOD networks, assisting commanders and responding to specific threats. The general's plan envisioned more than a hundred principal and support teams, bolstered by thousands of cyber warriors.

Finding and training those troops, though, has not been easy. "We are on the right track but are not where we projected to be at this point; we knew we set an aggressive schedule," said Maj. Gen. Williams. CyberCom is "currently at 50-60 percent of our goals for 2013 and will continue to close the gap in the coming year," he said.

"Outliers like the sequestration, furloughs and overall budget pressure make this force build even more difficult," Williams said. "We had to shut down our training programs for this summer and fall, impacting us significantly."

Now the organization is looking at a future without Alexander. Initially, his departure plans prompted the Obama administration to look at whether to split the military's cyber arm from the NSA, and the president's task force on surveillance reform recommended a divorce. But the White House announced it intended to preserve the existing relationship, arguing it's proven effective at addressing cyber threats.

Congress, however, remains torn on the issue. An early draft of the defense authorization bill included plans to study a division of NSA and CyberCom, but that provision was later dropped. Some lawmakers have said they don't want to make changes that would hamstring CyberCom's work. Still, other members of Congress are pushing for civilian leadership at the NSA as part of a broader surveillance reform — a change would likely result in a separation from the Pentagon-led cyber force.

In many ways, the command is still finding its place in the massive military bureaucracy. As part of the defense bill, Congress authorized a new "interdepartmental team" led by the defense secretary's office to

reorient the military on offensive cyber operations, and it directed the Pentagon to create a “deterrence policy” for cyber adversaries.

So far, lawmakers haven’t touched a bigger debate: whether CyberCom should become its own unified command, like Special Operations Command. Lawmakers for now only want to study such a move as they keep closer watch over the organization’s growth.

“This was a realm that literally didn’t exist a generation ago,” explained Peter Singer, director of the Center for 21st Century Security and Intelligence at The Brookings Institution. “By any kind of measure, cyberspace has become a crucial battleground … [and] the spending, of course, has skyrocketed.”

Table of Contents

PLA Considers Setting Up Joint Command for Era Of Modern Warfare

By Teddy Ng, South China Morning Post, 03 January 2014

The People's Liberation Army is considering establishing a joint operational command to improve co-ordination between its different parts.

The Ministry of National Defence said the reform was necessary for electronic and information warfare and was a common trend around the world.

A ministry statement said that after studying the issue it would "deepen reform at an opportune time, creating a path of reform for a joint operational command system with Chinese characteristics".

The news comes after a Communist Party plenum in November said the PLA should improve co-ordination geographically and between its different military branches.

The defence ministry's statement did not give a timeframe for the reform, nor specific details of the future structure. The Japanese Yomiuri newspaper reported this week that China was planning to cut the number of military area commands from seven to five.

Citing anonymous senior military officials, the report said each of the five areas would have a joint operations command for ground, naval and air forces, and the strategic missile corps.

The report said that, of the existing military regions, Jinan, Nanjing and Guangzhou would set up new joint commands to oversee the Yellow Sea, East China Sea and South China Sea within five years.

Military observers said the reform was necessary because security threats were shifting to the ocean as the nation was involved in bitter territorial disputes in the East and South China Seas. These created challenges for the current seven military regions, which traditionally focused on ground-based army units.

The different branches of the military also remained highly independent of each other, making centralised control and joint combat efforts difficult.

"The commanders may not have sufficient authority to mobilise the navy and air force," said Beijing-based military affairs commentator Yue Gang. "But nowadays, security challenges are not only ground-based, and the role of the navy and air force will be more prominent."

Yue said the reform indicated more authority would be delegated to the regional commands, while the supreme military policy-making Central Military Commission, headed by party chief Xi Jinping , would focus on setting broad strategies, including those for the use of aircraft carriers.

Discussions on military structural reform have been going on for years, but no significant progress has been made.

"It indicates Xi has consolidated authority over the military and can exercise more control, after tackling other domestic issues, such as corruption," said Ni Lexiong, director of the Sea Power and Defence Policy Research Institute at the Shanghai University of Political Science and Law. But observers said completing the reform would take a long time because it would affect the vested interests of different factions within the military.

Table of Contents

DoD Hones Skills with Cyber Flag Exercise

Published January 06 2014, FedWeek

DoD announced it recently carried out a successful 11-day Cyber Command exercise at Nellis Air Force Base in Nevada, bringing together cyber professionals from across the department to test their knowledge and skills against a foe on a closed network. The third annual Cyber Flag exercise included joint, combined and interagency forces that worked together to hone offensive and defensive skills across a range of operations. According to DoD, forces applied new and developing tactics, techniques, and procedures to help cyberspace

operators to rapidly detect, assess, mitigate, and respond in real time to cyber threats to DoD networks. DoD said Cyber Flag this year is the first time all components of the cyber mission force construct such as the Defense Information Systems Agency, as well as a Joint Force Cyber Headquarters element and various tactical teams, exercised as a cohesive force. The cyber mission force is being built over a three-year period and aims to produce national mission teams to detect and monitor foreign adversary cyber activity, and blockand defeat attacks; combat mission teams to support combatant commander priorities and missions; and cyber protection teams to defend DoD information networks and improve network security, according to DoD. It said Cyber Flag also challenged command and control mechanisms to both employ and support simulated capabilities from the air and maritime domains. NASA Extends IT Contract at Johnson Space Center NASA has announced it will exercise an option to extend its contract with DB Consulting Group, Inc., in Silver Spring, Md., for IT, multimedia, information management and external relations support services at the agency's Johnson Space Center in Houston. The value of the $50.5 million contract increases to $201.4 million from a base value of $150.9 million. NASA said Johnson's Information Resources Directorate and the Office of External Relations would manage services provided under the contract for the most part. Those are to include operation and maintenance of primary IT services, graphics, library management, imagery acquisition, processing and cataloguing, television systems support for human spaceflight missions, public affairs services, and education program support.

Table of Contents

General: Strategic Military Satellites Vulnerable to Attack in Future Space War

By Bill Gertz, Washington Free Beacon, 08 Jan 2014

U.S. strategic military satellites are vulnerable to attack in a future space war and the Pentagon is considering a major shift to smaller satellites in response, the commander of the Air Force Space Command said Tuesday.

Gen. William Shelton said in a speech that China currently has a missile that can destroy U.S. satellites and warned that the threat of both space weapons and high-speed orbiting debris is growing.

The threat of attack to large communications and intelligence satellites is prompting a major study on whether to diversify the current satellite arsenal of scores of orbiters.

The four-star general also said he is wary of the United States joining an international code of conduct for space, an initiative promoted by former Secretary of State Hillary Clinton. The code likely would constrain the United States' freedom of action in the increasingly contested realm of space, he said during remarks at George Washington University.

Over the past several decades, satellites have revolutionized war fighting and caused a shift in the character of military forces from large ground armies to forces that emphasize agility and speed.

Shelton said the United States' highest priority military satellites are those that provide survivable communications and missile warning. Current systems cost about $1 billion each.

If any of these critical satellites are attacked and destroyed in a conflict or crisis, the loss "would create a huge hole in our capability" to conduct modern, high-tech warfare, Shelton said.

"Space has become contested in all orbits, where we face a host of man-made threats that may deny, degrade, or disrupt our capabilities," Shelton said, noting electronic jamming, laser attacks and "direct attack weapons," which are all systems being developed by China's military.

Jamming satellites is "a cheap and effective way of blocking our signals from space" and lasers "can blind our imaging systems, and in the future, they could prove destructive to our satellites," he said.

"Direct attack weapons, like the Chinese anti-satellite system, can destroy our space systems," Shelton said.

China's successful landing of a robot rover on the moon last month revealed "an aggressive Chinese space program," Shelton said.

China is also building anti-satellite weapons that range from ground-launched missiles that destroy orbiting satellites, ground-based lasers, electronic jammers, and cyber attacks, according to defense officials.

The latest annual report of the congressional U.S.-China Economic and Security Review Commission stated that China recently conducted a test of a high-earth orbit anti-satellite missile.

The test signaled "China's intent to develop an [anti-satellite] capability to target satellites in an altitude range that includes U.S. Global Positioning System (GPS) and many U.S. military and intelligence satellites," the report said. The Free Beacon first reported the test.

Defense officials also disclosed in January 2013 that China launched three small maneuvering satellites as part of its ASAT program, including one with a robotic arm that can be used to capture or destroy orbiting satellites.

Shelton said he favors better communication with the Chinese military on its space warfare efforts and that recent exchanges are encouraging and could avert a future military "miscalculation" in space.

"Miscalculation is one of the biggest threats we face," he said.

China has repeatedly rebuffed U.S. government efforts to engage in discussions on space weapons and warfare, among the Chinese military's most secret programs.

"Like the old Billy Joel song says, we didn't start the fire, but we're certainly in it, and it would be irresponsible for us, irresponsible at a minimum, not to protect ourselves," he said.

To better protect satellites in a future conflict, the military is currently studying new ways of replacing or restructuring satellite systems, along with better methods to dissuade and deter enemies from attacking them.

The policy of loading large satellites with numerous types of sensors and missions worked well in the past. But in the new contested space environment, a new strategy and architecture are needed, Shelton said.

One new strategy advocated by the general calls for "architectural alternatives" that are currently being studied by both military and industry.

The new focus calls for shifting away from large, multiple-payload satellites in favor of a larger number of smaller and simpler systems, which would be less expensive and conform to the currently tight defense budgets.

"By distributing our space payloads across multiple satellite platforms, we increase our resiliency to the cheap shot or premature failure," Shelton said. "At a minimum, it complicates our adversaries' targeting calculus."

A new system of "disaggregation" also calls for new satellite operating methods. In one recent experiment, the military equipped commercial communications satellites with a missile-warning sensor. Shelton said the test was "very successful."

Bureaucratic opposition in government and industry to a smaller, diversified satellite structure can be expected.

But Shelton warned: "Now, I'm not a fan of waiting for a catastrophe to propel change. The signs of a radically different space environment are all there. We just have to pay attention to them."

America's enemies have been studying U.S. war fighting efforts in the past several decades and are "going to school on us," Shelton said, specifically the revolutionary way the U.S. military uses satellites to integrate information assets in combat.

He compared the current threat of space warfare to the beginning of the space flight age in the 1960s.

"Just as the start of space flight signaled a fundamental shift in military operations, in my mind, so does this new era of challenging another nation's space assets," he said. "Sad, but true, in every medium, mankind has found a way to make it a medium of conflict. Land, sea, undersea, air and now space and cyber."

The growing threats to space, now crowded with around 1,000 active satellites and 23,000 pieces of space debris, has increased the need for closer space intelligence and surveillance, currently based on radar and optical sensors at ground stations around the world and a dedicated satellites orbiting 23,000 miles in space to track things in high-earth orbit.

"Keeping a constant eye on space and the activity that's going on there is vital to our national security," Shelton said, noting over 60 nations have a financial stake in at least one satellite and 11 countries have space launch capabilities.

Shelton said all nations have a right to access space but U.S. policy calls for opposition to "aggressive behavior and debris creation."

"We believe in freedom of navigation and freedom of maneuver and we will constantly work to maintain both," he said.

On the space code of conduct, Shelton said he favors the concept but is concerned that an international accord would "unnecessarily constrain us."

"We believe in freedom of action and freedom of maneuver in space," he said. "If we have gotten to the place with a code of conduct that it ties our hands in some way with what we need to do to accomplish national security objectives, I think that's problematic."

Also, verifying a space agreement would require honest participants, he said.

The Obama administration announced in 2012 that it was considering joining the European Union in formal talks on the code, which has been promoted by Russia and China.

The Pentagon's Joint Staff in an assessment of the code of conduct warned at that time it would constrain U.S. military operations in space.

"Just simple calculation: My search volume, if you will, of what I'm responsible for protecting is 73 trillion cubic miles, geosynchronous orbit to the surface of the earth. Think about trying to monitor the activity in that vast space and making sure nobody's doing anything to violate either that code of conduct or the treaty or whatever it is you've come up with in terms of an international agreement," Shelton said.

"We have to think this through, and I guess I put myself in the realist class instead of the idealist class," he said. "And if it doesn't have reality to it, I'm not sure it's got a whole lot of value."

On deterring space warfare and dissuading states from waging it, Shelton said both subjects are a concern.

"How does the United States deter activity against its space capability? How does it dissuade nefarious actions in space? How does it dissuade people even building systems that provide that capability to potential adversaries?"

"To me that is a tremendous challenge because if you look at traditional deterrence theory and try to apply that to space, part of it works, but a big part of it doesn't work at all."

Developing the most powerful U.S. space weapons to deter adversaries may not be useful for deterrence and dissuasion, he said.

Nuclear war deterrence theory during the Cold War would be very different when applied to both the space and cyber domains, Shelton said.

China military affairs expert Richard Fisher said Shelton's emphasis on "disaggregation" of strategic satellites relies on passive defenses. China, on the other hand, is building active, offensive space warfare capabilities.

"The United States also needs to develop its own active military space systems to deter China," Fisher said. "The U.S.needs multiple anti-satellite systems, that can be launched from ground, naval, and air platforms."

To counter any U.S. attempts to make strategic satellites more resilient, China is investing in micro and ultra-small satellites, Fisher said, noting that China's entire space program is run by the People's Liberation Army.

Table of Contents

Rebooting Country Studies

By Anna Simons, War on the Rocks, December 31, 2013

For all the talk about "big data," what about deep understanding? Surely in the wake of Iraq and Afghanistan—and faced with other conflicts burbling all over the place—some enterprising office in the Department of Defense or Department of State is busy re-conceptualizing the nature of what constitutes a good country study for those deploying abroad in the 21st century. And surely that office is being run by individuals with ample experience both in non-Western countries and with the U.S. military. Right?

I ask because the field grade officers I know and teach at the Naval Postgraduate School need more than just data (facts), information (assemblages of facts), and knowledge (cumulative information). Until the pendulum swings back and Congress proves willing to issue declarations of war in circumstances that permit no-holds-barred fighting, the military will continue to be asked to act with finesse. Yet, one problem with finesse is that it requires more than just being able to populate databases with names, dates, and information about who's connected to whom. Data, information, and knowledge certainly matter. But, what they can't do—ever—is make what others do make sense. They can't explain how others perceive events, conditions, their predicament, or you.

Meanwhile, there are two ways to gain a sense of what makes others tick. You can either acquire understanding experientially, which is sometimes hard to come by. Alternatively, you can acquire understanding second-hand. In a perfect world, both methods should be iterative. Arguably, great drama—and television series, like The Wire—can help convey a "sense of" and "appreciation for." Maybe, too, someone will be able to convince me someday that simulations can likewise build understanding. But, for now I want to extol books.

The kinds of books I have in mind are narratives, non-fiction accounts that tell a literal story (with a beginning, a middle, and an end)—books that are just long enough that they can't be read in a single sitting, and books that can't effectively be skimmed. The kinds of books I have in mind impel the reader to want to come back to them for more. They are also books that educate, in the sense that they rearrange their readers' point(s) of view.

For years, I have contended that the best journalists do a better job than most of the rest of us at evoking the principles that underpin life in foreign places and foreign systems. Twenty years ago, David Remnick (*Lenin's Tomb: The Last Days of the Soviet Empire*), Tom Friedman (*From Beirut to Jerusalem*), and Joseph Lelyveld (*Move Your Shadow: South Africa, Black and White*) topped my list. This wasn't just because these reporters wrote fluidly about complicated situations, but because at some point during the 1970s and 1980s academics started to indulge in truly awful writing. In fact, to earn tenure you were given little choice, but to learn to write tortured prose.

Consequently, I still prefer to assign journalists' accounts, since at least then there's a greater chance students will actually read them. Current favorites include Andrew Rice's The Teeth May Smile but the Heart Does Not Forget set in Uganda, Peter Godwin's When the Crocodile Eats the Sun and The Fear, both set in Zimbabwe, and Douglas Rogers' The Last Resort (also set in Zimbabwe). What makes these works resonate is that they zoom in and out from past to present, and from micro to macro levels, which means they educate as well as inform. They are also written in the first person and each does an excellent job of humanizing the otherwise incomprehensible.

But, I have also discovered that even when I come across what I consider to be the best single overviews of other countries, these books don't always work for students. For instance, Richard Cockett's *Sudan: Darfur and the Failure of an African State* is probably the single most insightful recent book about both Sudans. But, when I assigned it a couple of years ago, students were overwhelmed. Despite all of Cockett's skill as a correspondent, students came away convinced of the complexity, but feeling nothing for the place or the people. No one in the book grabbed them, which meant they walked away with no "sticky" principles for how either of the two Sudans worked. Thus, I didn't dare assign the next single country book I liked, Daniel Branch's *Kenya: Between Hope and Despair, 1963-2011*. I worried that the very thing that most impressed me about Branch's account would be the very thing to turn the students off; there would be too much that couldn't be familiar to people who had never been to Kenya. This brings me to Tamim Ansary.

Unlike Branch (a professor) and Cockett (a correspondent), Tamim Ansary is an author who, until 9/11, specialized in children's books. He is also half Afghan and half American and happened to grow up both in Afghanistan (until the age of 16) and in the U.S. I came across *West of Kabul, East of New York*, Ansary's first adult book, in the public library right after it was published in 2002. As soon as I read the first few chapters I knew: here was someone who could do a better job than I could at transmitting the very things I was trying to teach, whether about the strength of extended families or the significance of faith. Even better, Ansary could do so in such a way that even students who had already served in Afghanistan put down his book wishing they had read it before they deployed. A significant number also passed it on to their wives, just because.

During the ten years I assigned West of Kabul, it always had this same effect. It opened eyes. It gave even the most cynical officers a new appreciation for Afghans and for that country's rich, but tormented history. Of course, Ansary is a gifted writer. But, even more important, he understands what most Americans have such a hard time understanding, which he is perfectly positioned to do since he is one of us.

Up until a few days ago, I would have insisted that West of Kabul exemplifies the kind of writing to which members of the military need to be exposed to counterbalance their universe's warping demand for data and information. But, then I read Ansary's most recent book, *Games Without Rules: The Often Interrupted History of Afghanistan*, which may hit even more nails on the head.

West of Kabul is a memoir. *Games Without Rules* is a country study—though hardly in the sense of a CIA Fact Book or the Library of Congress's Country Study: Afghanistan. *Games* is more of a primer: here is how Afghanistan used to work and how power used to flow; here are all the things that interrupted Afghans' ability to develop Afghanistan; and here is what (and who) has thrown wrench after wrench into the country since 9/11. Ansary describes both the fixity and flux in Afghans' operating codes over time. He does so using short sentences, colorful anecdotes, not too many tribal names, and plenty of sly asides.

Take, for instance, his take on buzkashi, a game somewhat reminiscent of polo "that is played only in Afghanistan and the central Asian steppes. . . The game is governed and regulated by its own traditions, by the social context and its customs, and by the implicit understandings among the players."

Of course, most people invoke buzkashi when writing about Afghanistan. So, consider Ansary's first twist: "If you need the protection of an official rule book, you shouldn't be playing." And his second: "Two hundred years ago, buzkashi offered an apt metaphor for Afghan society. The major theme of the country's history since then has been a contention about whether and how to impose rules on the buzkashi of Afghan society."

By the time Ansary gets to his postscript, readers should appreciate exactly what he means when he writes, "The rules may be hard to discern in part because there isn't just one set." In fact, one theme throughout the

book is that every time Afghanistan—and a sense of Afghan-ness—begins to coalesce, outside forces come barreling in, and,

> *Every foreign force that comes crashing in thinks it's intervening in 'a country,' but it's actually taking sides in an ongoing contest among Afghans about what this country is. . .The foreign power essentially tries to swing the pot by grasping its handle, but the pot shatters, and the foreign power is left holding only a handle.*

It is hard for me to imagine former students, many of whom have now deployed to Afghanistan multiple times, not nodding their heads throughout their reading of this book and then voicing the same "woulda, coulda, shoulda" regrets they have after reading West of Kabul. Though, in this case and at this point in time, the questions I would pose them—and would really like to pose to the three and four star general officers who have been in charge—are: why didn't you know any of this? Where could (or should) you have gone to learn it? Why didn't you? And, wouldn't a deeper understanding have done everyone a greater service?

It is this last question that matters most. Syria. Libya. Central African Republic (let's hope not). Policy intellectuals might like to talk about a globalized world. Yet, the places where troops are sent are exactly the places where intelligence is hard to come by, the hunt for information turns desperate, and no one in uniform has the time, let alone the inclination, to develop understanding.

Meanwhile, as U.S. coffers shrink, the pressure to get things done quickly in such locations will only intensify. Elsewhere I have written about the problems finesse poses and why force and an altogether different rubric suits the U.S. better. But, presuming that Washington persists in sticking to its current path, it seems only prudent—nay, responsible—to develop a new kind of country study. In other words, not just reference books or smart cards, but narrative accounts the kinds of books those in uniform will want to read, and the kind that will help them grasp what is most essential to understand: no society exists without rules and every system gets gamed. At the same time, the who, what, when, where, and why of how systems get gamed will always be locally contingent.

To be clear, reading only one book should never suffice and overviews will never provide the granular local-level information operators, analysts, and commanders also need. But, there is a reason that J.K. Rowling's books appealed to an entire generation: she vividly described a whole other reality. For this reason alone, twenty-first century country studies shouldn't just humanize others the way great novels do. Instead—or rather, in addition—they need to bring to life other people's operating principles, so that those sent abroad on behalf of the U.S. understand a) what they are up against; b) what there is to work with; c) how different other peoples' sensibilities can be; and d) how others are likely to improvise and adapt in order to try to overcome.

Table of Contents

Fridge Sends Spam, Cyber Attack Hits Smart Gadgets

Times of India, Jan 21, 2014

WASHINGTON: A fridge was among more than 100,000 devices hacked by cyber criminals to send out spam emails — in what may be the first proven cyberattack on household "smart" appliances, researchers say. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centres, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks, researchers said.

Personal computers can be unknowingly compromised to form robot-like "botnets" that can be used to launch large-scale cyberattacks. Scientists at California-based security group, Proofpoint, found that cyber criminals have begun to commandeer home routers, smart appliances and other components of the Internet of Things (IoT) and transform them into "thingbots" to carry out the same type of malicious activity.

The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide.

More than 25% of the volume was sent by things that were not conventional laptops, desktop computers or mobile devices; instead, the emails were sent by everyday consumer gadgets such as compromised home-networking routers, connected multi-media centres, televisions and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location — and in many cases, the devices had not been subject to a sophisticated compromise. Instead, misconfiguration and the use of default passwords left the devices completely exposed on public networks, available for takeover and use.

"Botnets are already a major security concern and the emergence of thingbots may make the situation much worse," said David Knight, general manager of Proofpoint's information security division. "Many of these devices are poorly protected at best and consumers have virtually no way to detect or fix infections when they do occur," Knight said.

Table of Contents

Terabyte Leaks and Political Legitimacy in the U.S. and China

By Greg Austin, Globalist, January 24, 2014

The “leaking” of information is a time-honored tactic to undermine the legitimacy of a political opponent or a policy. Sir Winston Churchill relied on it during the run-up to World War II to attack what he saw as weak British responses to German rearmament.

Ever the master of using information and disinformation, he would use question time in the parliament to reveal morsels of secret information. As part of an embarrassment strategy, these were drawn from UK intelligence assessments of Germany’s military build-up and from UK policy planning documents.

At another level, the sustained control of information has always been viewed as central to political power. The totalitarian governments of the 20th century were among the best practitioners. The term propaganda came to symbolize this technique of political control of information.

Leaks and global governance

In such a governance frame, the idea of a strategic leak has always been one of a slow trickle of pieces of information. Meanwhile, the event itself or the process in question was unlikely to undermine the power of a determined state propaganda machine.

But now the old style of a steady flow of bit-by-bit “leaks” may be passing into history. Welcome to the brave new world of avalanche-like leaks, where the unauthorized release of secrets has moved from a trickle to a virtual flood.

And now, that flood has even biblical proportions. Wikileaks has been a manifestation of the changing times. All that is required is having a suitable platform to release those occasional floods of secret information.

In publishing 251,287 diplomatic cables from the U.S. government, the Wikileaks website provided a sustained embarrassment to the United States.

Wikileaks is passing into history

While there were temporary setbacks, the leaks did not shake the government to its core — or bring about the end of any political career. The total file size of the entire package of leaked cables was less than two gigabytes (2 billion bytes).

But Wikileaks is passing into history. By comparison, on some estimates, Edward Snowden took from the NSA 2,000 times as much information (4 terabytes, or 8 trillion bytes).

This did shake the United States government to the core. It did so not because Snowden revealed unusual activities that were not previously contemplated. The surprise lay in the scale of activity for which the U.S. government was fingered. That stunned people around the globe, foreigners first and, remarkably, American citizens later.

Leaks and legitimacy

The terabyte leaks of Snowden raised serious questions about the capacity of the United States government at a high political level: Can it contain the enormous technological potential of its own machines as well as the officials and managers who operate them?

The issue is not just one of basic constitutional rights. It also immediately raises questions of the moral legitimacy of government. The contest over whether Snowden’s acts were heroic or traitorous speaks to the depth of his impact on the legitimacy of the Obama administration.

That was June 2013. Within just seven short months, the wheel has turned again. The numbers have become even more staggering and the political environment around information security has become more chaotic as a result.

As the absolute size of the “leaks” is growing, it seems there will be growing threats to political legitimacy not really imaginable in earlier days.

China’s Snowden moment

Just as Wikileaks shook the US government to its core, China is now facing a similar seismic event.

This has been particularly visible in reports this week analyzing 2.5 million leaked files from offshore tax havens in the British Virgin Islands and the Cook Islands.

The leaks in question occurred more than a year ago and led to rapid adjustments in many tax jurisdictions to close loopholes highlighted by particular cases in the leaked documents.

But the sheer volume of the material meant that it has taken a team of more than 50 journalists worldwide over a year to start to see the totality of the files in a way that speaks very directly to bigger issues of political legitimacy.

As one might expect of journalists, to address the way these leaks threaten political legitimacy, they chose a prime news target: China's ruling Communist Party and its wealthiest entrepreneurs.

In these tax havens, the International Consortium of Investigative Journalists (ICIJ) has identified 22,000 separate clients residing in China (including Hong Kong) who held offshore accounts. These are included in a database accessible through the ICIJ website.

The "red nobility" goes fishing

Their reports on China this week highlight the wealth and offshore trading of China's "red nobility", descendants or relatives of former or current Chinese leaders. There are no smoking guns revealed in the ICIJ reports on China so far, but there is no doubting the political sensitivity of the leaks.

To be sure, China's internet censors have blocked all access in China to the database webpage and almost all access to the reports.

International media have correctly pointed out the link between this sort of information leak and the cases in 2012 of reports on the personal wealth of the extended family members of Wen Jiabao (then the Prime Minister) and Xi Jinping (then the named successor as Communist Party Secretary General).

Yet, the bigger story is not in the specifics of even these two notable families, but rather in the new phenomenon that the ICIJ database and its information sources represent.

Credibility at stake

Even if the Chinese offshore accounts are not illegal, many will be in some way connected with corrupt activity. Either way, the available data is so extensive and so unfamiliar to most Chinese citizens that it puts the credibility of the entire Chinese ruling elite in play. It does not matter whether this is elaborated in broad daylight or not.

Behind the scenes in China, the leaders have moved aggressively to shore up cyber security arrangements affecting their personal lives. But all indications are that this is an exercise doomed to failure.

There is now no single issue more sensitive in China than internet reporting on the leaders. Nor is there a topic of more public interest which, depending on your viewpoint, may either be curious or predictable for a formerly very closed society.

To counteract that imminent threat, China's leadership has tried the route of technical surveillance by any means and of anyone.

Internet terror, anyone?

The term "internet terror" is used in newspapers in China to describe the practice of using leaked information to affect political careers and personal lives. The leaders now know that it affects them, and their hold on power, as well.

They fear the near certainty that there is a Chinese Edward Snowden out there who will deliver an even greater information catastrophe to them.

They also fear that one day soon, the U.S. intelligence community, with its massive cyber surveillance capability, will link up with investigative journalists or other activists to publish sensitive information about the leaders on such a scale that the Community Party itself will be discredited almost overnight.

They have images from 1989 in their minds: the Tiananmen protests and the collapse of Communist Parties in Eastern Europe. Now they fear the next wave of resistance will occur online.

Indeed, the U.S. government in 2010 offered funding for Falun Gong internet activity against the Chinese government.

Welcome to the info wars

These considerations give rise to a possible process of action and reaction. This mix of insecurity and conjecture could possibly lead to an information war.

The Chinese Foreign Ministry has already called into question the motives of the ICIJ, meaning a presumption that they are trying to dismantle Party legitimacy in China. As the terabyte leaks affecting China's political class accumulate, the leaders' insecurity will also increase.

One thing is for sure: The international information wars are moving to new levels. Issues of ethics and legitimacy long considered settled are now at risk in novel ways either because of the very large scale of leaks themselves or the scale they can take on through new internet-based media.

In the end, we may hope that liberal democracy — as in rule by the people in an atmosphere of personal freedom — can be the ultimate victor. But those who study the new technologies and politics, including in China, do not see that as inevitable.

Table of Contents

Election Coverage Shows Growth of New Afghan Media

By Kay Johnson, Associated Press, Feb. 4 2014

KABUL, Afghanistan (AP) — In a crowded room overlooking a gleaming television studio, Tolo TV's election team is strategizing for Afghanistan's presidential debate when the room suddenly goes dark. The staff doesn't miss a beat.

The 13 men and three women just keep on talking about soundboards, cameras and the taking of questions via Twitter until the station's generator kicks in and the overhead lights flicker back on.

"It's just technical difficulties," explains Mujahid Kakar, the Tolo anchor and moderator of the upcoming debate among six of the main contenders vying to succeed President Hamid Karzai in the April 5 election.

The moment is a reminder of the difficulties of reporting in an impoverished country torn by war. Yet, in many ways, Afghan media coverage of the crucial campaign that kicked off this week resembles what you'd see in any other modern democracy, with newspaper candidate profiles and political talk shows on numerous TV and radio stations.

And this week, for the first time, major contenders for the presidency will introduce themselves to the nation in a televised debate.

The proliferation of Afghan media in the past 12 years is one of the most visible bright spots of the fraught project to foster a stable democracy, even as the NATO military mission in Afghanistan nears its end with the country still riven by war with Taliban insurgents and mired in corruption and poverty.

Given that the Taliban banned television as sinful and allowed only one religious radio station before they were driven from power in 2001, the sheer number of media outlets — dozens of TV channels, more than 100 radio stations and hundreds of newspapers — is stunning. That they are mostly free to set their own agenda is even more so.

"It goes against some of that common wisdom that it's all doomed," says Nader Nadery, chairman of the Free and Fair Election Foundation, an Afghan pro-democracy group.

Where the Taliban banned sports, Afghans can now watch soccer matches on television. Where music aside from religious hymns was forbidden, there are "American Idol"-style singing competitions. Women were once erased from public life; now some host television shows.

What's less clear is what the future holds for all these media outlets after this year, when most foreign troops will go home and much of the billions in aid dollars is expected to be reduced.

For now, though, Afghan news outlets are enjoying a moment in the sun. Newspapers in Dari and Pashto, the country's main languages, are full of campaign coverage. Radio and TV stations from all over the spectrum — private for-profit ventures, aid-supported democracy boosters and stations supported by political parties or religious groups — compete to offer their views of the race.

Tolo TV, Afghanistan's most popular channel, is touting the debate as the first in the country to pit all the major presidential candidates against one another. State television hosted a debate between Karzai and two challengers during the last election, in 2009, but it excluded Karzai's main challenger Abdullah Abdullah, who is running again this year. Tolo TV held its own debate in 2009, but Karzai declined to attend.

"It's a historic debate for the country and for the people," says Kakar, 42, a former refugee who studied journalism in Pakistan and returned home after the U.S.-led military intervention. "This is a process of democracy. We prove to the people that these candidates, they have the responsibility toward the people."

It may be a first but probably won't be the last. With Karzai ineligible to serve another term and a wide field of candidates looking to distinguish themselves, debates are expected to be a fixture of the two-month campaign period.

With Afghanistan's low literacy levels, radio and television dominate the media landscape, with 63 percent of all Afghans listening to radio regularly and 48 percent watching television, according to research conducted in 2010 for the U.S. Agency for International Development.

Tolo TV — which is part of the privately held Moby Group founded by Afghan-Australian brothers in part with U.S. aid money and is now earning revenue of some $20 million — is by far the most popular channel, with an estimated 10 million viewers tuning in to its mixture of news, sports and light entertainment.

Other television outlets included Ariana and YakTV, which air a mixture of cooking shows, games and Afghan cultural fare. The government is still a major player, with a state television station and more than 30 government-linked radio stations. There are also numerous private stations funded by politicians and religious leaders.

While most of Afghanistan's television fare is tame by Western standards — female reporters wear headscarves, and imported Turkish soap operas are pixelated to mask any show of skin by women — the flourishing entertainment and news have drawn the ire of many religious conservatives.

Sadaf Amiri, 23, anchor of a political talk show on Tolo, knows that firsthand from the threats and the cold shoulders from some of the more conservative politicians she has interviewed.

"For a woman, working in the media is a threat in itself, whether someone threatens us personally or not," Amiri says. "But I have been threatened."

Whether the relatively free press will remain in Afghanistan is not certain. Even if the election goes smoothly, Afghanistan's religious conservatives still wield tremendous power, and there is no guarantee that future governments will be able to resist pressure to curtail the press.

A greater threat might be financial. Many of the newly minted stations and newspapers are dependent on foreign funding, and the few profitable private outlets, like Tolo, get much of their advertising revenue from businesses that rely on the coalition.

Still, Nadery argues that this year's unprecedented level of campaign coverage illustrates that Afghanistan has changed in fundamental ways in the past 12 years. Taking a more optimistic view than many, he says Afghans have become accustomed to the new, relatively freewheeling media and won't give it up easily. The same may also go for elections.

"Societal transformation here is a direct result of the free media," Nadery says. "The media also changed the way politics have been done in this country."

Table of Contents

The Pakistani Taliban's P.R. Offensive

By Huma Yusuf, New York Times, Feb. 3 2014

LONDON — A joke has been circulating among Pakistanis on Twitter: "How to negotiate with the Taliban: Blast. Condemn. Blast. Condemn. Blast. Condemn. #Fail." It mocks the government's swiftness at denouncing terrorist attacks while doing too little to stop them.

In 2013 alone, the Pakistani Taliban, a coalition of radical Islamists who want to overthrow the state and impose Shariah law, carried out 645 attacks in Pakistan, killing 732 civilians and 425 security personnel. And there can be no suicide bombing or gun attack, it seems, without politicians from the center, the opposition and even fringe parties joining a chorus of woe and regret.

Now the Pakistani Taliban are chiming in. The spokesman of the Pakistani Taliban condemned a blast on Jan. 16 at an Islamic center in Peshawar that killed 10 people and wounded more than 50. He spoke against attacks in public places that claim innocent lives and blamed the bombing on groups seeking to "tarnish the image of the mujahedeen."

No one claimed responsibility for the attack, but the target and its method were characteristic of the Taliban.

The disclaimer, however, was not. If anything, the Pakistani Taliban have long bragged about their operations, sometimes circulating gory videos to document them. In late September, the group posted on Facebook a clip showing a roadside blast in northwest Pakistan on Sept. 15; the attack killed a general, one of the group's highest-ranking targets in its bid to destabilize the state. Circulating such footage allows the Pakistani Taliban to glorify their commanders and try to convince the public and new recruits that their mission to bring Islamic law to Pakistan is making progress.

The Pakistani Taliban's P.R. strategy began to shift last year when the center-right government of Prime Minister Nawaz Sharif, which was elected in the spring, proposed holding peace talks, and perhaps offering members of the group amnesty in exchange for a cease-fire. (Previous governments had favored limited

military action, which only sparked more attacks.) But the idea of negotiating with the Pakistani Taliban — who have killed tens of thousands of Pakistanis since the mid-2000s — divides the country: Some people believe talks are the only option, others equate them with surrender. The public is confused partly because the Taliban fight in Islam's name and, feeding off rampant anti-Americanism, target officials they declare to be American stooges.

And so even as they have intensified the pace of their activities — increasing suicide attacks across Pakistan by 39 percent between 2012 and 2013, from 33 to 46 — the Pakistani Taliban have been trying to sow more confusion about their agenda. One of their spokesmen decried a double suicide bombing at All Saints' Church in Peshawar in October, which killed more than 80 Christians, saying the attack had been carried out by malign forces intent on sabotaging the peace talks. Yet the group has targeted religious minorities before, specifically Christians, in the name of avenging the victims of American drone strikes. And two minor terrorist outfits with known links to the Pakistani Taliban, Jundullah and Junood ul-Hifsa, eventually claimed responsibility.

The Pakistani Taliban are an umbrella group with many chapters in most cities and small towns, and close operational ties with other extremist organizations with sectarian or anti-India agendas. They train with anti-Shiite groups like Lashkar-e-Jhangvi. By virtue of their vast network, they can be said to have a hand in virtually any terrorist attack in Pakistan.

But there are so many different sub-groups, with their own names and chiefs, and there is so much infighting among them, that the public gets bogged down trying to differentiate them. More and more there also are "pop-up" militant groups — small radical bands that come together, often with support from the Taliban, to carry out specific attacks and then disband — that are virtually impossible for law-enforcing agencies to track.

Meanwhile, Pakistanis are primed for manipulation. For years, conspiracy theories have swirled around suggesting that terrorist attacks are being carried out by foreign agents who want to destabilize the country. And decades of shadowy politicking have left the public thinking that government officials may be less trustworthy than terrorists.

For years Pakistani politicians slammed Washington for violating Pakistan's sovereignty with drone strikes, but then, last April, Gen. Pervez Musharraf, the former president and army chief, admitted that his government had secretly signed off on the United States' drone attacks. In November, soon after announcing that the government had initiated talks with the Taliban, the interior minister backtracked. The government then designated center-right politicians and leaders of religious political parties to serve as interlocutors with the Pakistani Taliban — only to rescind the appointments a few days later. Last week, even as the government confirmed wanting to pursue talks, leaders of the ruling Pakistan Muslim League-N announced an imminent military operation against Taliban hideouts in North Waziristan.

The government's equivocations afford the Pakistani Taliban a rhetorical advantage: All they have to do is point out its contradictions and say the government isn't serious about negotiating. This puts the onus on the state to prove its commitment to peace, perhaps by meeting the Taliban's preconditions for talks, like an end to drone strikes. The point is also to generate public pressure on the government to pursue talks without resorting to military action.

With its history of savage attacks and audacious jail breaks, the Pakistani Taliban have long been two steps ahead of Pakistan's security forces and intelligence agencies. Now, the increasingly P.R.-savvy organization is also outwitting the government in terms of messaging. By obfuscating their precise responsibility for Pakistan's security issues, the Pakistani Taliban are dampening the public's enthusiasm for a sustained push against terrorist groups. And progress in the war of words is progress in its war for power.

Table of Contents

Russia to Create Cyberwarfare Units by 2017

From RIA Novosti, 30/01/2014

MOSCOW, January 30 (RIA Novosti) – Russia plans to create special cyber-defense units to protect the country against online warfare in the coming years, a senior military commander said Thursday.

The units are being formed "to defend the Russian armed forces' critical infrastructure from computer attacks," Major-General Yuri Kuznetsov said at a meeting of military officials.

Formation of the units will be conducted in stages and will be completed by 2017, Kuznetsov added without disclosing further details.

In August, a Defense Ministry spokesperson confirmed there were plans to train cyberwarfare units, but dodged a question on the timeframe of their activation.

Defense Minister Sergei Shoigu said in July the army must heavily recruit new programmers to meet the rising need for military software.

Computer experts have suggested in the past that the government has cooperated with hacker groups operating in the country.

Alexei Moshkov, the head of the country's cybercrimes Bureau of Special Technical Measures, said Thursday that his agency thwarted hacker attacks last year aimed at defrauding Russian citizens of a total of around $28 million.

Every second, 12 people around the world become victims of hacking, and the vast majority of attacks target financial assets, Moshkov said.

Online attacks also frequently target news outlets.

On Thursday, major Russian newspaper Vedomosti's website was knocked out for several hours by a denial of service attack.

Table of Contents

Senate Cybersecurity Report Finds Agencies Often Fail To Take Basic Preventive Measures

By Craig Timberg and Lisa Rein, Washington Post, February 4, 2014

WASHINGTON — The message broadcast in several states last winter was equal parts alarming and absurd: "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living. . . . Do not attempt to approach or apprehend these bodies, as they are considered extremely dangerous."

The reported zombie invasion was not something out of the "The Walking Dead." It was the federal Emergency Alert System under control of hackers — who exploited weaknesses that are disturbingly common in many critical systems throughout government, according to a Senate cybersecurity report set for release Tuesday.

U.S. officials have warned for years that the prospect of a cyberattack is the top threat to the nation and have sharply increased spending for computer security. Yet the report by the Republican staff of the Senate Homeland Security and Governmental Affairs Committee says that federal agencies are ill-prepared to defend networks against even modestly skilled hackers.

"As a taxpayer, I'm outraged," said Alan Paller, who is research director at the SANS Institute, a cybersecurity education group, and reviewed a draft version of the report ahead of its official release. "We're spending all this money and getting so little impact for it."

The report draws on previous work by agency inspectors general and the Government Accountability Office to paint a broader picture of chronic dysfunction, citing repeated failures by federal officials to perform the unglamorous work of information security. That includes installing security patches, updating anti-virus software, communicating on secure networks and requiring strong passwords. A common password on federal systems, the report found, is "password."

Obama administration officials quibbled with elements of the report but acknowledged that getting agencies to secure their systems against attack has been difficult.

"Almost every agency faces a cybersecurity challenge," said Michael Daniel, special assistant to the president on cybersecurity policy. "Some are farther along than others in driving awareness of it. It often depends on whether they've been in the crosshairs of a major cyber incident."

The report levels particularly tough criticism at the Department of Homeland Security, which helps oversee cybersecurity at other federal agencies. The report concluded that the department had failed even to update essential software — "the basic security measure just about any American with a computer has performed."

"None of the other agencies want to listen to Homeland Security when they aren't taking care of their own systems," said Sen. Tom Coburn, R-Okla., who as the ranking minority member of the committee oversaw the development of the report. "They aren't even doing the simple stuff."

The underlying problem, said Coburn and several outside experts, is the failure of federal agencies to hire top-notch information technology workers, pay them enough and give them enough clout to enforce routine security practices.

"It's a low-status, often low-paid, high-stress position because people only notice systems administrators when something breaks," said Steven Bellovin, a Columbia University computer science professor and former Federal Trade Commission technologist. "It becomes a very easy position to neglect."

Higher up the chain of command, agency directors are rarely held accountable for security failures, experts said, because it is often unclear who is responsible. No penalties are mandated by law.

Take the bogus zombie alert, which was carried by television stations in Michigan, Montana and New Mexico. It highlighted flaws in the oversight of the Emergency Alert System, which is mandated by the Federal Communications Commission and managed by the Federal Emergency Management Agency.

Hackers discovered that some television stations had connected their alert-system equipment to the Internet without installing a firewall or changing the default password, as the company's guide instructed, said Ed Czarnecki, an official with Monroe Electronics, which manufactured the equipment that was breached. He said those mistakes in elementary network security might have been prevented with more instruction from the government.

"Neither the FCC nor FEMA had issued clear guidelines on how to secure this gear," said Czarnecki said.

Though the incident was seen as a prank, it highlighted weaknesses that could have been dangerous if hackers had broadcast misinformation during an actual emergency or terrorist attack, experts said. Monroe Electronics and the FCC have worked with affected stations to prevent a recurrence, they said.

The Department of Homeland Security said that it, too, has worked to resolve problems identified in the Senate report.

"DHS has taken significant measures to improve and strengthen our capabilities to address the cyber risks associated with our critical information networks and systems," S.Y. Lee, a department spokesman, said in an emailed statement.

Other problems identified in the Senate report

- In every year since 2008, the GAO has found roughly 100 weaknesses in the computer security practices of the Internal Revenue Service, which took an average of 55 days to patch critical system flaws once they were identified. It is supposed to take only three days to do so.

- Hackers have cracked the systems of the Energy Department, gaining access to the personal information of 104,000 past and present department employees.

- The Nuclear Regulatory Commission, which keeps data on the design and security of every nuclear reactor and waste facility in the country, "regularly experiences unauthorized disclosures of sensitive information." An agency spokeswoman issued a statement saying it "takes information security very seriously and works continuously toward improvements."

- And at the Securities and Exchange Commission, laptops containing sensitive information were not encrypted and staffers sometimes transmitted private information about financial institutions on personal email accounts. On at least one occasion, an SEC staffer logged onto an unsecured Wi-Fi network at a convention of computer hackers.

While the report was released by Coburn, a Republican, the Democratic chairman of the Senate committee concurred with many of its findings.

"Federal agencies still have more work to do in this area, and the laws that govern the security of our federal civilian networks need to be reformed," said Emily Spain, spokeswoman for Sen. Tom Carper, D-Del.

Still, Washington has been slow to act. A 2000 law to improve government cybersecurity did not mandate consequences for agency lapses. In recent years, numerous bills calling for better computer and network security have languished in Congress. The White House, meanwhile, is pushing to give the Department of Homeland Security more authority to enforce cybersecurity rules across government.

"At the end of the day, it's a lot like the problem you have in businesses," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies. "The CEOs don't see cyber as their mission, as a fundamental problem. You don't see your job as running a secure network. If something goes wrong, nothing happens to you."

Table of Contents

U.S. Evaluates China's EMP Threat

By F. Michael Maloof, WND.com, 04 Feb 2014

While China calls the potential use of an EMP weapon against U.S. interests its “ace,” officials inside the American Defense Department have issued a statement that warnings of an increased threat are “reckless and irresponsible.”

WND reported only days ago that members of the Chinese military are looking to use an EMP as part of a "one-two punch" to knock out, literally within seconds, all defensive electronics not only on Taiwan but also on U.S. warships that could defend the island.

The damage would come from the electromagnetic pulse from an explosion, probably a nuclear weapon, that could be detonated at altitude over the region China wants to target. EMP damage

could include a complete loss of electronics, computers, automated systems, communications, food and utility services – even transportation.

However, the Department of Defense, or DOD, in response to an inquiry from Fox News' Bret Baier, downplayed the destructive use of an EMP.

"The Department is unaware of any increase in the threat of a deliberate destructive use of an EMP device," the unsigned DOD statement said. "Further, any reporting to the contrary by those without access to current threat assessments is both reckless and irresponsible."

Ironically, this latest statement is at odds with even a new report issued by DOD's Defense Science Board, or DSB, which concludes that DOD and the intelligence community currently lack national technical means sufficient to monitor the development of foreign, including terrorist, nuclear weapons programs.

"So how does the Obama administration know that Iran does not yet have the bomb?" asked Dr. Peter Vincent Pry, who was staff director of the congressional commission that produced the

2008 report warning of the impact of an EMP on the nation's national grid and its critical infrastructures.

Pry, who formerly worked at the Central Intelligence Agency, today serves as executive director of the congressional advisory Task Force on National and Homeland Security.

"How can DOD be so cocksure that the threat from EMP weapons is not increasing, contrary to all evidence?" Pry asked. "This is dynamite."

The report of the DSB, whose members hold the highest security clearances with need-to-know access, said closing the nation's global nuclear monitoring gaps should be a national priority. It

added that it will require a level of "commitment and sustainment we don't normally do well without a crisis."

"In short, for the first time since the early decades of the nuclear era, the nation needs to be equally concerned about both 'vertical' proliferation, or the increase in capabilities of existing nuclear states, and 'horizontal' proliferation with an increase in the number of states and nonstate actors possessing or attempting to possess nuclear weapons," the report said.

"These factors … led the Task Force to observe that monitoring for proliferation should be a top national security objective – but one for which the nation is not yet organized or fully equipped to address," the DSB said.

The report said monitoring to support treaties is but one part of the overall requirement that should be driven by monitoring for proliferation.

This broader scope, the report said, presents challenges for which current solutions are either inadequate, or more often, do not exist. Among these challenges are monitoring of: Small inventories of weapons and materials, even as low as a single "significant quantity of fissile material"; Small nuclear enterprises designed to produce, store, and deploy only a small number of weapons – intended as a proliferant's end goal, or as the first steps to achieve larger inventories or more sophisticated capabilities; Undeclared facilities and/or covert operations, such as testing below detection thresholds, or acquisition of materials or weapons through theft or purchase; Use of non-traditional technologies, presenting at best ambiguous signatures, to acquire both materials and components; Theater nuclear forces and associated doctrine, exercises, and training complicated by the use of mobile, dual-use delivery systems; Many more players to whom access by the U.S. or its allies will be limited or extremely difficult, some of whom will be globally networked with global access to relevant science and technology.

"The growing EMP threat seems to escape the Obama administration," according to Rachel Ehrenfeld of the Washington-based American Center for Democracy.

She pointed out that as far back as September 2002, Defense Secretary Donald Rumsfeld had warned that countries have placed ballistic missiles in ships, such as cargo, commercial ships, all over the world.

"Any given time," Rumsfeld said at the time, "there's any number off our coast, coming, going, on transporter-erector-launchers, and they simply erect it, fire off a ballistic missile, put it down, cover it up. Their radar signature's not any different than 50 others in close proximity."

Yet, Ehrenfeld said, America's electrical power grid is more vulnerable today to the effects of an EMP, either by a sun-burst or high altitude nuclear explosion, than it was five decades ago.

Despite the most recent DOD statement that it is unaware of any increase in the threat of a “deliberate destructive use of an EMP device,” the Defense Threat Reduction Agency in late December 2013 issued a solicitation to conduct “satellite system performance modeling, satellite system response-to-environments modeling, high altitude weapons electromagnetic pulse effects modeling and disturbed atmosphere effects modeling.”

As though the left hand at DOD didn’t know what the right hand was doing, DOD has completed a review mandated by Congress in the 2013 National Defense Authorization Act of potential sites for enhanced East Coast defense against intercontinental ballistic missiles.

While it took congressional action to look at closing security gaps in the U.S. missile defense system, the DOD has maintained that existing sites in California and Alaska provide sufficient protection from threats emanating from North Korea or Iran.

“The bad news is that such a site would not deal with Iran, or their terrorist surrogates, in launching ballistic missiles from off our coasts – particularly from the Gulf of Mexico, nor would it be effective in defending against nuclear weapons carried by Iranian satellites over the South Pole, so this threat is not hypothetical from a technological point of view,” Ehrenfeld said.

Ehrenfeld and other national security experts such as former Ambassador Henry Cooper, who heads High Frontier and was the first director of the Strategic Defense Initiative under President George H.W. Bush, said a fix would be to place Aegis ballistic missile defense ships in the Gulf of Mexico.

Cooper has contended that the North Koreans tend to undertake missile tests using a south polar orbit against which the U.S. does not have a missile defense, especially if the missile has an EMP nuclear device called a “super EMP,” which North Korea is thought to be developing.

Table of Contents

39th IOS: Foundations for the Future

By Senior Airman Michelle Vickers, 1st Special Operations Wing Public Affairs, 1/22/2014

1/22/2014 - HURLBURT FIELD, Fla. -- Airmen assigned to an air operations center work on a team consisting of members from several career fields. Together, they plan and execute air campaigns. Meanwhile, cyber Airmen have the no-fail mission of defending the nation's networks from attacks.

The 39th Information Operations Squadron here trains IO and cyber warriors to work in these environments.

The 39th IOS graduates more than 1,000 students annually from a variety of courses which cover subjects like electronic warfare and operations security.

"From my perspective, we aren't only educating, but we're training future graduates to be able to go out in their environment and react in real world situations," said Capt. Angela Shalduha, 39th IOS instructor.

The school house's instructors, which span 18 career fields, provide valuable expertise to students of all ranks.

Whether a brand new instructor like Shalduha, or a more seasoned veteran such as Staff Sgt. Latisha Taylor, the instructors bring their operational experiences from AOCs and defensive cyber units across the Air Force.

"My background as an intelligence briefer helped me with the public speaking aspect of teaching," Taylor said. "I was at an AOC for a year, which also gave me a good knowledge of what we teach on the IO side, as well as how everything integrates."

The broad range of career fields and experiences allow instructors to pull from their colleague's knowledge when topics they are less familiar with arise. It also allows students to see how different specialties work in unison.

"Parts of our classes involve IO or intelligence, so we'll pull experts from those areas to teach," Shalduha said. "It really helps having a diverse staff because it gives students a better perspective of the operational environment at their units."

New instructors go through a training process where they must take and excel in the course they will teach. They also attend an instructor methodology course to learn how to teach, test and develop curriculum. After their courses, training isn't over. They must complete 180 hours of student teaching and pass three classroom evaluations.

When not in front of the classroom leading guided discussions or directing students through simulations, instructors research the latest techniques in their fields, according to Shaldhua.

"The instructors on the podium actually make updates to the curriculum," Shalduha said. "If you're not current, you're losing in cyber."

While the background research and preparation may require long hours, the instructors said they see the payoff in their students.

"We have actually received emails from students who have been through the training, which said, 'If I hadn't gone through the training, I wouldn't have known what to do at my unit,'" Taylor said. "Just seeing this, and realizing I had a hand in it, is rewarding and satisfying."

Table of Contents

Russian Cyber Capabilities, Policy and Practice

By David J. Smith, inFocus Quarterly, Winter 2014

Although most commentators on cyber threats to the United States appear fixated on China, we ignore Russia at our peril. "Unlike China," Jeffrey Carr explains on his Digital Dao blog, "Russian cyber operations are rarely discovered, which is the true measure of a successful op."

Russia—its government and a motley crew of sometimes government-sponsored but always government-connected cyber-criminals and youth group members—has integrated cyber operations into its military doctrine, has used cyber tools against enemies foreign and domestic, and is conducting strategic espionage against the United States. Moreover, it spares no diplomatic effort in trying to forge a path for its nefarious activities while resisting efforts to do anything constructive in the international arena.

To explain all this, it is necessary to set out two points about Russia: 1) Russia is characterized by a unique nexus of government, business, and crime; and 2) Russia takes a much broader approach to information operations than do most Western countries.

Corruption is the dominant characteristic of the current Russian polity. And with systemic corruption come opportunities for collusion on just about everything. The rule of law flies out the window, replaced by personal relationships and payoffs. Laws are enforced arbitrarily—what matters is one's circle of friends.

The second point is that Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda. Computers are just among the many tools of information warfare, which is carried out 24 hours a day, seven days a week, in war and in peace. Seen this way, distributed denial of service (DDoS) attacks, cyber espionage, and Russia Today television are all related tools of information warfare.

Moreover, Russia's way of kinetic war includes information warfare and it follows that information warfare against Russia will be considered warfare. The current Russian military doctrine calls for "prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces."

Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine. Although it was not fully successful, we must assume that the Russian military has studied the lessons learned, just as it has done for every other facet of its poor performance against Georgia. Given all the doctrinal attention paid to the subject, we must assume that Russia is honing far more sophisticated military cyber capabilities.

At home, Russia also has a concept of information security very different from Western countries. The September 2000 Doctrine of Information Security of the Russian Federation— released just eight months into Putin's presidency—sets forth three objectives. Russia shares the first with just about every country in the world: to protect strategically important information. However, the second and third objectives set Russia apart, at least from democratic countries: to protect against deleterious foreign information and to inculcate in the people patriotism and values.

Another unique feature of the Russian approach is extensive reliance on youth groups such as the Kremlin-controlled Nashi and cyber-criminal syndicates such as the now invisible Russian Business Network (RBN). There are three reasons Russia sub-contracts some of its cyber work to youth groups and criminals.

- It is super cost-effective—imagine a reserve force that not only does not cost money, but actually makes money when not employed by the state.
- Without cost, it hones skills and specialization to a degree to which no government training program could aspire.
- The use of kids and criminals confounds the attribution problem. Even after extensive cyber forensics, attacks are not traced back to government computers. This is particularly confusing to many Westerners who cannot imagine a government so intertwined with crooks and punks.

And there are plenty of well-trained people to carry out these activities. Russia exhibits many characteristics of an extractive economy, while still enjoying the benefits of the quite good Soviet educational system. Great wealth is concentrated in the hands of a few, while many people with training in math, science and computers want for work.

The result is a thriving cyber-criminal industry. An excellent Trend Micro report literally catalogs the malware and services for sale or rent on the deep Runet, as the Russian portion of the Internet is known. This illustrates both the lawlessness that prevails on and around the Runet and the availability of talent for hire, including for hire by the Russian state.

Apparently rented botnets went to work against Estonia in 2007. The Estonian government had decided to move the "Bronze Soldier of Tallinn" statue from the city center to a military cemetery. Ethnic Russians and Russia took this as an offense—or at least as an excuse for trouble. Russian politicians arrived in Estonia to rile things up and some Russian language websites offered instructions about which Estonian websites to attack and how to do it. For a week in late April and early May, simple DDoS attacks were carried out, somewhat ineffectively. Then the professional botmasters went to work with DDoS attacks, threatening essential services, doing significant damage to the Estonian economy.

In 2008, it was Georgia's turn in the first ever combined kinetic and cyber-attack. Many of the same techniques and computers involved against Estonia a year earlier resurfaced against Georgia.

Exhibiting remarkable insight on the part of the perpetrators, DDoS attacks on Georgian government websites, particularly the president's website, began more than two weeks before the kinetic Russian invasion. On the day the kinetic war started, sites such as stopgeorgia.ru sprang up with a list of sites to attack, instructions on how to do it and even an after-action report page. It is instructive that all this was ready to go—surveys, probing, registrations, and instructions—on day one! An Internet blockade was traced to five autonomous systems—four in Russia and one in Turkey—all controlled by the criminal syndicate RBN.

When one considers the forensic evidence, geopolitical situation, timing, and the relationship between the government and the youth and criminal groups, it is not difficult to conclude that the Kremlin was behind it all.

Three years later, we learned that the Kremlin treats all enemies, foreign and domestic, the same. In the spring of 2011, again with many of the same techniques and computers employed against Estonia and Georgia, DDoS attacks were directed against websites generally associated with opposition to the Putin government. Among the targets were particularly meddlesome pages on the LiveJournal blog site, websites run by anti-corruption crusader Aleksey Navalny, and the Novaya Gazeta newspaper.

People's Freedom Party leader Boris Nemtsov commented, "Hardly anyone could have done this other than the security services."

The March-April attacks were apparently a dry run for the December 4 Duma elections. On the day of the elections, a number of websites generally associated with the opposition were taken down by DDoS attacks. However, the perpetrators apparently miscalculated the power of the Internet.

They appear to have been obsessed with a site called kartanarusheniy.ru, an interactive map of election violations, sponsored by the election watchdog Golos, which receives funds from the American National Endowment for Democracy. Kartanarusheniy itself was taken down, as were sites that linked to it or mentioned it. However, many other sites were untouched, indeed, one could read about the sites that were dark on the sites that remained up. It seems that a few DDoS attacks do not cow everybody as a few arrests and beatings used to do.

Social media and blog sites were very active right through the March 4, 2012 presidential election; however, the Kremlin's botmasters were apparently called off altogether. Another indication that the government controls them is the discipline with which they all desisted. Had they been truly independent patriotic hackers, one would have expected at least a few of them to have persisted in their online hijinks.

"The infrastructure for political battle," Navalny observed, "has become cheaper. Now you can just use your computer." And the Kremlin is worried—worried about Arab Spring, London riots, unrest in the North Caucasus, likely attempts to subvert the 2014 Sochi Winter Olympics and, of course, the unprecedented social media-borne anti-Putin demonstrations across Russia.

Nonetheless, as a matter of domestic politics, the Putin government appears to be in a quandary. In July 2012, a law "for the protection of children" on the Internet was passed. Activists such as Navalny fear that the law will be used to stifle political opposition on the Runet.

Navalny was convicted on what were clearly bogus embezzlement charges, but allowed to run for the post of mayor of Moscow. Despite renewed DDoS attacks on LiveJournal, there did not appear to have been any major government or government-backed online skullduggery associated with the September 9, 2013 mayoral

race. Perhaps the Kremlin is still trying to devise a workable strategy. Perhaps the certain victory of Kremlin favorite Sergei Sobyanin diminished the perceived need for one. More difficult to fathom is that soon after the election, Navalny was handed a five year suspended sentence, but he remains free and politically active. However, he has recently been targeted with further embezzlement charges.

Moscow's online behavior as the 2014 Sochi Winter Olympics approach may afford a good indication of whether there has been any evolution with regard to the use of the Internet for internal repression. Meanwhile, there is no reason to believe that Russia's external outlook has changed one iota.

Unsurprisingly, Russia's diplomatic activities on the cyber front reflect its policies on information warfare and information security. While steadfastly refusing to sign the European Convention on Cybercrime, a highly effective international approach to cyber security challenges, it joined China and a few others in plying proposals aimed at enhancing information security—that is, shielding autocratic states from the free flow of information across the Internet. It has also joined with China, Iran, and the International Telecommunications Union leadership in a grab at Internet governance, most recently manifested at the December 2012 World Conference on International Telecommunications.

Meanwhile, Russia undertakes a major effort at strategic cyber espionage against the United States. It is strategic in the sense that it is not just a government's spy agency trying to steal this or that bit of classified information or an enterprise conducting industrial espionage. Rather, it is a concerted effort to steal American intellectual property to achieve a level of technological development that Russia cannot achieve on its own. In this regard, it is worth repeating an October 2011 finding of the U.S. Counterintelligence Executive:

Motivated by Russia's high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward U.S. and other Western interests at the expense of Russia, Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security.

In sum, Russia—in its capabilities and its intent—presents a major cyber challenge to the United States. The only difference between it and China may be, as Jeffrey Carr points out, that it is seldom caught. And that, alone, may make it the number one cyber threat.

Table of Contents

National Guard Fights For Cyber Role In 2015 Budget

By Sydney J. Freedberg Jr., Breaking Defense, February 05, 2014

Chinese and Russian hackers have everybody running scared. So whatever else happens with the president's budget request for fiscal year 2015, we know it will include more money for things cyber, from purely defensive network security to black-budget "offensive cyber weapons" such as the Stuxnet worm. But one big thing remains in doubt: the role of the National Guard.

Cyber Command wants the Guard to help. Guard leaders want to help CYBERCOM. And the Army has at least considered a proposal to fund 390 positions in 10 new "Cyber Protection Teams" to be created in the Army National Guard. Whether this idea will get funded is being wrestled over behind locked doors and in the context of increasingly bitter fights between active-duty and reserve forces.

The budgetary question marks loom so large that one senior official at the National Guard Bureau emailed a warning to the Adjutants General, the Guard commanders of every state, territory, and the District of Columbia: Don't get out in front of what the federal budget will support.

"We have entered a new normal called sequestration," read the senior official's email. "To fund 'excess' or ill-defined requirements out of hide is impossible. I continue to be concerned with further investments in Cyber and ISR [intelligence, surveillance, and reconnaissance] without definitive requirements documentation from COCOM/MAJCOMs [Combatant Commands and Major Commands]. In my opinion this posture could put [Guard] force structure at risk depending on strategic choices being made by DoD leaders." (We agreed not to identify the official.)

So what are they choosing? "The Department continues to conduct analysis to determine the appropriate force structure for cyber in the Guard and Reserve components," was all a DoD official would tell me, after I'd been harassing people for an answer for weeks. "At this time, the Department's senior leadership has not made any decisions," he said – which is one of the reasons we're writing this story.

The outside experts we spoke to agreed that the Guard had a unique role to play. "I think they are the linchpin for being able to effectively defend the nation," said John Quigg, a retired Army officer and former senior CYBERCOM official, in an interview with my colleague Colin Clark. "The thing that is not obvious and is

wonderful about the Guard is that it sits between the federal government and the states, and that makes it very useful."

Both budgets and bureaucracy, however, are getting in the way.

Gen. Alexander: "The Guard Can Play A Huge Role"

Despite all the obstacles, there's certainly four-star support for giving the Guard a share of the cyber mission.

"The Guard can play a huge role," Gen. Keith Alexander, the (outgoing) chief of both CYBERCOM and the embattled National Security Agency, told Congress last year. "There's two key things that they can do. First… it gives us additional capacity that we may need in a cyber conflict. The second part is, it also provides us an ability to work with the states."

For their part, state governments "are clamoring" for Guard help on cybersecurity, Gen. Frank Grass, the chief of the National Guard Bureau, told reporters in November when he outlined the proposal for the 10 Cyber Protection Teams.

"Gen. Alexander and our chief Gen. Grass believe the Guard has a key role to play in cybersecurity," said Col. David Collins, the National Guard Bureau's chief cyber staffer (the "J-6"), in an interview. "So there is resounding agreement on that — [but] we're waiting for missions and force structure from the Army and the Air [Force]. We are still in the embryonic stages."

"It's not so much money," Collins told me. "The fundamental first step in all of this is, what is the Guard's place in the federal and DoD cyber response?"

The original Department of Defense (DoD) directives setting up the current cyber strategy "essentially took the reserve components out of consideration," Collins said. Why? "The presumption was all those forces needed to be on active duty 24-7, 365," he said. "[But] why can't you surge us as you do for other things?"

In fact, the Guard is arguably better suited for cyberwar than for physical war. It takes weeks to months to mobilize, train, and prepare Guard forces for deployment overseas, potentially up to 110 days for the largest and most complex units. A Guard cybersecurity expert could (almost) roll out of bed, log on and start defending networks around the planet before his coffee gets cold.

But this subjective assessment needs to get encoded into the formal military requirements process before anything can happen in the budget. "The National Guard has to have forces that are built primarily for a federal purpose," Collins said. Whenever state governors call out the Guard to control wildfires, floods, or rioters, the troops, trucks, and helicopters that respond are almost entirely paid for by the federal government for military missions.

On paper, the Department of Homeland Security would be in charge of defending the nation's non-military networks, but against high-tech or large-scale threats DHS would have to ask the Pentagon to help. The Guard could be part of that homeland defense response, but "the government doesn't have a plan that clearly indicates how that would be done," Collins said bluntly. "The National Cyber Incident Response Plan, in my opinion, is not very thorough….I don't mind going on record as the J-6 of the National Guard Bureau saying that the nation has a lot of progress that it needs to make."

He's hardly alone in that opinion, Not only is cybersecurity legislation chronically stalled on Capitol Hill, said Quigg, the former CYBERCOM official, "Cyber Command is increasingly attack-focused and the defensive mission has stalled….We're actually in worse shape now in some ways than we were five years ago."

What The Guard Can't Do

If the Guard were allowed to help out in homeland defense, Collins argues it would have three advantages over the active-duty force:

- First and most important, he said, Guard troops are physically present in armories, communities, and indeed civilian workplaces across the country, not concentrated in a few large bases. That puts them in constant contact with civilian networks and their operators.
- Second, the Guard can operate either on federal orders (so-called Title 10 status) or on the orders of the state governor (Title 32). Guard troops under the governor's command aren't bound by the Posse Comitatus Act or other restrictions on using federal troops for law enforcement.
- Third and last, as part-time troops, Guard cyber warriors would have full-time jobs in the civilian information technology world, giving them a different and often deeper expertise than the active-duty force, which tends to be younger.

Those are in order of importance: "A lot of people want to jump to No. 3 when they talk about the Guard," Collins emphasized. "That's out of sequence."

The Guard already has limited cybersecurity capability, but it's "very ad hoc," Collins said. Every state is authorized to have an eight-soldier Army National Guard network security team, though some Adjutants General didn't even know this option even existed until recently, and they have to find the funding themselves without federal help. The Air National Guard has a range of "network warfare" and "information warfare" squadrons of varying sizes, structures, and skill levels.

Some of these Air Guard units are impressive, said Atlantic Council cyber expert Jason Healey: "[There's] the 262nd Network Warfare Squadron in Seattle (which includes lots of people from Microsoft), [and] the 175th Network Warfare Squadron at Fort Meade is deeply embedded in NSA work."

"But states are increasingly trying to grab cyber mission for more budget, especially as more traditional missions are pared back," Healey went on. "This threatens to poison the whole effort as so many state piranha are trying to feed from the same mission."

Table of Contents

Red Star Rising: China's Ascent To Space Superpower

By Phil McKenna, New Scientist, 12 Feb 2014

ON 14 December 2013, the top trending topics on China's biggest social networks were a popular TV show and a football match. If it hadn't been for a concerted push from China's state-controlled media, the casual observer might never have noticed that China had just become the third country in the world to land on the moon.

The news was not greeted with sweeping enthusiasm. After all, landing the Yutu robotic rover, aka Jade Rabbit, on Earth's closest neighbour was a feat human explorers had bagged many decades before. "We're now only 50 years behind Russia and USA," quipped one commenter on Weibo, China's version of Twitter. "Our country's designers have some catching up to do," wrote another, before worrying that the joke would lead to police detention.

But if China itself seemed a little bored, that was nothing compared with the collective yawn echoing around the world. Apart from failing the novelty test, the mission was accomplished using knock-off equipment, and Yutu was dismissed as a tragic "me too" exercise by a country lagging decades behind the world's leading space powers.

This common reaction missed the point. Jade Rabbit's successful launch, landing and exploration is evidence of China's meteoric rise in the space stakes, and one that will only accelerate. "It is a classic example of the tortoise and the hare," says Dean Cheng of the Heritage Foundation, a conservative think tank based in Washington DC. From the sophisticated communications network that guided the rover to its destination, to emerging satellite technology that is the envy of other nations, to its plans for a new international space station, China is a force other space superpowers ignore at their peril. The ripples are reaching out to affect everything from your phone's settings to the first future footprints on Mars.

To get an idea of China's burgeoning space programme, look no further than its satellites. Starting in 1970, China launched low-quality transponders and rudimentary spy satellites capable of only the most basic tasks at an entirely unimpressive rate of one per year. By 2012, the country had surpassed the US with 19 launches in a single year. China had also sent its first taikonaut into space, conducted its first space walk and completed its first rendezvous and docking with a small space laboratory. "The manned program they are building is progressing a lot faster than the US did with theirs in the sixties," says Richard Holdaway, Director of the Rutherford Appleton Laboratory Space division, one of the UK's closest collaborators on the Chinese space programme. "They are catching up at an astonishing rate."

"In 15 years they have gone from bit player to leading player," says Jonathan McDowell of the Harvard-Smithsonian Center for Astrophysics in Cambridge, Massachusetts. And they have done so on a shoestring. China's space budget is less than one-tenth of the US one, according to a recent estimate by the Space Foundation, a non-profit organisation based in Colorado Springs.

So what accounts for the rapid acceleration? A common, and not entirely charitable, answer is that other nations have already solved many of the challenges. "When it was just the US and the Soviets, there were basic questions of survival – like what would astronauts breathe, how much oxygen, how much nitrogen – that no one knew the answer to," says Cheng. "Today China can benefit from much of that having been worked out and made publicly available."

His words reflect a familiar attitude that China's technological progress has been built largely on the ideas of others – whether given freely or not. "We get hacked from people in China every day," Holdaway says. "Most systems are pretty robust but some stuff gets through." Indeed, the received wisdom is that China has

acquired so much intellectual property from external and sometimes unwilling sources that they may not be capable of innovation. "They are still in a developmental stage using essentially Russian technology and knock-offs," says Robert Bigelow, the founder of Bigelow Aerospace, a space technology company in Las Vegas.

However, on closer inspection this picture seems incomplete. Granted, as Bigelow points out, China's Shenzhou space capsule looks nearly identical to Russia's Soyuz capsule. And beneath Chinese spacesuits, taikonauts often wear an inner pressure suit made in Russia. And yes, Jade Rabbit looks like an updated version of Lunokhod 2, a Soviet rover that landed on the moon in 1973.

Long march

Many of these similarities stem from a deal that took place in the mid-1990s, when China purchased much of Russia's human spaceflight technology, including Soyuz capsules, spacesuits, life support, and docking systems. However, China has made vast improvements to the original designs. For example, the Shenzhou capsule is roughly 30 per cent larger, with solar panels, advanced avionics and electronics. "China has developed what the next generation would have been," says Leroy Chiao, a former US astronaut.

Other crucial improvements, however, are not incremental – China has leaped ahead of other countries, thanks to basic science. For example, to operate a rover successfully on the moon, Chinese engineers had to make it impervious to lunar soil, an incredibly sharp, fine-grained, and sticky substance that nearly scuttled the Apollo missions. To test rover prototypes without advice from countries with access to fake moon dust, Chinese scientists developed their own simulated lunar soil from scratch. They did it using only a tiny sample of moon rock acquired decades earlier from the US, says Yongchun Zheng, a planetary scientist at the Chinese Academy of Sciences in Beijing.

China's rocket technology has a similar tale to tell. Its Long March rockets are an original design, and quickly became more advanced than Russian rockets, which have changed very little over the years, relying primarily on kerosene, a low-power but easy-to-use fuel source. The Long March 3 – which sent the Jade Rabbit on its path to the moon – uses a more advanced hydrazine and dinitrogen tetroxide fuel. "It's something the Russians have tended to stay away from," says McDowell. "It has more oomph but it's harder to work with." He refers to the Chinese success with this fuel as a "high-tech achievement".

And so, thanks to these and other rapid advances in China's space programme, Jade Rabbit spent six weeks mapping lunar regolith before an equipment malfunction froze it in its tracks. This week, the end of lunar night will reveal whether the rover survived.

If space were simply about moon rovers, the story might end there. But China has also been busy elsewhere, developing a full suite of systems including software, satellites, and communications infrastructure with the goal of total space independence.

To communicate with its probes on previous lunar orbiting missions, for example, the country relied heavily on the European Space Agency's global deep space antenna network. But not for much longer perhaps. "The Chinese are building up their own network," says ESA's Karl Bergquist. "There is less necessity to rely on us." For the Jade Rabbit mission, China still used both networks, but depended less on ESA's.

Satellite navigation is in the middle of a similar overhaul. China is a little less than halfway done with BeiDou, its answer to the GPS satellite navigation system. As of today, 15 navigation satellites are in orbit with plans for 20 more by 2020.

Indeed, satellite technology is where the country really shines. In 2010, China demonstrated its capacity for precision manoeuvrability when two satellites appeared to rendezvous and briefly touch before continuing on their separate ways. "It's one thing to simply come screaming in at high speed and bounce off or destroy the other," says Cheng. "But to come in, nudge something and back off is indicative of very high-end technology and very highly advanced skill sets." A satellite this sophisticated could repair other ageing satellites to stop them becoming space junk – or help assemble a space station.

Indeed, a second space lab will be in low-Earth orbit by 2015, placed there by the next-generation Long March 5 rocket, capable of lifting 600 kilograms more than the now-retired US space shuttle. A full-scale Chinese Space Station (CSS) will join it by 2020. A report published by the Chinese Academy of Sciences spells out China's next steps, which include a crewed lunar base – a goal Holdaway considers reasonable – a human mission to Mars, and robotic planetary exploration by 2050.

For a country that has yet to set foot on lunar soil, such projections may seem unrealistic. But China's long and persistent march is not the only reason to believe the road map: the country also possesses at least two resources no other country can compete with. The first is people. "A quarter million people are working on their space programme," says Holdaway. And these scientists and engineers are young, says Gregory Kulacki,

China expert at the Union of Concerned Scientists based in Washington DC. Echoing the idealistic, young NASA culture of the 1960s, he says, "the average age is low 30s, which is 20 years younger than other countries' programmes."

Another key to China's present and future success is the unique ability – granted by one-party rule – to stick to their plans longer than the political cycles of most Western governments. "The Chinese have a long-term plan and they're willing to devote resources to it," says Cheng. "I don't just mean money, I mean human resources, industrial resources, and political resources. Eventually we should expect they will surpass us."

But perhaps the most important catalyst for Chinese innovation was being frozen out of international collaboration. The US strictly forbids their scientists, astronauts, and aerospace contractors from collaborating with China in space, citing concerns that the country would co-opt any shared technology.

Being barred from sending astronauts to the US-led International Space Station (ISS) led China to develop its CSS. Similar examples abound. It was only after the European Union ended Chinese participation in the Galileo project – the European rival to GPS – that China began working on BeiDou in earnest. Its exclusion from the party also accounts for much of China's rapid advancement in satellite development – access to which has been most heavily restricted by other countries. "They decided to rely on their own technology," Kulacki says. "They have advanced faster because of the sanctions."

Global effects

And even as China is busy developing its capacity in space, the abilities of existing space powers are on the wane. "It is not clear that the United States' rate of technological improvement will continue as you look 10 to 20 year out into the future," McDowell says. He cites budget cuts, political gridlock, and failing educational systems. Much existing US and European space infrastructure is also ageing.

To hedge its bets, ESA is now positioning itself to partner with China in human space flight. "We have currently three or four astronauts and astronaut trainers who are in language training," says ESA's human spaceflight director Thomas Reiter. "We are taking steps to intensify our links with the Chinese Space Agency."

But what's in it for China? After decades of being shut out of collaboration, Cheng says China may be at a point where it would prefer to continue going it alone. "It's not at all a given that China wants to cooperate with us. Given the US hiatus on manned space flight, it's not at all clear what we would bring to the table," he says.

Collaboration with Russia may be equally unattractive. In 2011, Russia launched a Chinese space probe to Mars as part of its Phobus-Grunt mission, but the Russian spacecraft never made it out of Earth's orbit. "From the Chinese perspective, it was a high-visibility, high-prestige project that failed because of the Russians," Cheng says.

Indeed, the shifting balance of space powers could have all manner of unexpected consequences. The Pentagon recently acknowledged that the US military command in Africa now relies on a Chinese satellite for communications, reflecting the military's ever-larger appetite for bandwidth, which has surged in recent years as it relies increasingly on remotely operated drones and satellite radio communications.

For the same reason, many commercial applications will benefit from Chinese satellite development, such as smartphones, which can already access both GPS and its Russian alternative, GLONASS, as a backup. BeiDou would offer a third option. While GPS is robust, it has been vulnerable to jamming, causing chaos at airports from San Francisco to New Jersey and leading to widespread concerns about overreliance on the system. A significant number of car manufacturers are also reportedly equipping their systems to access BeiDou in case of GPS failure.

Then there's the US's ageing weather satellite infrastructure, a topic subject to annual congressional hand-wringing. Last year a controversial government report found that the agency's best alternative would be to turn to China for help.

But these are not the only ways China's space dominance could affect the world. For one thing, it might motivate other countries to reinvest in their languishing space programmes. On 9 January, shortly after the Jade Rabbit landing, the US administration announced at a space conference that funding for the ISS would continue for four additional years. While McDowell doubts that the landing had anything to do with the decision, officials could well have cancelled the ageing space station's $3 billion a year funding. Chiao is sure the spectre of the CSS influenced the decision not to. "There was a threat that we were going to sit on the sidelines as all of our partners go over and start working with China," he says.

But perhaps the most utopian consequence of China's space ambitions would be a renewed realisation that space is not divided according to national boundaries. At the same forum, US deputy secretary of state

William J. Burns announced an international space road map aiming to unite the separate paths of the national space agencies. "It didn't say 'except China'," says Chiao, noting that this is a subtle but significant departure.

The road map, Burns told the assembly, would create realistic prospects for long-shot projects commonly considered too expensive for individual governments to undertake, such as human missions to the surface of Mars, and an asteroid defence shield. In any case, none of this can happen without China, says Holdaway. "My educated guess is that the US, which can't afford to go to Mars on its own any more than ESA can, will initiate some dialogue with China about a global human mission," he says.

Stranger things have happened: Chiao points out that US cooperation with Russia was thought similarly unthinkable – right up until the moment it happened.

Table of Contents

Cyber Warfare and Information Security For India

By Asif Ahmed, EurasiaReview, February 16, 2014

"The defence forces on their part have adopted information warfare doctrines, which include infosec as a vital element. There is a growing partnership between defence and private industry to evolve IT security solutions for the defence information infrastructure….As defence reliance on commercial off the shelf technology (COTS) grows, the dilemma of selecting an appropriate vendor has been to a large extent addressed by the CII [Confederation of Indian Industry] online defence directory—a web-based listing of Indian software vendors working on defence related systems and applications." – Lt. Commander Prashant Bakshi, "Security Implications of a Wired India: Challenges Ahead" Strategic Analysis, April 2001

Introduction

Security analysts are predicting that 2013 is when nation-sponsored cyber warfare goes mainstream — and some think such attacks will lead to actual deaths. In 2012, large-scale cyber attacks targeted at the Iranian government were uncovered, and in return, Iran is believed to have launched massive attacks aimed at U.S. banks and Saudi oil companies. At least 12 of the world's 15 largest military powers are currently building cyber warfare programs, according to James Lewis, a cyber security expert at the Center for Strategic and International Studies. So a cyber Cold War is already in progress. But some security companies believe that battle will become even more heated this year. The U.S. has already put would-be attackers on notice. Defense Secretary Leon Panetta said recently that the United States reserves the right to use military force against a nation that launches a cyber attack on the country.

Even if hackers aren't capable of killing with a cyber attack, there is no doubt that they've become more destructive1. Cyber attacks pose more than a theoretical challenge to the Indian government's day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi's nuclear weapons test and in the confrontation with Pakistan over Kashmir. The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations.

An IT roadmap, enumerating a comprehensive ten year plan, was published. In the framework of the roadmap, the government has granted permission for closer government/industry cooperation to leverage the output of India's world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established. According to journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies2.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through siloed ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialised has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as an NW (network) created by academics for the use of the military, it has now become a global social and economic and communications platform.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which the number of Internet users has doubled between 2005 and 2010 and surpasses two billion. Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage. The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users.

While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other3. In our research, we found that experts employ diverse definitions of cyber warfare, depending on the weight or emphasis accorded to various actions, actors, and intent. We attempted to minimize the all-encompassing and academically confusing expression “information warfare” to describe electronic attacks.

In this document, we also eschew other terms, such as information operations, electronic warfare, “hacktivism”, information disruption, or cyber terrorism. In each of these terms there exists a common link to cyber activities, yet each term is different enough to not entirely capture or mostly miss the definition of cyber warfare4. As stated at the outset, cyber warfare, involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. In the future, if not already common practice, individual cyber warfare units will likely execute through the wires attacks against targets in a cooperative and simultaneous manner. The overall intent is to seek advantage over an adversary by compromising the integrity, confidentiality, or availability of a computing device.

Internet Governance – Challenges and Constraints

The success of the Internet has partly been attributed to its relative openness and low barriers (including minimal security features) to entry. However, the same openness, while allowing companies to flourish, has also facilitated those with malicious intent to operate with relative ease. The origins of the Internet can be traced back to the attempts by the Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense to create a communications NW that would survive a nuclear exchange between the two superpowers of the time. It was subsequently used by academia as a means of communicating and collaborating on research projects.

The uniqueness of the Internet in being an open structure with few barriers to entry is the outcome of the circumstances in which it was conceptualised and a result of the worldview of its initial champions. Though a military project, its very nature of being a communications project plus the fact that it was quickly adopted by academics as a means of collaboration led to a quick crossover to the civilian domain. The fact that the technology did not belong to any one company saw the implementation of standards for its various protocols, which was responsible for continuing innovation and improvements of its capabilities.

In the early stages of development of the Internet, much of the task of developing cyberspace was in the hands of line organisations such as the Department of Information Technology (DIT) at the national level or the ITU at the international level, and other expert bodies. While these organisations were competent in their own right, they were unable to bring a holistic perspective to the issue, given their domain-specific focus on issues. This also resulted in fragmented approaches to cyber security, dictated by different requirements and priorities at different points in time.

Among the many institutions that came up and have endured are the Internet Engineering Task Force (IETF), set up in 1986. It comprised a number of experts on various aspects of the Internet who worked through a cooperative consensus-based decision-making process. The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998 on similar principles to manage the Domain Name System (DNS), another key infrastructure of the Internet. Most of the ICANN’s powers and functions were devolved to it by the US government, which hitherto controlled DNS. The multistakeholder approach to discussing the development of the Internet that was institutionalised though these organisations was further carried forward in the UN-sponsored series of conferences beginning with the World Summits on the Information Society held in 2003 and 2005, and ultimately resulting in the Internet Governance Forum (IGF), convened by and reporting to the UN Secretary General.

The US has had a major influence on the development of cyberspace by virtue of the fact that much of the initial infrastructure and use was centered in that country and it continues to be a major force in its development and use. The US has thus been in a position to fend off periodic attempts to challenge its supremacy, and those times when it has been forced to shed some of its control, as in the case of ICANN, it has done so very reluctantly. Though it has been a participant in multilateral fora, the United States’ agenda invariably has been to ensure that its dominant position is not disturbed. More recently, approaches to cyberspace have taken on ideological hues, with countries ultimately seeking to gain effective control over deciding the form and shape of cyberspace within their national boundaries.

The jockeying for influence to impact Internet governance issues has seen increased activity in recent times. Most of these have taken place at the multilateral level, with countries forming coalitions and introducing resolutions at multilateral fora. While Russia has been introducing resolutions on cyber security at the United

Nations since 1998, it recently joined hands with China, Tajikistan and Uzbekistan to introduce an "International Code of Conduct for Information Security" (ICCIS). Some of the clauses within this resolution have been criticised as an attempt to increase control over content and information in the guise of securing cyberspace. Proposals by the IBSA forum (India, Brazil, South Africa) have also been seen with similar scepticism.

One of the unstated goals of the recent Cyber Security Summit held by the British government would be seen as an effort on the part of the advanced economies to regain the initiative in drawing up norms for cyberspace that highlight core Western values5. Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003. Though the rate of growth has slowed subsequently, with Internet users now approximately numbering 100 million, exponential growth is again expected as Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%. The target for broadband is 160 million households by 2016 under the National Broadband Plan6.

The Indian Cyberspace Scenario

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three N/Ws (networks) were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) N/W for public sector organisations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities. Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003. Though the rate of growth has slowed subsequently, with Internet users now approximately numbering 100 million, exponential growth is again expected as Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%.The target for broadband is 160 million households by 2016 under the National Broadband Plan.

Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India7. Similar figures have also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites. An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India's top e-commerce retailer, saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million)8.

Cyber Threats

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets: cyber espionage, cyber terrorism, cyber crime and cyber warfare.

- Cyber Crime
- Cyber terrorism
- Cyber Espionage
- Cyber warfare

Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.

Cyber Crime

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber crime being in billions of dollars worldwide. While other countries are reporting enormous losses to cyber crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage. Though the report of the National Crime Records Bureau (NCRB) for 2010 reported an increase of 50% in cyber crime over the previous year, the numbers were quite small in absolute terms. The total number of cases registered across various categories was 698; but these low numbers could be because cyber laws have proved ineffective in the face of the complex issues thrown up by Internet. As a case in point, though the cyber crimes unit of the Bengaluru

Police receives over 200 complaints every year, statistics show that only 10% have been solved; a majority of these are yet to be even tried in the courts; and the cases that did reach the courts are yet to reach a verdict since the perpetrators usually reside in third countries.

Even though the Information Technology Act (IT Act) 2000 confers extraterritorial jurisdiction on Indian courts and empowers them to take cognisance of offences committed outside India even by foreign nationals provided "that such offence involves a computer, computer system or computer network located in India", this has so far existed only on paper. Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere. Companies attribute this to the primacy placed on information assurance in the outsourcing business. Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such as the establishment of the Data Security Council of India (DSCI) and the National Skills Registry. The Indian government has also aided these initiatives in a variety of ways, including deputing a senior police officer to NASSCOM to work on cyber security issues, keeping the needs of the outsourcing industry in mind. That said, cyberspace is increasingly being used for various criminal activities and different types of cyber crimes, causing huge financial losses to both businesses and individuals. Organised crime mafia has been drawn to cyberspace, and this is being reflected in cyber crimes gradually shifting from random attacks to direct (targeted) attacks. A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets. The vast amounts of money lubricating this ecosystem is leading to increased sophistication of malicious codes such as worms and Trojans.

The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars. At the other extreme, components of critical infrastructure such as Programmable Logic Control (PLC) and Supervisory Control and Data Acquisition (SCADA) systems were targeted by the Stuxnet malware that attacked supposedly secure Iranian nuclear facilities. Stuxnet exploited five distinct zero-day vulnerabilities in desktop systems, apart from vulnerabilities in PLC systems, and exposed the grave threat to critical infrastructure such as nuclear plants and other critical infrastructure. Cyber criminals are using innovative social engineering techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage.

While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber crime, as evinced by the increasing number of complaints on consumer complaint forums. The low levels of computer security are also apparent in recurring statistics that show that India is the third-largest generator of spam worldwide, accounting for 35% of spam zombies and 11% of phishing hosts in the Asia-Pacific-Japan region. Over 6,000,000 computers were part of both NWs. India ranked first in the Asia-Pacific region and contributed 21% to the regional total. A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average. According to CERT-In, India sees an average of 788 bot-infected computers per day. With regard to web-based attacks, India has seen a significant increase and has ranked seventh, with 3% of the world attacks, and second in the Asia-Pacific region.

Cyber terrorism

Cyberspace has been used as a conduit for planning terrorist attacks, for recruitment of sympathisers, or as a new arena for attacks in pursuit of the terrorists' political and social objectives. Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes. From that perspective, the challenge of non-state actors to national security is extremely grave. The shadowy world of the terrorist takes on even murkier dimensions in cyberspace where anonymity and lack of attribution are a given. The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities, especially in the aftermath of the terrorist attack in Mumbai in November 2008.

Parliament passed amendments to the IT Act, with added emphasis on cyber terrorism and cyber crime, with a number of amendments to existing sections and the addition of new sections, taking into account these threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements. While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyber terrorism both in terms of methods and end goals.

Cyber Espionage

Instances of cyber espionage are becoming quite common, with regular reports of thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and NWs of both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. It may also be that theft of intellectual property from private enterprises is not an issue here because R&D expenditure in India is only 0.7% of GDP, with government expenditure accounting for 70% of that figure. Companies are also reluctant to disclose any attacks and exfiltration of data, both because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public. As far as infiltration of government NWs and computers is concerned, cyber espionage has all but made the Official Secrets Act, 1923 redundant, with even the computers in the Prime Minister's Office being accessed, according to reports.

The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult; governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive networks, and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exfiltrated.

Cyber Warfare

There is no agreed definition of cyber warfare but it has been noticed that states may be attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. Mainly, it refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. The attacks on the websites of Estonia in 2007 and of Georgia in 2008 have been widely reported. Although there is no clinching evidence of the involvement of a state in these attacks, it is widely held that in these attacks, non-state actors (e.g. hackers) may have been used by state actors. Since these cyber attacks, the issue of cyber warfare has assumed urgency in the global media. The US has moved swiftly and set up a cyber command within the Strategic Forces Command and revised its military doctrine.

In the latest official military doctrine, the US has declared cyberspace to be the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. It is almost certain that other countries will also respond by adopting similar military doctrines. The issue whether cyber attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated.

Multilateral discussions are veering around to debating whether there should be rules of behaviour for state actors in cyberspace. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution. There is, however, ongoing debate between those who believe that cyber warfare is over-hyped and those who believe that the world is heading towards a cyber Armageddon. Both sides have valid arguments, but even as that debate continues, cyber warfare as a construct has become inevitable because the number of countries that are setting up cyber commands is steadily growing.

These commands have been accompanied by efforts at developing applicable military doctrines. There is, therefore, a pressing need to think about norms for cyber warfare, whether the laws of armed conflict (LOAC) can be adapted to cyber warfare, and how principles like proportionality and neutrality play out in the cyber domain. Current rules of collective security such as Article 41 of the UN Charter and Chapter 7 are found wanting in the context of cyber warfare, particularly when it comes to the rapidity of cyber attacks, and the inordinate time it takes for decision making and action under these rules9.

The Need to be Prepared for Cyber War

The growing threat of cyber warfare has not been well appreciated or sufficiently understood. Cyber warfare is a term that has been loosely used to describe almost all events in cyberspace, irrespective of perpetrator, motive or scale. Cyber warfare forms a part of Information War (IW), which extends to every form of media, and inter alia includes aspects of propaganda and perception management. Cyberspace, though technically restricted to the Internet, is now increasingly linked by convergence to every communication device. With

greater connectivity, this divide is narrowing and every citizen or aspect of life is vulnerable. It is also an important constituent of NCW.

The cyber realm, like the universe, is expanding and it is estimated that by 2015 there will be almost double the number of devices connected to the Internet as there are people. The scope for exploitation by inimical elements, ranging from mischievous hackers, to criminals, terrorists, non-state actors as also nation states, is thus unlimited. The damage could be immense and many countries are pressing ahead and taking steps to build capabilities and capacities for defending themselves, as also taking offensive action in cyberspace.

The United States was the first country to formally declare this as the fifth domain warfare after land, sea, air and space. It has also formally classified the use of cyberspace as a "force", a euphemism for offensive capability. The Chinese adopted the concept of "informationalisation" in the mid-1990s and have relentlessly built up structures and operations in this domain. Consequent to the raising of the US Cyber Command (USCYBERCOM), South Korea followed with the creation of a Cyber Warfare Command in December 2009. This was also in response to North Korea's creation of cyber warfare units. The British Government Communications Headquarters (GCHQ) has begun preparing a cyber force, as also France. The Russians have actively been pursuing cyber warfare. In 2010 China overtly introduced its first department dedicated to defensive cyber warfare and information security in response to the creation of USCYBERCOM.

The race is thus on. India is a target. There have been numerous incidents of sensitive government and military computers being attacked by unknown entities and information being stolen. A group, which called itself the Pakistan Cyber Army, hacked the Central Bureau of Investigation website in December 2010. Further mocking India's cyber security the same group of hackers raided the Bharat Sanchar Nigam Limited website a few months later. Earlier this year, Pakistan-based hacker groups hacked 112 Indian websites in a span of three months leaving India red-faced. The panic that spread after the Assam violence because of images uploaded from Pakistan that caused thousands of people from the northeast to flee Bengaluru is a matter of grave concern. However, little has been done to put the national cyber security policy in place.

Union Home Secretary has accused websites in Pakistan of spreading false rumors and that investigators had found that most of the websites used images of people killed in cyclones and earthquakes and passed them off as Muslims killed in violence earlier this year to spread fear of revenge attacks. This clearly is the biggest instance of cyber warfare on India in recent times and the threat continues not only from Pakistan but also from China. While China looks to snoop into important defence information, Pakistan on the other hand defaces Indian websites and uses Indian networks to spread hatred via cyber space.

The greatest threat comes from the Pakistan Cyber Army and from a group called the Team_H4tr!ck, which have been largely responsible for hacking Indian websites. Both these groups in the past have hacked the BSNL website and claimed to have gained access to users' information, which included names, e-mail addresses, phone numbers and location details. Investigators had pointed out then that the database that they managed to collect could have been used for subversive activities. Pakistan has engaged in a cyber war since 1998 and since then created many groups to hack into websites of developing nations especially India. There have been several attempts by Pakistani hackers to hack into the Bhabha Atomic Research Centre website. Groups such as the armyinkashmir, Pakistan G Force, Pakistan Cyber Army, Pakistan Hackers Club have targeted nearly 500 websites while Indian hacker groups have made 40 such attempts.

Moreover, social media today is a favourite tool of terror groups to spread jihad. Recently, investigations into the Indian Mujahideen and its activities revealed that encrypted messages have been passed on through social media. The IM during the Delhi blasts used networking sites to create fake accounts. Not only did they share information between each other but also managed to conduct a recruitment drive. During this investigation, it was also found that the IM had been using lesser-known websites to communicate. According to experts, the National Cyber Security Policy is not fully in place. In addition to this, our servers are vulnerable. Moreover, Pakistan-based hackers are completely funded by its intelligence and unlike their counterparts in India they are fully protected. There has been a lot of intelligence regarding Pakistan groups using the social media and other websites to create panic. It was in this context that the Rs 800-crore National Cyber Coordination Committee was mooted. The NCCC will monitor content on social media and pass on information to intelligence agencies. Experts however feel that these are organisations are controlled by the government and this would lead to red-tapism. Although India does have a cyber army, many feel that they need more patronage from the government.

The frequency and intensity of such episodes is increasing. There is enough evidence to suggest that this is the action of nation states either directly or through proxies. There have also been cases of offensive action such as reports of shutting down of power systems. Such attacks on critical infrastructure either singly or in multiples are of serious concern, especially with respect to national security. The draft National Cyber Security Policy (NCSP) mainly covers defensive and response measures and makes no mention of the need to develop

offensive capacity. This is a must if we are to ensure capability for self-defence granted under Article 51 of the UN Charter.

This leads to the question: what is cyber warfare?

In the absence of a formal definition of cyber warfare, we may define it as “actions by a nation-state or its proxies to penetrate another nation’s computers or networks for the purposes of espionage, causing damage or disruption”. These hostile actions against a computer system or NW can take two forms: cyber exploitation and cyber attacks. Cyber exploitation is in a manner nondestructive and includes espionage. It is usually clandestine and is conducted with the smallest possible intervention that allows extraction of the information sought. It does not seek to disturb the normal functioning of a computer system or NW. The best cyber exploitation is one that a user never notices. These are silent and ongoing, and as mentioned earlier, have shown an upward trend. Cyber attacks on the other hand are destructive in nature. These are deliberate acts of vandalism or sabotage – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy an adversary’s computer systems or NWs or the information and programs resident in or transiting these systems or networks. Actors in both types of activities cover a wide range, as mentioned earlier. Of these, nation states and their proxies are of the greatest concern. For easier understanding, the domains of cyber warfare may broadly be classified as:

- Espionage and National security breaches
- Vandalism
- Sabotage

Espionage and national security breaches

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers. Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. Specific attacks on the United States have been given codenames like Titan Rain and Moonlight Maze. General Alexander notes that the recently established Cyber Command is currently trying to determine whether such activities as commercial espionage or theft of intellectual property are criminal activities or actual “breaches of national security10.”

Vandalism

Defacing web pages or use DDOS to take them down. Such actions were evident in Estonia or Georgia.

Sabotage

This has the most serious implications and includes DDOS, destruction of data, insertion of malware and logic bombs. It also encompasses actions in war such as those taken for preparation of the battlefield. Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromisation of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption.

According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market. In mid July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered “the first attack on critical industrial infrastructure that sits at the foundation of modern economies,” notes The New York Times11.

Denial-of-service attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

Electrical power grid

The federal government of the United States admits that the electric power transmission is susceptible to cyberwarfare. The United States Department of Homeland Security works with industry to identify vulnerabilities and to help industry enhance the security of control system networks, the federal government is also working to ensure that security is built in as the next generation of “smart grid” networks are developed. In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left

behind software programs that could be used to disrupt the system, according to current and former national security officials. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack. China denies intruding into the U.S. electrical grid. One countermeasure would be to disconnect the power grid from the Internet and run the net with droop speed control only. Massive power outages caused by a cyber attack, could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

Howard Schmidt, Cyber-Security Coordinator of the US, commented on those possibilities: It's possible that hackers have gotten into administrative computer systems of utility companies, but says those aren't linked to the equipment controlling the grid, at least not in developed countries. [Schmidt] has never heard that the grid itself has been hacked12.

Military

In the U.S., General Keith B. Alexander, first head of the recently formed USCYBERCOM, told the Senate Armed Services Committee that computer network warfare is evolving so rapidly that there is a "mismatch between our technical capabilities to conduct operations and the governing laws and policies. Cyber Command is the newest global combatant and its sole mission is cyberspace, outside the traditional battlefields of land, sea, air and space." It will attempt to find and, when necessary, neutralize cyber attacks and to defend military computer network.

Alexander sketched out the broad battlefield envisioned for the computer warfare command, listing the kind of targets that his new headquarters could be ordered to attack, including "traditional battlefield prizes – command-and-control systems at military headquarters, air defense networks and weapons systems that require computers to operate13."

One cyber warfare scenario, Cyber ShockWave, which was wargamed on the cabinet level by former administration officials, raised issues ranging from the National Guard to the power grid to the limits of statutory authority. The distributed nature of internet based attacks means that it is difficult to determine motivation and attacking party, meaning that it is unclear when a specific act should be considered an act of war. Other cyberwarfares caused from political motivations can be found worldwide. In 2008, Russia began a cyber attack to Georgian government website, which was carried out along with military operation in South Ossetia. In 2008, Chinese 'nationalist hackers' attacked CNN as CNN announced on Chinese repression on Tibet14.

Neighbour Countries's Cyber War on India

India has been facing cyber warfare for a long time. In the absence of adequate cyber security in India, cyber attacks and cyber warfare are posing real danger to India. As on date, India is vulnerable to cyber warfare. As on date we have no cyber warfare policy of India. As on date we have no implementable cyber crisis management plan of India15.

In August 2010 the Indian government told its agencies to enhance their capabilities in cyber warfare. The strategy directed government agencies to develop capabilities to break into networks of unfriendly countries, set up hacker laboratories, set up a testing facility, develop countermeasures, and set up CERTs for several sectors. The agencies at the forefront of this strategy were the National Technical Research Organization, the Defense Intelligence Agency, and the Defense Research and Development Organization. Not long after the strategy was announced, India discovered a Chinese variant of the Stuxnet worm in Indian installations. India has since stepped up efforts in its offensive cyber capabilities. In December 2010 hackers from the Pakistan Cyber Army defaced India's Central Bureau of Investigation, which was supposed to be one of the nation's most secure websites. This attack caused the Indian government to call for increased capabilities in cyber security. The increasing focus on cyber security is evident through the planning of India's second cyber warfare conference, which will be held in November 2011.

A government-private sector plan being overseen by National Security Advisor (NSA) Shivshankar Menon began in October 2012, and intends to beef up India's cyber security capabilities in the light of a group of experts findings that India faces a 4.7-lakh shortfall of such experts despite the country's reputation of being an IT and software powerhouse16.

The next generation of warfare, the cyber war, can not only disrupt data-links, electronic devices and networks, but can also create panic by use of the social media as we witnessed in the mass exodus of people of North-East from Bengaluru, Hyderbad and Pune recently. The Pakistani Military Establishment, including ISI, is frustrated with its inability to create problems in Kashmir and the lowering of intensity of insurgencies in the North-East. They feel that in spite of their best efforts, these areas are slipping out of their hands permanently.

The Pakistan Military lost major wars with India. To offset such losses, they started a proxy war through covert means with the help of export of terrorism. Despite every effort, the proxy war also appears to be failing, as India moves on. Now with the help of their Irregular Forces consisting of the jihadi groups, it has decided to create havoc with the help of internet and the social media. First, their websites culled out photographs of violence and disasters from different countries and morphed and uploaded to show violence against Muslims in Myanmar and Assam. Second, they used SMS messages through their sleeper cells in India to circulate threat to all the North-East people working in major cities like Bengaluru, Hyderabad, Pune Delhi etc. The result was that there was mass exodus from these cities due to the threat posed in these messages.

In other words, Pakistan successfully used the next generation warfare, i.e. 'Cyber War' and managed in creating a false perception of insecurity amongst the people from the northeast, as well as spread of disaffection. Unfortunately, the Indian intelligence agencies, the local police and the government at large were fairly clueless. The result was almost half a million people in panic left for their hometown in Assam. The government response was pathetic – it lodged a protest with Pakistan. Pakistan's home ministry as usual, rejected the Indian protest and asked for proofs for investigations.

In the past 65 years, Pakistan has never accepted our legitimate concerns and yet New Delhi, to gain time and avoid criticism, 'passed the buck' once again. In peacetime, if an adversary can with ease manipulate perceptions with the help of cyber space, just imagine the danger that India faces in times of war. The fly-by-wire fighter aircrafts can be neutralized. Missiles instead of firing on the enemy can be redirected to destruct within. The electricity grids can be disrupted and that will create mayhem from hospitals to airports.

Fake orders can be passed to military units as also nuclear strategic command. The television transponders can be imposed with false news to create panic in the country. The subverted networks will bring to halt the bank transactions. The jamming of telephone lines can leave the civil government and the military blind, and the people gasping. The result will be rumors, panic, and chaos. The only successful defence in any war is offence, whether it is conventional, overt or covert or cyber war. The enemy will always use the next generation warfare, i.e. cyber war as the first instrument to neutralize us before it launches its military forces. The cyber war will be used to soften the target, just like artillery is used by the Army. Government's policy therefore should be based on twin principles, namely that India's cyber army should be able to defend networks, data links and electronic devices, and at the same time launch counter attack on the enemy. India fortunately boasts of a young demographic profile, which is IT savvy. Therefore, New Delhi can raise one of the best Cyber Armies in the world. The answer does not lie in shutting down the social media as demanded by many ignorant, but in wielding the weapons of the 21st century in a far superior fashion that can outwit the adversary17.

Cyber War: Fifth Domain of Warfare

The cyber warfare that this section addresses is that which is practised mainly by nation states or their proxies. The potency of this threat has compelled almost every country to develop capabilities in the cyber domain, as is the case for land, air, sea and space. According to Spy Ops, by the end of 2008 nearly 140 countries possessed varying degrees of cyber attack capabilities. In addition, an unknown number of extremist groups and non-state actors have developed or acquired cyber weapons.

Some commercially available products are flexible enough to be classified as dual purpose – security testing tools and weapons of attack. Thus some organisations have or are developing cyber weapons and cloaking them as security testing tools. All this is classified information and each nation works on its own. An assessment of cyber warfare threat matrix by the USA, which covered over 175 countries and organisations, made a watchlist in which the top ten in order of priority were: China; Russian business network; Iran; Russia tied with France; extremist/terrorist groups; Israel; North Korea; Japan; Turkey; and Pakistan. India on its growth path is vulnerable. Located in an unstable region where the larger neighbours possess this capacity, it is logical to assume that the country is under serious threat and constant attack. The impact on national security is thus serious and such that all institutions and organs of the state must jointly work to counter this challenge. In order to understand the challenge, the following issues need to be addressed:

- Coordination
- Defining Objectives and Doctrine
- Proactive Cyber Defence
- Critical Infrastructure
- Legal Provisions18

Coordination

It is appreciated that in keeping with current needs, the Defence forces, DRDO (Defence Research and Development Organisation), NTRO (National Technical Research Organisation), CERT-In (Computer Emergency Response Team India), RAW (Research and Analysis Wing), IB (Intelligence Bureau), C-DAC (Centre for Development of Advanced Computing), Ministries, NIC (National Informatics Centre), NASSCOM (National Association of Software and Services Companies), private industry et al. have to work in concert. The impact of this on every aspect of electronic media requires a coordinated and integrated approach. Given its all encompassing nature, it also follows that control of all cyber and IW (Information Warfare) activities at the national level must fall under the purview of the NSC and controlled by its Secretariat i.e. the NSCS. Within this lead agencies for executing offensive cyber operations interalia could be the NTRO, CIDS (Chief of Integrated Defence Staff) and the DRDO.

Defining Objectives and Doctrine Application

Defining Objectives and Doctrine Application of such measures must be in accordance with clearly defined objectives that would be in keeping with customary international law and practice. The primary objective would be to garner knowledge to find how systems are breached and thus provide the ability for defensive measures to be developed and put in place. There is a further argument that it must be visible as an armour of selfdefence so as to deter an attack. While this capability will be ambiguous, subtle signals and clear definition of objectives will lend credibility. Moral arguments stand thin in the face of realities. There is therefore a need to lay down the objectives and include them in the draft NCSP (National Cyber Security Policy) or issue a doctrine in this regard.

Proactive Cyber Defence

This comprises actions taken in anticipation to prevent an attack against computers and NWs. As opposed to the current practice of passive defence, it provides a via media between purely offensive and defensive action: interdicting and disrupting an attack, or an adversary's preparation to attack, either pre-emptively or in self-defence. Proactive cyber defence will most often require operationalising upstream security mechanisms of the telecommunications or Internet providers. The most compelling reasons for a proactive defence can be couched in terms of cost and choice. Decision-makers will have few choices after an impact, and all of them are costly to start with. Proactive defence is thus the key to mitigating operational risk. The USA had set up a Proactive Pre-emptive Operations Group (P2OG) in 2002. Such actions thus find international acceptability.

Critical Infrastructure

There is a need to prioritise and protect critical infrastructure. In the USA 18 sectors have been identified. In India's case, the sectors of power, water supply, communications, transportation, defence and finance are vital constituents of national security. These need to be defined and suitable protection measures ensured as laid down in the IT Act. Steps to guard against threats, i.e. destructive actions or cyber exploitation will constitute a basis for research on offensive action. The electric power system merits top priority. While the risk of an attack can be reduced, it would be unrealistic to assume that an attack can be prevented. This leads to the conclusion that containment, isolation, minimising the impact, backup systems and reactivation are areas of capacity building. The debate on which agency will undertake this in India rages and begs immediate resolution. As critical infrastructure spans both the public and private domains, the organisation to ensure its protection has to be in the public realm and, in a manner, accountable.

Legal Provisions

The IT Act of 2008 covers all actions in this domain. Sections 69, 69A and 69B contain provisions for intercepting, monitoring or blocking traffic where, amongst other reasons, there is a threat to national security. Section 70A covers protection of critical infrastructure. There is a need to work within these provisions. LOAC (Laws of Armed Conflict) provide the primary legal framework within which one can analyse constraints for offensive cyber operations. Immunity for actions taken against another nation, institutions, hostile group or individual is possible if taken under LOAC or for selfdefence under Article 51 of the UN Charter. The cyber realm, with scope of non-attributable actions as also ease of deniability, provides immense scope for exploitation. The fact that there are no international cyber laws or treaties at present is also used to advantage. Offensive cyber operations by their very nature have to remain in the grey realm and restricted. Each nation would thus determine the structure best suited to its needs. However, the necessity to clearly enunciate such measures or self-defence actions in a doctrine as also the NCSP is essential for steps in this regard; it also acts as an element for deterrence. The emphasis must remain on protecting NWs, systems and users.

Controversy over terms

There is debate on whether the term “cyberwarfare” is accurate. In October 2011, for instance, the Journal of Strategic Studies, a leading journal in that field, published an article by Thomas Rid, “Cyber War Will Not Take Place.” An act of cyber war would have to be potentially lethal, instrumental, and political. Then not one single cyber offense on record constitutes an act of war on its own. Instead, all politically motivated cyber attacks, Rid argued, are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion19.Howard Schmidt, an American cybersecurity expert, argued in March 2010 that “there is no cyberwar… I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment.” Other experts, however, believe that this type of activity already constitutes a war. The warfare analogy is often seen intended to motivate a militaristic response when that is not necessarily appropriate. Ron Deibert, of Canada’s Citizen Lab, has warned of a “militarization of cyberspace.” The European cybersecurity expert Sandro Gaycken argued for a middle position. He considers cyberwar from a legal perspective an unlikely scenario, due to the reasons lined out by Rid (and, before him, Sommer), but the situation looks different from a strategic point of view. States have to consider military-led cyber operations an attractive activity, within and without war, as they offer a large variety of cheap and risk-free options to weaken other countries and strengthen their own positions. Considered from a long-term, geostrategic perspective, cyber offensive operations can cripple whole economies, change political views, agitate conflicts within or among states, reduce their military efficiency and equalize the capacities of high-tech nations to that of low-tech nations, and use access to their critical infrastructures to blackmail them20.

Meeting the Cyber Warfare Challenge

Cyber warfare encompasses government and public and private domains. As clarified earlier, this must be coordinated by the NSCS (National Security Council Secretariat). In the USA it comes directly under the White House. Thus the need to create a Directorate or Special Wing in the NSCS for this. It would oversee and coordinate both defensive and offensive cyber operations. There is also a requirement for intimate involvement of the private sector, as they are equal, if not larger, stakeholders. Regular meetings must be held and, if needed, working groups created. Current organisations which could be tasked to take on the cyber warfare challenge include the NTRO, HQ IDS (Headquarter Integrated Defence Services), DRDO, RAW and IB. Representatives of CERT, NASSCOM, etc. will invariably be involved. Each would have to function under guidelines and through proxies. This includes:

- Raising of Cyber Command
- Territorial Army (TA) Battalions for Cyber Warfare
- Perception Management and Social Networks21

Raising of Cyber Command

While cyber warfare is ongoing activity during peacetime, there is a dire need to develop this capacity for a warlike situation. Cyber warfare in a manner is NCW and will form an essential part of preparation of the battlefield in any future conflict. Such attacks may also precede the kinetic war. Building this capability will take time and must remain covert and ambiguous. It could also form part of the strategic deception process. This should be the responsibility of the Armed Forces (HQIDS) along with the DRDO and other experts. Detailed discussions and consultations in this regard require to be initiated. India must raise a Cyber Command. This will comprise not only the three services but personnel from the DRDO and scientific and technological community. It could work with the space command because many aspects overlap and would economise on resources. It will oversee all activities undertaken during peacetime, as also plan for offensive cyber operations as required, to include preparation of the battlefield. It must work in close concert with the NTRO. To determine the structure it would be prudent to study the mission and objectives of USCYBERCOM (US Cyber Command) as a guide. USCYBERCOM plans, coordinates, integrates, synchronises and conducts activities to: “direct the operations and defense of specified Department of Defense information NWs and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.” The Command is charged with pulling together existing cyberspace resources, creating synergy and synchronising war-fighting effects to defend the information security environment. It comes under the Strategic Command, which also has the Space Command as a constituent. A similar structure for India could be considered, especially as the US has evolved its structure based on experience and also because it functions as an open democracy. India already has the Strategic Forces Command, which could be augmented with both Space and Cyberspace Wings. These may be of smaller size to start with, and will develop in accordance with threats and needs. Each service has its own requirements. The structure therefore has to be need-based and flexible. The various elements of this could be:

• Army, Navy and Air Force CERTs

These would monitor traffic, disseminate information, ensure remedial measures to ensure ongoing security to networks and systems. They would also in a manner be charged with protection of critical infrastructure of each service, i.e. communication backbone, power systems, high-priority networks. The structure thus envisages a Defence CERT which works in concert with each service CERT.

• Intelligence and information operations

A Defence Intelligence Agency exists under HQ IDS. Its cyber and information operations elements could work with this command. Intelligence gathering is an accepted reality and cyberspace possibly provides the best scope for this as also information operations.

• Defence communication NWs

Each service has its special requirements and own communication directorates. Joint operations, strategic communications as also high-security NWs need to be coordinated under HQ IDS and the proposed Cyber Command.

• Cyber operations which are required for preparation of the battlefield

This again would be a tri-service organisation, with additional experts from the DRDO or any other such institution. This would include R&D.

Territorial Army (TA) Battalions for Cyber Warfare

While cyber warfare is ongoing, there are periods of heightened threat. A recent example was the Commonwealth Games, when networks were subjected to attacks. There is therefore need to create and maintain a “surge capacity” for crisis or warlike situations. Young IT professionals constitute a vast resource base and a large number would be willing to loyally serve the nation when required. This resource must be capitalised by raising of cyber warfare TA battalions similar to those for Railways and ONGC, which could be embodied when required. In addition to purely “defence” requirements these could also provide for protection of critical infrastructure.

Perception Management and Social Networks

In the current age of “democratisation” or “instant availability of information” and growth of social NWs, there is tremendous scope for perception management and manipulation of information. The year 2011 saw extensive use during the “Arab Spring” and London Riots. This media is seen as a potential tool for psychological and no-contact warfare and must form part of any offensive or defensive action. All this requires central coordination and study with respect to national security.

Capacity Building

Capacity building is vital. It must also be sustainable and of larger benefit. There is a need to create an R&D base and institutions. Growth forecasts of Internet usage, especially with e-governance, will create an employment potential for “cyber doctors” and sleuths. Just as the terrorist attack on Mumbai in November 2008 created a whole new dimension of requirement of physical security, protection of Internet usage and transactions will create millions of jobs in the near future. It will be a seller’s market for which India with its HR base must be ready. Consequently, the government must accelerate this process. Some thoughts in this regard are:

• Partnerships
• HR and R&D
• Testing and Certification
• Language Training
• Legal Capital
• Understanding Vulnerabilities
• Identification of Technologies22

Partnerships India cannot go it alone. Various past attempts have not been of much success. It has to be seen as a global issue and capacities developed.

HR and R&D DIT (Department of Information Technology) has set up the Information Security Education and Awareness (ISEA) programme with funding of Rs 100 crore. Other options which need to considered are government and public and private institutions. The Chinese models could be studied in this regard. They set up four universities for this purpose in 1999. Security of data for the BPO industry has brought up the necessity for such institutions. Talent spotting with competitions is an easy option. Programmes and competitions such as “Cyber Patriot” need to be followed up in schools and educational institutions. These

could be self-financed. Army Training Command (ARTRAC), as also the other two services, must take the lead in partnership with the private sector.

Testing and Certification The outsourcing model has affected testing and certification. Hardware and HR in this regard has to be Indian. This can then be adapted for proactive defence. Steps taken by DIT need to be implemented.

Language Training HR trained in language of our potential adversaries is a must. This must be provided suitable incentives and permanence of employment.

Legal Capital Legal aspects of developing capacities, understanding use of cyberspace as a "force", implications of the UN Charter, negotiating international laws and treaties – all of this needs trained personnel. While the legal aspects are covered in a separate section, expertise with respect to cyber warfare needs special attention.

Understanding Vulnerabilities Study of vulnerabilities both of own systems as also those of potential adversaries must be undertaken to prevent intrusion and exploit weaknesses.

Identification of Technologies There is a need to identify technologies in this regard. These should also include isolation of NWs within the country, close monitoring of gateways and backbone, identification of "zero day" vulnerabilities, protection of power grids, secure communications for defence and critical services, penetration, et al.

Efforts at prohibition of Cyberwar worldwide

The Shanghai Cooperation Organisation (members include China and Russia) defines cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". In September 2011, these countries proposed to the UN Secretary General a document called "International code of conduct for information security". The approach was not endorsed by western countries as it entailed too many hints on political censorship of the internet. In contrast, the United States' approach focuses on physical and economic damage and injury, putting political concerns under freedom of speech. This difference of opinion has led to reluctance in the West to pursue global cyber arms control agreements23. However, American General Keith B. Alexander did endorse talks with Russia over a proposal to limit military attacks in cyberspace24. A Ukrainian professor of International Law, Alexander Merezhko, has developed a project called the International Convention on Prohibition of Cyberwar in Internet. According to this project, cyberwar is defined as the use of Internet and related technological means by one state against political, economic, technological and information sovereignty and independence of any other state. Professor Merezhko's project suggests that the Internet ought to remain free from warfare tactics and be treated as an international landmark. He states that the Internet (cyberspace) is a "common heritage of mankind25." The UN has urged countries to seek a "peaceful resolution" in cyberspace to avoid the threat of global cyberwar.

Conclusion

India's armed forces have initiated a shift in military doctrine to embrace more directly offensive and defensive cyber warfare, leveraging India's strengths in IT research and software development. India has a robust hacking network. In addition, the government has announced several operational steps, such as founding a National Defense University with a key focus on computer software, and establishing a new intelligence communication and electronic surveillance agency. In parallel with these steps, India's traditional pre-occupation with protecting military secrets has given way to closer government/industry collaboration to keep pace with competitive challenges within the region and at the global level. New Delhi actively seeks military-technical and scientific cooperation and exchange with strategic partners such as Israel and Russia that reputedly possess exceptional cyber capabilities. In addition, there is significant open discussion relating to adoption of the Israeli model of military/industry strategic cooperation, i.e., a national software export strategy centered on product-supplier relationships and military hi-tech spin-offs. Understanding the threat of cyber warfare and developing capacity for offensive actions in this domain is a sine qua non. Nations, non-state actors, terrorist groups and individuals pose a challenge to growth, which is increasingly going to be dependent on the cyber domain. Cyber warfare will also be central to any hostile or conflict situation. Clearly defined objectives and national doctrine in this regard along with supporting structures and matching capabilities are thus inescapable. Even the prime Minister of India now acknowledged that India must be prepared to meet the challenges arising out of Internet and cyberspace. However, if this acknowledgement is just another speech for another occasion, we may not see any ground level action for another decade or more. Defending against cyber warfare requires maturity and skills and lots of patience. If India thinks that it can produce cyber warfare experts at the eleventh hour that would be a big blunder. India has to give attention to this aspect right now and then only it may be able to acquire necessary expertise in this regard after some years.

(Assistant Professor, Defence & Strategic Studies, Department of Political Science, Kurukshetra University, Kurukshetra, E-Mail asifahmed081@gmail.com)

References:

1. Nations prepare for cyber war, ByDavid Goldman@CNNMoneyTech, January 7, 2013 http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html

2. CYBER WARFARE – Institute for Security Technology Studies. www.ists.dartmouth.edu/docs/cyberwarfare.pdfSimilar

3. http://idsa.in/system/files/book_indiacybersecurity.pdf

4. For a discussion on the evolution of cyber warfare terminology see Lieutenant Colonel (ret.) Timothy L. Thomas, "Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory," Journal of Information Warfare, February/March 2003 pp. 109-116.

5. Ibid 3.

6. www.trai.gov.in. According to the Report for 2010 of the Telecom Regulatory Authority of India (TRAI), over 381 million mobile subscribers possessed the ability to access the Internet through their mobiles, with 35 million having accessed at least once.

7. www.comscore.com. According to Internet research firm Comscore, 62% of Internet users in India use Gmail

8. www.imrbint.com. A report compiled by the Indian Market Research Bureau (IMRB) projects domestic ecommerce to be in the region of $10 billion by the end of 2011.

9. Ibid 3.

10. "Clarke: More defense needed in cyberspace" HometownAnnapolis.com, 24 September 2010.

11. "Malware Hits Computerized Industrial Equipment" New York Times, 24 September 2010.

12. http://en.wikipedia.org/wiki/Cyberwarfare.

13. "Cyber-War Nominee Sees Gaps in Law", New York Times, 14 April 2010.

14. Steve Ragan Report: The Cyber ShockWave event and its aftermath. The Tech Herald. 16 February 2010.

15. http://cjnewsind.blogspot.in/2012/07/cyber-warfare-and-india.html

16. "5 lakh cyber warriors to bolster India's e-defence". Times of India (India). 16 October 2012. http://articles.timesofindia.indiatimes.com/2012-10-16/india/34498075_1_cyber-security-cyber-attacks-cyber-warfare. Retrieved 18 October 2012.

17. Pakistan unleashes Cyber War on India By Bharat Verma, Issue Net Edition | Date : 20 Aug , 2012

18. Ibid 3.

19. Rid, Thomas (October 2011). "Cyber War Will Not Take Place". Journal of Strategic Studies. doi:10.1080/01402390.2011.608939. http://dx.doi.org/10.1080/01402390.2011.608939. Retrieved 21 October 2011.

20. Ibid 12.

21. Ibid 3.

22. Ibid 3.

23. Tom Gjelten (23 September 2010). "Seeing The Internet As An 'Information Weapon'". National Public Radio. http://www.npr.org/templates/story/story.php?storyId=130052701. Retrieved 23 September 2010.

24. Gorman, Siobhan. (4 June 2010) WSJ: U.S. Backs Talks on Cyber Warfare. Online.wsj.com. Retrieved 8 November 2011.

25. Politik.org.ua. Retrieved 8 November 2011.

Table of Contents

Smarter Counterterrorism in the Age of Competing Al Qaeda's

By Clint Watts, Foreign Policy Research Institute, February 10, 2014

Last week Ayman al- Zawahiri, al Qaeda's global leader publicly dissolved the relationship between al Qaeda Central and the group currently known as the Islamic State of Iraq and Al Sham (ISIS) and formerly known as al Qaeda in Iraq. Zawahiri and al-Qaeda's General Command said in what was effectively a press release:

"[ISIS] is not a branch of the al-Qaeda group . . . does not have an organizational relationship with it and [al-Qaeda] is not the group responsible for their actions,"

Zawahiri's announcement comes only two weeks after Dr. Michael Doran, Dr. Will McCants and I addressed the challenges accompanying the premature designation of al Qaeda affiliates in an article entitled "The Good and The Bad of Ahrar Al Sham".

Our thesis put forth that today's terrorism threat picture looks far different than a decade ago--more complicated and subsequently more challenging to navigate. Appropriately understanding the true terrorist threats to the U.S. and the West requires in-depth analysis from multiple disciplines and an open mind to pursue counterterrorism strategies informed by the lessons learned from the past decade but not constrained by past models of al Qaeda activity.

This post and several to follow represent my assumptions and opinions on how the U.S. might push forward in counterterrorism against al Qaeda and those jihadist groups emerging from al Qaeda's wake. (These are my opinions and not necessarily shared by my co-authors Drs. Doran and McCants-–I speak only for myself here.)

The posts are meant to stir discussion and debate; I have no illusions that I have all the answers or am exactly correct in my prescriptions.

For my first post in this series, I have six assumptions and/or principles that shape my opinions to come in future posts.

■ Al Qaeda is not one big thing

Analysts and pundits should stop focusing on building links between al Qaeda affiliates seeking to present loose networks as one large insurmountable threat. Billing al Qaeda as "One Big Thing" over the past decade resulted in the U.S. pursuing strategies, such as military occupation and backing corrupt dictators, which galvanize competing al Qaeda adherents and unify disparate affiliate actions. The US should pick its fights wisely and for the greatest counterterrorism return at the lowest cost. Since Bin Laden's death, we've seen unprecedented al Qaeda infighting in Somalia, Syria and the Sahel. Rather than build new fears of an al Qaeda juggernaut, we should instead be employing our vaunted "smart power"--that's if the U.S. can act smartly rather than in a partisan manner and still has power in a region where it has pursued a campaign of disengagement in recent years.

■ All al Qaeda affiliates are not equal in intent, commitment and capability

Most all Sunni militant groups from Africa to South Asia will express some level of support for al Qaeda and targeting of the West. However, their commitment to al Qaeda and its objectives varies considerably depending on local agendas and operating environments. An upstart al Qaeda affiliate constantly weighs the costs and benefits of attacking the U.S.-–comparing the resulting credibility and support produced by a successful attack against the immediate and intense U.S. counterterrorism pressure to follow any attack. For most affiliates, its better to wave the al Qaeda banner and passively allow safe haven of "Old Guard", core al Qaeda operatives than to actively pursue their own attacks on the U.S. Beyond intent and commitment, the capability of affiliates to attack the U.S. is limited to only a few nodes. Even if an al Qaeda affiliate wanted to attack the U.S., most are limited to picking off the stray, undefended American or Westerner that floats through their area of operations. If an al Qaeda upstart affiliate lacks the commitment and capability to attack the U.S., should the U.S. expend millions of dollars to destroy ten guys waving an al Qaeda flag? I think not, most of these gun-toting disenfranchised youth do not pose a direct or immediate threat to U.S. national security. But I also don't think these upstarts should be ignored. Intelligence collection and analysis will be essential to understanding when these nascent groups cross the line and become a significant threat to the U.S.

■ Destroy al Qaeda's core, "Old Guard" network

Rather than chasing every militant from Morocco to Pakistan, the main effort should remain on the "Old Guard" al Qaeda network committed to attacking the U.S. I estimate this network consists of the following elements plus or minus a few people:

- Ayman al Zawahiri and his closest advisors of "Old Guard" al Qaeda in Pakistan. I'd estimate this to be no more than a couple dozen individuals.
- AQAP's top leadership in Yemen led by Nasir al-Wuhayshi as well as AQAP's external operations branch, which includes the talented bombmaker Ibrahim al-Asiri. Since 2005, this element has presented the most credible and significant threats to the U.S.
- al Qaeda leaders and foreign fighters embedded in al Shabaab in Somalia as an external operations force executing attacks regionally and in the West. This includes al Shabaab's top leaders (i.e., Godane and key deputies) as well as those known Western passport holders plotting attacks (see, for example, Ikrima).
- AQIM's top remaining leadership in the Sahel to prevent their reconstitution in the desert and resulting push for attacks against the West and in particular Europe (i.e., Yahya Abou el-Hammam, Sultan Ould Badi, Ould Kheiru). This includes Mukhtar Bel Mukhtar's "Those Who Sign With Blood" who have been a divisive force in AQIM, but have also demonstrated clearly their intent to attack the West.
- Jabhat al-Nusra in Syria, al Qaeda's most important affiliate today who seeks a long-run strategy of building al Qaeda's next safe haven and tapping into the greatest foreign fighter migration in history. Also in Syria, al Qaeda envoys to other group's in the Islamic Front must be interdicted or disrupted (see, for example, Abu Khalid al Suri worming into Ahrar al Sham).
- al Qaeda operatives and foreign fighters from Syria moving into Egypt that are building a jihadist force to destabilize Egypt and antagonize Israel with cross-border attacks designed to unify Islamists, Salafists and Jihadists under one banner.

In addition to these leadership elements, I also believe that the U.S. should take steps when appropriate to interdict:

- Occasional envoys dispatched from al Qaeda seeking to expand the group's influence into second-tier affiliates in Libya, Tunisia, the Sahel, Nigeria and other places.
- Americans or U.S. persons in al Qaeda or its orbit with the ability to infiltrate back into the U.S. or specifically target the U.S. homeland (see these three as examples: Abousamra, Mostafa, Gadahn).

When I hear the words "al Qaeda", I think of the above elements consisting of a few hundred "varsity" players rather than 10,000 disenfranchised young boys firing guns in the air, toting black flags and posting YouTube videos. Only a few of the smartest survivors of the Syrian jihad will be a threat to the West in the future. I'm not advocating ignoring emerging affiliates; persistent intelligence collection will be critical, but go after the bigger fish that threaten the U.S. rather than every small fish floating in the stream. Groups like ISIS may pose a threat to the U.S. and should be countered if necessary, but in the meantime, ISIS and other faltering groups hurt "Old Guard" al Qaeda as much as any U.S. action--let partners with a larger stake in defeating ISIS take the lead. Despite media stories suggesting al Qaeda's rise, I think the U.S. counterterrorism community is actually focused appropriately on the right al Qaeda targets. I hope public and Congressional pressure to fight last decade's al Qaeda won't push them off course.

■ When we designate groups as foreign terrorist organizations (FTO), we should destroy them.

During the discussion on Ahrar al-Sham, Dr. Doran, Dr. McCants and I were trying to illustrate the complications that come along with designating a group an FTO. The designation restricts U.S. options for dealing with the group in non-military ways and can actually strengthen al Qaeda's hand. For me personally, I believe in the concept of FTO designation but only if the U.S. is serious about countering the FTO. Designating a FTO and then doing nothing to destroy the group results in the FTO getting the credibility of fighting the U.S. without any adverse effects. Over the long-run, failing to destroy a FTO makes the U.S. look ineffective and weak. Designation of a FTO or foreign terrorist (FT) for that matter should come with decisive action commensurate with what one should expect from a global superpower.

■ Effective counterterrorism strategy focuses on doing a few tasks well, not several hundred tasks lightly.

Lumping each pseudo-jihadist under an all encompassing Al Qaeda banner dilutes US counterterrosm efforts resulting in a repeat of the strategic complications of the 2004-2007 era--when defeating al Qaeda could only be accomplished by solving all of the developing world's problems via a 500-700 point implementation plan spread across a massive bureaucracy. Nineteen al Qaeda hijackers executed the 9/11 attacks, not 19 million. More than twelve years after 9/11, we should look back on US counterterrorism and recognize that protecting our country and Americans overseas has come from one task far above all others: killing or capturing core al Qaeda members. Further quelling al Qaeda or what it is to become also comes via two important supporting elements: conducting counterterrorism consistent with American values (i.e., minimizing the killing of innocent bystanders, ending indefinite detention, supporting democratic principles & abandoning corrupt dictators) and maintaining dominant intelligence capabilities that help distinguish the most dangerous elements of al Qaeda for targeting separate from those more innocent and less threatening to U.S. national security. Ironically, the American public's overriding self-interest in civil liberty protection has likely rendered it more difficult for the US government to distinguish friend from foe. Lastly, putting an end to our notions of regime change via military occupation, abandonment of Arab spring dictators and renewed commitment to American values further eroded the last decade's fodder for al Qaeda's narratives. Unfortunately, the U.S. has more recently backed Arab Spring uprisings through inaction. The battle between democracy and Sharia has only just begun and further dimming opportunities for "Old Guard" al Qaeda requires a long-run strategy in countries where democracy is not likely to flourish in the near-term. Until the U.S. can figure out its strategic interests in the Middle East (assuming it can, I'm not convinved this is possible), I recommend a narrow counterterrorism strategy focused on a small set of tasks executed by a limited set of actors.

■ Terrorism is a lesser threat to our national security compared to other long-run issues.

The media and counterterrorism pundits are notorious for maps of al Qaeda where entire countries are shaded ominous colors when there are maybe only a half dozen al Qaeda members/supporters in a country consisting mostly of uninhabitable desert. Al Qaeda threat conflation convinces Americans that terrorism is a national security threat more dangerous than all others leading to over extension of counterterrorism efforts. (My next post will further discuss why we are hooked on one big "al Qaeda"). Terrorism poses a less serious threat than many other national security issues such as climate change, excessive US national debt, Chinese cyber theft of intellectual property, an aggressively resurgent Russia, Iranian nuclear gamesmanship and a hothead North Korean supreme leader with daddy issues. Each of these threats poses a far greater threat to long-run US

national security than lost young boys trapped amongst al Qaeda affiliates that are just as likely to kill their own members as they are Americans.

Table of Contents

Treating America's al Qaeda Addiction - Part 2 of "Smarter Counterterrorism"

By Clint Watts, Foreign Policy Research Institute, February 17, 2014

(This is the second post in this series, see the initial post at "Smarter Counterterrorism in an Era of Competing al Qaeda's")

For a dozen years, Americans have suffered through endless debates about an amorphous al Qaeda and its current strength. One argument will consistently suggest al Qaeda is stronger, again on America's doorstep waiting to pounce and presents a significant threat to U.S. National Security and the West. More recently, a counterargument has emerged that al Qaeda is no longer, the war on terrorism is over, and that Americans can return to a 1990's security posture where we focus on process (i.e. civil liberty protection, accountability, and transparency) rather than the end state of preventing another 9/11 attack. These two arguments represent the outcome of a hollow debate that relies on a false assumption; that al Qaeda is a singular unified threat to the U.S. and operates in a manner consistent with its structure at the time of September 11, 2001. Thus, when television pundits vaguely say, "al Qaeda", no one knows for sure what they are referring to; they are in effect saying nothing at all.

Today, al Qaeda exists only as a subset of a multi-faceted jihadi militant landscape strewn across three continents and at least a half dozen insurgencies. While some warn of the dangers of a resurgent, singular al Qaeda, the real danger of terrorism comes from the unknown-–a plurality of armed jihadi groups spread throughout the Middle East and Africa lightly watched by the West due to a fixation on outdated models of al Qaeda and a persistent winnowing of Western surveillance and intelligence resources. To wage smarter counterterrorism moving forward, the U.S. must deal with its al Qaeda addiction.

So how did we get addicted to "al Qaeda"? A few factors converged to narrow our vision.

The Trauma of 9/11 – The most obvious reason is that we in the U.S. can't move on from al Qaeda because of the trauma of 9/11. I shouldn't discount it. But, Americans have fueled their fears with never-ending replays of this trauma. Since 2001, every perceived threat stirs up the images and pain of 9/11 and to always remain on the side of caution, we've let fear drive our actions. We will never forget, but we must move on; move beyond al Qaeda and recognize that even if al Qaeda attacks the U.S. again, it will not bring an end to the United States. I'm not calling for complacency, but instead reasonable awareness of the risks terrorism presents – a risk that is not adequately understood by the all-encompassing name "al Qaeda". Our media could help us move on, but…

One Big "al Qaeda" Threat Is Easier For the Media To Convey – Mass media has spent more than a decade priming audiences to the term "al Qaeda". When a story or report says "al Qaeda", a mental image quickly forms - planes crashing into buildings, falling twin towers, hooded men shooting weapons, climbing monkey bars and crawling under barb wire. The story quickly plays on emotion, neatly frames the argument in two parties (the U.S. & the West vs. al Qaeda) and makes for great "click bait" on websites.

I feel for journalists and their editors as they are caught in a trap of engaging and maintaining an audience while trying to explain a highly complex set of issues in only a few hundred words or a 30-second sound bite. They can't succinctly describe how Ansar-al-Flavor-Of-The-Week may impact U.S. security and resulting policy.

The latest in this conundrum comes from al Qaeda Central's disavowing of the Islamic State of Iraq and al Sham (ISIS, formerly known as al Qaeda in Iraq) which presents a threat to both "Old Guard" al Qaeda and U.S. interests. The term used most recently is "al Qaeda Splinter Group", a name stripped from a Tom Clancy novel/video game spinoff I assume. This term also confuses the issue for the reader, as al Qaeda's global leader Ayman al-Zawahiri broke it off with ISIS, not the other way around – ISIS didn't break off from al Qaeda, they were kicked out. The media sits in a tough spot and normally they could look to academia and experts to help clarify the landscape and the issues. Well, that would be in normal circumstances….

The Terrorism and Counterterrorism Industry crumbles without al Qaeda – The years since 9/11/2001 have created an unprecedented research and industrial buildup to support counterterrorism; a sea of money no academic or analyst ever imagined during the 1990s. With the beginning of nation-wide campaigns in Afghanistan and Iraq, the need for expertise was apparent and the resources flowed freely. Every corner of the U.S. government sponsored some form of 'terrorism analysis' or 'counterterrorism planning' where

academia and the private sector brought specialists together to anticipate al Qaeda's next move and implement an unwieldy counterterrorism plan. (Full disclosure: I am a product of this buildup.)

In the early years, this worked well, those with strong language skills tended to cover the hot conflict zones and others migrated to study jihadi ideology and al Qaeda's pursuit of WMD. Many were former Sovietologists more adept at transitioning their psychohistorical and psycholinguistic analysis skills to a new threat in a different theater. I ended up working on terrorist threats in Africa, for example, because I lacked Arabic language skills, was genuinely interested in learning more about Africa and because everyone else desperately wanted to get in on the action in Iraq and Afghanistan. Ironically, they are now scampering to become Africa or Syria experts today. It's a never-ending chase.

This system progressed fine until the drawdowns in Iraq and now in Afghanistan. As the big theaters closed, this forced analysts to chase the next big threat, rapidly research a new al Qaeda affiliate and region, reassert their relevance and publish prose on al Qaeda's next rise – all done in an effort to protect our nation from terrorism and our own livelihoods in the process. (Remember, I am a member of this industry.) The reports routinely prescribe one of three patent solutions for defeating al Qaeda: 1) the only way to defeat al Qaeda is to completely wipe the planet of al Qaeda's ideology 2) we must win the hearts and minds of every disenfranchised community from Africa to South Asia or 3) both of these things. In all three cases, a multi-billion dollar campaign of undetermined length, under-researched methods with fuzzy long-run objectives is required – completely infeasible, utterly unsustainable and not appropriately scoped for the more narrow and severe threat of 'Old Guard' al Qaeda.

The net result of this system has been a splurge of terrorism and counterterrorism punditry by analysts increasingly removed from the frontlines with al Qaeda, relying on less and less journalist reporting and primary documents, framing thinking based on notions of al Qaeda circa 2001 rather than 2011 and trying to piece together a global al Qaeda strategy from a noisy jihadi social media landscape. Each report, if sufficiently scary, presents another opportunity for funded research or a speaking engagement. Who wants to read a complicated report on the rise of the next serious threat presented by Lashkar-Fill-in-the-Blank or Ansar-Fill-in-the-Blank unless its "tied", "connected" or "linked" to al Qaeda – and "al Qaeda" means whatever you need it to be. The counterterrorism punditry isn't doing anything devious or deliberate. They are not members of the top 1% nor trying to lead their country astray. Most are passionate about their profession, genuinely well intentioned and highly competitive with one another. Anyone that's ever sat in a meeting of terrorism and counterterrorism analysts and academics knows its really a passive aggressive game to see who's smartest – the equivalent of the TV Show "Survivor" for people that don't like to go outside, where everyone protects or bluffs about their sources and builds alliances to protect their food (I mean funding). The outcome is al Qaeda threat conflation, an endless game of Back-to-Bin Laden or Zawahiri informed by limited sourcing and perpetuated by competition over relevancy.

The worst part of today's CT punditry is over the long-run it's a self-fulfilling prophecy: by over-classifying things as al Qaeda, we hunt for more al Qaeda, and we find more al Qaeda. We end up over pursuing, making more mistakes, spreading ourselves thin and in fact creating more al Qaeda than we eliminate. Today's al Qaeda and the jihadi militants swirling around them are too diffuse, scattered amongst too many cultures and countries and evolving too quickly for any one counterterrorism pundit or TV talking head to maintain a persistent understanding.

The alternative to hoping the media can appropriately classify "al Qaeda" or that the counterterrorism industry can narrowly deduce the true threat of terrorism is to have a system where information can flow from multiple sources across every jihadi theater to one place where the world's most experienced analysts can work together to determine the true nature of the terrorist threat to the U.S., and craft nimble policy and appropriate action to defeat those most dangerous threats to U.S. national security. If only we such a system…hhmmm….that's right we do, its called the U.S. counterterrorism community. Could the U.S. government help focus discussions about the threat of terrorism? Probably not because the…….

U.S. Government Needs "One al Qaeda" To Keep Counterterrorism Options Open – I think the only entity capable and actually informed about today's threat of terrorism is the U.S. counterterrorism community (The Intelligence Community, State Department, FBI, DoD, etc.). They see the open source reporting of the counterrorism industry, have the most important intelligence from higher classification levels and have cadres of operators and analysts with a decade-plus of counterterrorism experience. They've learned many lessons the past decade and the recent, nearly simultaneous raids in Tripoli, Libya and Barawe, Somalia demonstrate just how nimble they can be. I do believe the U.S. counterterrorism community is the only single entity sufficiently capable and resourced to decipher today's chaotic terrorist landscape. Unfortunately, three forces prevent them from curing America's al Qaeda addiction.

- Armed Use of Military Force (AUMF) hinges on the existence of al Qaeda – Gregory Johnsen's recent Buzzfeed article provides the best overview on how our counterterrorism capabilities continue to pursue terrorist threats that hinge on the existence of al Qaeda. Without the AUMF, many counterterrorism authorities and tools necessary for protecting the U.S. from emerging jihadi variants would come off the table. Thus the words "linked", "connected" and "tied" in counterterrorism analyses and stories are essential for keeping the AUMF in place. Unfortunately, the U.S. Congress appears completely incapable of updating the AUMF for today's threat landscape.
- Edward Snowden's leaks – Snowden's disclosures have called into question what counterterrorists view as crucial intelligence and surveillance tools and techniques. Signals intercepts and sources essential for understanding the myriad of extremist groups around the world must be justified. Most of these capabilities were built in response to al Qaeda, so now in the face of scrutiny, we must reaffirm there is an al Qaeda to justify their development and continued existence.
- Politics – The American political climate stinks and its effect on national security is perverse. Neither party wants to be found weak on terrorism or downplaying al Qaeda as there is about a 100% chance al Qaeda or some entity connected to al Qaeda will kill an American in the future. Congressmen in general so poorly understand terrorism to begin with that the U.S. counterterrorism community has to keep the "One Big al Qaeda" going to explain national security threats to those that approve their budgets. For an example of this pointless dynamic, watch last week's Senate Armed Services Committee discussion about al Qaeda. See minute 43:40 where Senator Inhofe asks "Yes or No, is al Qaeda stronger?" to which the Director of National Intelligence James Clapper and Director of the Defense Intelligence Agency LTG Michael T. Flynn must answer. Senator Inhofe even references an ominous map like I discussed in my first post.

How do we cure our addiction to Al Qaeda?

For America to cure its "al Qaeda" addiction several things must happen.

For everyday Americans we must:

Accept that al Qaeda or other jihadi militant groups will ultimately kill Americans again sometime in the future. - When this happens, we must control our emotions, analyze what has happened and narrowly focus on retaliating against the actual perpetrators and not their "connections".

Understand the threat of terrorism and America's need to pursue counterterrorism will not end in our lifetimes. - We cannot know when al Qaeda is defeated when we cannot agree on a definition of what al Qaeda is. Even if al Qaeda were to cease to exist tomorrow, there would be some disenfranchised individual or group, boasting a jihadi ideology from a far off safe haven that would want to attack the U.S. for one reason or another.

For the media, please:

Expand your terms – Please expand beyond "al Qaeda" to describe the vast landscape of Sunni militant groups in the world. As we see now with the separation of ISIS from al Qaeda, there will be serious terrorist threats to U.S. national security, and al Qaeda will be only one of them. The more you inform the public without the limitations of the al Qaeda mental model the better we will all be.

Stop using singular terrorism and counterterrorism talking heads. - If you are relying on one or two experts to cover every story from domestic homeland security to al Qaeda in Pakistan, its time to make a change and build a bigger and broader set of experts you can call on. If your expert refers to everything as "al Qaeda" or "bad guys", show them the door. This change has already started to happen somewhat, and it needs to continue if there is any hope for Americans to understand the threats facing them.

For the terrorism and counterterrorism pundit and academic community, I recommend the following:

Work collaboratively rather than individually - The academic community and industry could establish systems of cooperation and sharing rather than competition – seeking collective rather than individual funding. Understanding al Qaeda or any emerging terrorist threat requires an interdisciplinary team with deep knowledge on dozens of regions, cultures, languages and extremist groups. For example, today, there are dozens of researchers creating open source datasets logging foreign fighters to Syria-–an important area of research. But each researcher has only a partial dataset, all slightly skewed based on the collector, their skills, their sources and their funders. When combined, these analysts and researchers likely have the insight needed to appropriately assess today's complex terrorism environment. Maybe the upcoming University of Massachusetts Center for Terrorism and Security Studies event "Communication and Collaboration for Counter-Terrorism" is a first step in the right direction.

For our government to pursue the terrorists of greatest threat to the U.S., I recommend the following:

Maintain our intelligence capabilities – Despite the post-Snowden trend to question the need for intelligence capabilities, they've never been more essential for keeping an eye on a diffuse terrorist landscape. Rather than taking tools off the table, the U.S. should be reinforcing its most valuable capabilities.

Decouple politics from counterterrorism – This is impossible, I know. But as long as both political parties feel trapped in a zero defect climate of fear (such as the constant harranguing about Benghazi) then the U.S. counterterrorism community will be required to play the "is al Qaeda stronger?" game indefinitely. Additionally, Congress must move to update U.S. laws and policies to appropriately address authorities for countering terrorist groups that threaten the U.S. Only updated laws and policies will allow for the appropriate streamlining of processes, adequate oversight and desired transparency needed to appropriately counter the plethora of non-state threats we will face in the coming years.

Alright, enough big picture talk, in the next post (part 3 for later this week), I'll focus on "Jihadi Competition After al Qaeda Hegemony"

Table of Contents

S. Korea Pushes To Develop Offensive Cyberwarfare Tools

By Kim Eun-jung, Yonhap News Agency, 2 Feb 2014

SEOUL, Feb. 19 (Yonhap) -- South Korea will push to develop sophisticated cyberwarfare tools that could wreak havoc on North Korea's nuclear facilities as part of its plans to beef up offensive capabilities, the defense ministry said Wednesday.

The ministry reported a long-term plan for cyberpolicy to the parliamentary defense committee, at a time when calls have risen to reform the Cyber Warfare Command, which has been dogged by allegations of an online smear campaign in the 2012 presidential election.

The military vowed to toughen regulations on the cyberwarfare officials' use of social networking sites to prevent them from posting political writings while conducting psychological warfare missions against North Korea's propaganda activities.

A strategic plan for the second phase calls for developing cybertools for offense like Stuxnet, a computer virus that damaged Iran's uranium enrichment facility, to cripple North Korea's missile and atomic facilities.

The reform plan also calls for beefing up its psychological warfare capability to paralyze the origin of a cyberattack.

"Once the second phase plan is established, the cyber command will carry out comprehensive cyberwarfare missions," a senior ministry official said, asking for anonymity.

The cyber command was created in 2010 under the defense ministry to guard off rising cyberthreat posed by North Korea, which is believed to have masterminded massive attacks on networks of South Korea in recent years.

The command, however, has put a much greater focus on psychological warfare activities against Pyongyang's propaganda and slandering in cyberspace, which questioned the legitimacy of the secretive unit.

The ministry plans to set up the "Cyber Defense Department" under the Joint Chiefs of Staff (JCS) in May, which would serve as the control tower of cyberwarfare missions.

"The new department will oversee the defensive cyberwarfare missions when major networks are hit by hacking attacks, while carrying out orders of the chairman of the Joint Chiefs," the ministry official said.

To dispel lingering suspicions over the command's psychological warfare mission, the ministry plans to create a regular monitoring system to prevent cyber-related officials from engaging in missions related to political activities.

By law, soldiers and military personnel are obligated to maintain political neutrality.

The ministry also said it will operate a committee to review cyberwarfare operations in advance and establish a whistleblower program to allow soldiers to report politically biased missions.

More than a dozen members of the command's psychological warfare unit have been under investigation by military prosecutors for allegedly posting politically charged messages online against the opposition camp and its candidate ahead of the 2012 vote.

Opposition lawmakers have accused the military of trying to cover up more pervasive election meddling by purposely carrying out a shoddy investigation into the online smear campaign by the Cyber Warfare Command, calling for a special prosecutor to launch an independent probe.

Table of Contents

How America's Soldiers Fight for the Spectrum on the Battlefield

By Brendan I. Koerner, Wired, 02.18.14

An electromagnetic mystery in northern Iraq changed the course of Jesse Potter's life. A chemical-weapons specialist with the US Army's 10th Mountain Division, Potter was deployed to Kirkuk in late 2007, right as the oil-rich city was experiencing a grievous spike in violence. He was already weary upon his arrival, having recently completed an arduous tour in Afghanistan, which left him suffering from multiple injuries that would eventually require surgery. In the rare moments of peace he could find in Kirkuk, Potter began to contemplate whether it was time to trade in his uniform for a more tranquil existence back home—perhaps as a schoolteacher. Of more immediate concern, though, was a technical glitch that was jeopardizing his platoon: The jammers on the unit's armored vehicles were on the fritz. Jammers clog specific radio frequencies by flooding them with signals, rendering cell phones, radios, and remote control devices useless. They were now a crucial weapon in the American arsenal; in Kirkuk, as in the rest of Iraq, insurgents frequently used cell phones and other wireless devices to detonate IEDs. But Potter's jammers weren't working. "In the marketplaces, when we would drive through, there'd still be people able to talk on their cell phones," he says. "If the jamming systems had been effective, they shouldn't have been able to do that."

A self-described tech guy at heart, Potter relished the chance to study the jammers. It turned out that, among other problems, they weren't emitting powerful enough radio waves along the threat frequencies—those that carried much of the city's mobile traffic. Once the necessary tweaks were made, Potter was elated to witness the immediate, lifesaving results on the streets of Kirkuk, where several of his friends had been maimed or killed. "To see an IED detonate safely behind our convoy—that was a win for me," he says. It was so thrilling, in fact, that when Potter returned from Iraq in 2008, he dedicated himself to becoming one of the Army's first new specialists in spectrum warfare—the means by which a military seizes and controls the electromagnetic radiation that makes all wireless communication possible.

It is well known that America's military dominates both the air and the sea. What's less celebrated is that the US has also dominated the spectrum, a feat that is just as critical to the success of operations. Communications, navigation, battlefield logistics, precision munitions—all of these depend on complete and unfettered access to the spectrum, territory that must be vigilantly defended from enemy combatants. Having command of electromagnetic waves allows US forces to operate drones from a hemisphere away, guide cruise missiles inland from the sea, and alert patrols to danger on the road ahead. Just as important, blocking enemies from using the spectrum is critical to hindering their ability to cause mayhem, from detonating roadside bombs to organizing ambushes. As tablet computers and semiautonomous robots proliferate on battlefields in the years to come, spectrum dominance will only become more critical. Without clear and reliable access to the electromagnetic realm, many of America's most effective weapons simply won't work.

The Pentagon failed to foresee how much the wireless revolution would alter warfare.

Yet despite the importance of this crucial resource, America's grip on the spectrum has never been more tenuous. Insurgencies and rogue nations cannot hope to match our multibillion-dollar expenditures on aircraft carriers and stealth bombers, but they are increasingly able to afford the devices necessary to wage spectrum warfare, which are becoming cheaper and more powerful at the same exponential pace as all electronics. "Now anybody can go to a store and buy equipment for $10,000 that can mimic our capability," says Robert Elder, a retired Air Force lieutenant general who today is a research professor at George Mason University. Communications jammers are abundant on global markets or can be assembled from scratch using power amplifiers and other off-the-shelf components. And GPS spoofers, with the potential to disrupt everything from navigation to drones, are simple to construct for anyone with a modicum of engineering expertise.

Stateless actors aren't the only—or even most troubling—challenge to America's spectrum dominance. The greater an opponent's size and wealth, the more electromagnetic trouble it can cause. A nation like China, for example, has the capability to stage elaborate electronic assaults that could result in nightmare scenarios on the battlefield: radios that abruptly fall silent in the thick of combat, drones that plummet from the sky, smart bombs that can't find their targets. The US may very well never engage in a head-to-head shooting war in the Far East, but the ability to effectively control the spectrum is already becoming a new type of arms race, one that is just as volatile as the ICBM race during the Cold War—and one that can have just as big an impact on global diplomacy.

The American military is scrambling to develop new tools and techniques that will help it preserve its electromagnetic edge. But that edge continues to shrink by the day, and very soon our inability to completely control the spectrum might result in a different kind of war.

Any old crow will gladly tell you that spectrum warfare is nothing new. The men and women who go by that avian moniker, which derives from a World War II codename, are veterans of the American military's decades-old efforts to attack and defend the electromagnetic domain. Their secretive trade dates back to the Russo-Japanese War: While facing an impending naval bombardment in 1904, a Russian telegraph operator used his spark-gap transmitter to jam the radio of a Japanese ship that was orchestrating the assault. Though this electronic gamesmanship worked wonders—the Japanese were unable to complete their bombardment—the czar's military brain trust failed to learn from the experience. The following year at the Battle of Tsushima, Russian admiral Zinovy Rozhestvensky foolishly declined to jam his opponent's radios, allegedly because he didn't trust that his own transmitters would work. The Japanese, whose ships were outfitted with the latest Marconi wireless equipment, used their communications superiority to outmaneuver and destroy the majority of Russia's Baltic Fleet.

Four decades later, during World War II, the advent of radar spurred both Axis and Allied powers to invent ways to cloak the true natures of their aerial exploits. One of the most famous innovations was Moonshine, a British system that absorbed, amplified, and then echoed German radar waves, so that a group of just a few planes could mimic an armada of hundreds. When the Cold War commenced, the US focused on refining and improving these early methods of electronic bamboozlement. During the latter stages of the Korean War, for example, American B-29 bombers were outfitted with primitive jammers that befuddled the radar on antiaircraft guns. And starting in 1965, Navy jets in Vietnam were equipped with torpedo-shaped jamming pods that knocked out early-warning systems with torrents of electronic noise.

"The next war will be won by the side that best exploits the electromagnetic spectrum," a Soviet admiral observed in 1973, shortly after Israel used jamming techniques to outwit Syrian guided missiles during the Yom Kippur War. Clearly in agreement with that prognostication, the US Air Force spent a good chunk of the Reagan era developing the EF-111A Raven, an electronic jamming plane that would play a key role in shutting down Iraq's radar stations during the early hours of Operation Desert Storm

But after that emphatic victory, the American military lost interest in the Old Crows' geeky specialty. This was due partly to a vogue for stealth technology: Since aircraft like the B-2 bomber were designed to evade radar by virtue of their sleek shapes, jamming equipment seemed superfluous. But the Pentagon also failed to foresee just how much the new millennium's wireless revolution would alter warfare—by making unmanned vehicles pervasive and giving asymmetric forces new means to coordinate and execute attacks.

The folly of this strategic myopia became apparent soon after the 2003 invasion of Iraq. Insurgents quickly mastered the art of constructing radio-controlled IEDs, which they set off with a range of common gadgets—cell phones, of course, but also more basic devices such as garage-door openers and toy-car remotes. The Army lacked the technical expertise to prevent the insurgents from using the spectrum, so it turned to the Navy and Air Force for assistance. But those branches hadn't done enough to update their spectrum-warfare capabilities over the preceding decade. Their jammers were designed to affect large-scale radar installations, not the narrow slivers of spectrum used by civilians. And much of this equipment was ancient: The Navy's preeminent jamming pod, the ALQ-99, had debuted in the early 1970s and was plagued by reliability problems related to its age. (The ALQ-99 will remain the state of the art in the Navy's arsenal until at least 2020, when it's scheduled to be replaced by the yet-to-be-built Next Generation Jammer.)

When the Army finally began to equip its armored vehicles with hacked-together jammers, a new set of problems arose. The systems' antennas blasted out radio waves with such reckless abandon that plenty of friendly communications links got zapped in the process—a problem that the military terms "signal fratricide." These jammers were so unruly, in fact, that they often forced vehicle commanders to deal with a potentially lethal conundrum. "I had a choice as a guy driving down the road—do I want to communicate, or do I want to conduct a defensive electronic attack against a potential IED?" says colonel Jim Ekvall, chief of the Army's Electronic Warfare Division. Wrong decisions led to lost lives.

Over time the Army learned how to fine-tune its jammers to target only the most worrisome portions of spectrum, rather than enormous swaths that included Americans' preferred frequencies. To make this possible, soldiers known as spectrum managers created detailed maps of all of Iraq's electromagnetic activity, a chore that required laborious intelligence work. In addition to tracking and recording the emissions of every piece of friendly military hardware, the managers had to compile a list of which frequencies were used by a galaxy of cheap civilian devices.

This mountain of data was incorporated into spectrum usage plans that likely helped reduce both signal fratricide and roadside bombings: Between June 2007 and June 2009, monthly IED attacks in Iraq decreased by 90 percent. The campaign's success awakened the Army to the need to cultivate as many spectrum-savvy soldiers as possible. In 2009 it made electronic warfare a distinct career for enlisted soldiers, who could elect to study the craft in a new program at Fort Sill, Oklahoma. Jesse Potter, the master sergeant who helped

solve the 2007 jammer mystery in Kirkuk, was among the program's first graduates, thereby earning the right to wear a special insignia featuring a lightning bolt crossed with a skeleton key.

These newly minted spectrum warriors found that their skills were much in demand in Afghanistan, where the Taliban recovered from its initial defeat in part by learning how to hack mobile technology—not only to detonate IEDs but also to maintain communications while on the run. To stay in touch with one another in the nation's hinterlands, Taliban operatives often extend the range of existing mobile networks. "They pay some guy 10 bucks and say, 'Go climb up that mountain over there and put up this repeater,'" says Brian Filibeck, a chief warrant officer who picks candidates for the electronic warfare school at Fort Sill. Many Taliban ambushes were planned using those simple bundles of antennas and amplifiers.

US forces had to rapidly come up with solutions to this challenge. Tasked with dominating the spectrum in regions largely inaccessible to ground vehicles, the Army built Ceasar, a modified version of a Navy jammer that can be affixed to a C-12 Huron turboprop airplane. Ceasar can sense the emissions of the Taliban's repeaters, then jam their signals. The Army is now trying to miniaturize the system so it can be loaded onto unmanned aerial vehicles such as the Gray Eagle or even the hand-launched Wasp.

The Taliban and its ideological brethren are constantly trying to improve their spectrum-warfare weaponry. Chief among their goals is to reduce the threats posed by American drones. In 2009, US forces discovered that Iraqi insurgents were using a commercial program called SkyGrabber to intercept video feeds from Predator UAVs. The software allowed the insurgents to use ordinary satellite dishes to capture data as it was being transmitted back to base; because the data was unencrypted, SkyGrabber was then able to convert it into watchable media files. The US has since begun encrypting the drones' video feeds. But according to a classified report leaked to The Washington Post by NSA whistle-blower Edward Snowden and then published last September, al Qaeda is also trying to figure out how to sever the links between drones and their human operators, who can be stationed half a world away. One of the organization's most promising lines of inquiry has involved the construction of GPS jammers, which could theoretically be used to corrupt a drone's navigation and missile-guidance capabilities. Analysts with the Defense Intelligence Agency observed that such systems, if further developed, "probably would be highly disruptive for US operations in Afghanistan and Pakistan."

The building that houses the army's spectrum elite is fittingly tough to locate without help from GPS. The bland redbrick edifice is perched on a hilly corner of Fort Leavenworth, Kansas, far beyond the 187-year-old Army base's horse stables and forested picnic area. From down below on McClellan Avenue, the place is easy to mistake for a dormitory or unusually dour day-care center. But the Electronic Warfare Proponent Office (EWPO) is actually a hotbed of classified activity, all geared toward building US spectrum dominance—an already difficult task that keeps getting harder by the year.

Life was much simpler for the Army back when ruling the skies, rather than the electromagnetic waves, was its chief prerequisite for success. Gaining air supremacy may require colossal amounts of fuel and bombs, but it's easy to define and hard to overcome once established. When Army general Norman Schwarzkopf declared that coalition forces had secured total control of Iraq's airspace just two weeks after the start of Operation Desert Storm, he was able to cite indisputable evidence: A significant chunk of Iraq's air force had been annihilated, along with the aviation infrastructure that supported it. There was no chance that Saddam Hussein would be able to field a fleet of replacement MiGs in a matter of weeks.

Spectrum supremacy, by contrast, can never be more than fragile. For starters, it is tricky to ascertain when it has even been attained—there is no quick formula for evaluating when an enemy has been entirely ejected from an immense, invisible battlespace. More important, even a reeling opponent can rebound quickly in the spectrum: Launching an electromagnetic counterattack doesn't require hundreds of millions of dollars' worth of jets, just a handful of gadgets and some basic engineering skills. "For a warlord to go and get their hands on a piece of equipment that can create a huge communications black hole and create serious havoc, that's very cheap, very realistic," says Filibeck, one of the top officers with the EWPO.

As al Qaeda has discovered, waging do-it-yourself spectrum warfare against the US is not quite as easy as jamming a cell phone tower. American communications devices are fortified to resist elementary attempts at electromagnetic meddling. The next generation of military radios, for example, will feature an antijam mode in which signal power is automatically increased in response to perceived electronic threats. Yet weaknesses still abound, particularly in systems that use GPS data—notably the drones that now make up more than 40 percent of the US military's aerial fleet. GPS relies on a technique called direct-sequence spread spectrum to fend off jamming. But DSSS, which involves the scrambling of data into hard-to-guess patterns, is far from foolproof. In early 2012, for example, when North Korea spent 16 days emitting signals from truck-sized GPS jammers, more than 1,000 South Korean aircraft reported feeling the effects. And that June a University of Texas at Austin team managed to hijack a drone by sending it counterfeit GPS instructions. Incidents like

these recently spurred a Department of Homeland Security official to warn that “a single well-placed low-power GPS jammer or spoofer could disrupt an entire region [of the US].” (To prevent the smuggling of these devices, which are illegal in the US, the Air Force Research Laboratory is developing a jammer detector that can be installed at border crossings.)

Nor would it take much for even relatively unsophisticated enemies to develop those tools. “You can go onto the Internet and Google how to build low-cost GPS denial-of-service devices,” Jesse Potter says. “They’re about the size of a small computer. If an enemy can build a thousand of those and place them all over the battlefield so I can’t find them all, then I’ve got a problem.” One of those problems could involve an Army convoy suddenly losing its navigation and communication capabilities right as it’s crossing a perilous stretch of enemy-held territory—soldiers isolated in such a manner would be vulnerable to attacks from guerrillas who know the terrain. Or the enemy could snatch a drone out of the sky and crash it or even take it over.

And if an enemy truly lacks the technological wherewithal to pull this off? Then they can simply buy it. Plug-and-play jammers and electromagnetic analyzers are widely available for purchase, as are software packages designed to identify and defend against electronic threats on the battlefield. The Israeli firm Your Total Security, for instance, sells entire vehicles tricked out with all the gadgets necessary “to block a wide spectrum of radio and wireless communications frequencies.” And the French company ATDI offers HTZ Warfare, a “comprehensive radio planning solution” that promises to help forces avoid signal fratricide, intercept enemy communications, and repel attempts at jamming. A rogue nation equipped with this sort of technology could challenge American troops across the spectrum, hindering if not completely eliminating their ability to use their electronics during an invasion. And the road to Tehran or Bamako is a terrible place to lose every last bit of situational awareness.

With its time in Afghanistan finally coming to an end, the American military is in the early stages of the Pacific Pivot—a long-term strategy to counter China’s growing influence in Asia. The US is keen to deploy more troops to places like Australia and Guam, to station more Navy ships in Singapore, and to offer more cooperation to key regional allies such as the Philippines, all in the name of keeping pressure on the region’s heavyweight.

The nature of the geography in that sprawling part of the world, where strips of land are separated by vast expanses of water, will create fresh vulnerabilities in our military’s communications networks. “Things get much harder against Far East targets when we don’t have a dominating US military footprint in the region as we did with Iraq and Afghanistan,” says Charles Clancy, director of the Hume Center for National Security and Technology at Virginia Tech. “Command and control become even more exposed to attack, because we lack the resources on the ground to protect it. Also, without a physical footprint we rely even more greatly on unmanned systems.”

China is well aware that the Pacific Pivot will strain the US military’s ability to protect its networks against electromagnetic sabotage. The People’s Liberation Army is thus pumping tremendous resources into beefing up its spectrum-warfare operations, much as it has funded the formation of an elite hacker corps to wage cyberwar against its rivals. Thanks to this investment, the scientific literature now teems with Chinese-authored papers on topics like how to design better simulation software for aircraft that jams electronic signals. This research is supporting the development of devices that will make China our most formidable opponent in the spectrum.

Even if a full-on military confrontation is unlikely, there are still real benefits to gaining the technological upper hand. The ability to anticipate and counter an opponent’s weapons is valuable even if no attack ever comes—it gives a country leverage in the broader geopolitical sphere. And China is working hard to gain this leverage through the electromagnetic realm.

Some of its devices are designed to confuse guided weapons, which often rely on radar to home in on their targets. “We are now painfully aware of the jamming systems for their aircraft, some of which have the potential of making systems like air-to-air missiles inoperable,” says Richard Fisher, a senior fellow at the International Assessment and Strategy Center. There is every reason to believe that this technology could be adapted to bewilder active guided cruise missiles, a weapon essential to American naval might.

The Chinese are also working on ways they could, in a pinch, take out GPS, which would likely let them control the skies above Taiwan or the Korean Peninsula in the event of war. China’s fighters, bombers, and drones won’t suffer if GPS goes down: By 2020, the country will have completed work on Compass, its own 35-satellite navigation system. (Presumably, the US is working on a plan to jam it.) The US air fleet, by contrast, will be significantly handicapped without precise guidance from above. The Air Force takes the threat of a Chinese electromagnetic assault so seriously that it’s stepping up efforts to train its pilots how to fly without the aid of GPS, radar, or even radio communications. The Navy, meanwhile, is testing an antenna that will

hopefully allow drones to quickly reestablish links with GPS satellites in the wake of a significant jamming attack.

But American airpower will not suffer alone if the Chinese win the battle for spectrum—ground power will also take a hit. Congress has mandated that two-thirds of the military's ground vehicles be unmanned by 2025, and these machines are the ideal candidates to lead amphibious assaults along the Pacific Rim. But like aerial drones, ground-based drones will not be able to function without a dash of human guidance and a steady stream of navigational data. If Chinese jammers can overwhelm their systems, any robot vehicles racing up a beach in occupied Taiwan would simply fall idle.

In true Cold War fashion, Chinese-made spectrum-warfare technologies are likely to spread far beyond East Asia. "Everything that China manufactures is eventually offered for sale, up to and including nuclear weapons technology and ICBM technology," Fisher says. "If they have a jamming system, it's likely comparable or even superior to whatever alternatives are out there, and it's likely to be sold." The China Electronics Technology Group Corporation, a government-affiliated company that produces much of the nation's spectrum-warfare hardware, is a fixture at major arms trade shows such as Peru's Sitdef. If and when the US military is pulled into future missions in the steppes of East Africa or the forests of Central America, it may run into opponents armed with jammers that were manufactured in greater Shanghai. And if our military gets bogged down in those conflicts because it can't dominate the spectrum to its liking, the Pacific Pivot will become significantly harder to pull off—much to China's joy.

The orbit test bed looks vaguely ominous, like an interrogation chamber from an avant-garde sci-fi film. The room is cavernous and stark, with gleaming white floors and barren walls. The ceiling is lined with orderly rows of what look like upside-down Ikea standing lamps. Inside each hangs a yellow box emblazoned with the word winlab—the name of the Rutgers University laboratory where this curious array is located. The boxes, 400 of them in total, are radio nodes, all part of a robust network for putting experimental communications protocols and applications through their paces. Orbit is where wireless-technology researchers go to test new methods for sending data across cellular and wireless networks. It's also where the US military hopes to find the algorithms that will tilt the spectrum-warfare playing field in its favor.

That precious code is emerging as part of the Spectrum Challenge, a tournament sponsored by the Defense Advanced Research Projects Agency. With $150,000 in prize money at stake, 18 teams are vying to create software that can recognize when radio waves are smacking into interference, then route them around the obstacles by adapting their waveforms and the frequencies they use. The challenge uses Orbit to host one-on-one clashes in which teams score points by successfully delivering packets of data from one end of the network to the other, a task complicated by the fact that competitors are allowed to jam one another at will.

"We first concentrate on denying the other team, then we try to push our trickle of packets through," says Peter Volgyesi, head of the Vanderbilt University squad that won a $25,000 prize in a preliminary round last September. The jamming has been unexpectedly ferocious: Darpa was hoping that the winning team would be able to transmit 15,000 packets of data, but Volgyesi and his colleagues won the round by sneaking through just around 100 packets. In preparation for the tournament's final round in March, the competitors are now modifying their code with an eye toward making it stronger and more agile; the algorithms need to be heavily redundant so information can still get through when faced with a barrage of electromagnetic noise. It's a constant cat-and-mouse game in which opponents must try to outwit one another in new and innovative ways.

Darpa stresses that the Spectrum Challenge is primarily intended to elicit solutions to problems on the home front: With the American spectrum increasingly clogged by civilian traffic, the military is worried about interference around bases and testing grounds. But the tournament also has obvious implications for the future of combat. In a world where every opponent has the ability to conduct electronic attacks, the US knows that software is its one big advantage. If the challenge yields algorithms that can elegantly guide signals past jamming attempts, the American military will be immeasurably more confident in its future strategies.

The widespread adoption of tablet computers is one example of those plans. The Army recently awarded a $455 million contract for the development of ruggedized tablets, to be mounted in more than three dozen types of vehicles and weapon systems. Soldiers will rely on these computers to receive critical updates about the locations of threats or the movements of friendly forces. If those updates don't arrive as intended because the Army's mastery of the spectrum has been degraded, the results could be deadly.

Software will also help spectrum warriors do a better job of explaining their work to superiors. A big challenge they've faced is how to talk to commanders who know all about pounding targets with munitions but are puzzled by the abstractness of spectrum warfare. Jesse Potter jokingly disparages these officers as "meat eaters" who don't readily process why their fortunes depend on the reliable transmission of radiation from one node to another.

This expository task should become easier in 2015, when the Army is set to roll out software that will create more user-friendly visualizations of the spectrum's real-time status on the battlefield. Soldiers like Potter will be able to point out which locations are securely in American electromagnetic hands and which are susceptible to electronic attack.

Perhaps this effort will succeed in making the meat eaters understand the importance of spectrum. Perhaps the brains at the Electronic Warfare Proponent Office can keep a step ahead of their foes. If not, the US military will discover that no amount of firepower can assure its dominance.

Table of Contents

Navy to Build Its 'Information Dominance' Forces Through New Command

By Jared Serbu, Federal News Radio, 2/24/2014

The Navy says it's about to create a new home for its growing cadre of what it calls "information dominance" forces.

A new organization will begin to take shape this fall, taking on the responsibility for manning, training and equipping the entire service for information warfare.

The move is a significant follow-up to the Navy's 2009 decision to merge several disciplines, including cyber, intelligence, meteorology, oceanography and electronic warfare into a single large workforce cadre called "information dominance forces."

Within the next few weeks, officials expect Chief of Naval Operations Jonathan Greenert to sign off on an implementation plan to stand up a new command to continue to build and organize that force.

Vice Adm. Ted Branch, a deputy chief of naval operations and the Navy's chief of information dominance, said the service expects the new organization to reach its initial operating capability by October. It will fall within the auspices of the existing Navy Cyber Forces, headquartered in Suffolk, Va.

"That means that resources will move from my staff at the Pentagon, from the Office of Naval Intelligence, from the commander of naval oceanography and from Fleet Cyber Command into that new type command," Branch said Friday during an AFCEA gathering in Tysons Corner, Va. "That type commander will be responsible for the manning, training and equipping of the entire information dominance corps and for moving forward information dominance in the Navy."

The ninth command

The Information Dominance Forces Command would be the ninth type command (TYCOM) in the Navy, and would have similar responsibilities to the others, but a broader reach. The others are all responsible for holding administrative control over specific categories of platforms, like naval aircraft, submarines or surface ships.

"For the platform TYCOMs, it's pretty easy to figure out what they're dealing with if it looks like a ship or a submarine or an airplane. This one will have the information dominance corps and the cyber activities, all that kind of man train and equip, but it will also have responsibility for the rest of the Navy," Branch said. "The systems commands, naval reactors, medical, anybody that has a network will have a line to the information dominance TYCOM. So it's a big job, but it's the right thing to do as we move information dominance down the path and make it a warfighting pillar."

Navy officials say the standup of the command will mean some other changes to the way the service organizes its current cyber workforce.

Some of Navy Cyber Forces' existing responsibilities for operating and defending Navy networks will transition to the service's 10th Fleet/Fleet Cyber Command, the Navy component of U.S. Cyber Command. Navy Cyber Forces, meanwhile, will focus more exclusively on training and equipping the workforce.

Branch said the new organization's relatively difficult task will be to integrate the skills and expertise of what used to be five distinct career fields in the Navy: Intelligence specialists, information warfare officers, information professionals, oceanographers and the space cadre.

"We brought that all together and said, 'OK, we used to be five different tribes, now we're going to be one corps and be able to practice information dominance warfare,'" Branch said. "That's moving along, but it's not cooked yet, because people who grew up in those different specialties are pretty zealous about what those specialties bring to the game, and they don't want to lose their identities. I tell people all the time, though, that we're not trying to homogenize the community or diminish the depth of expertise. What we're doing is providing a broader experience. We're doing cross-detailing so we can move from a multidisciplinary group of

folks to an interdisciplinary corps, so we can innovate and find answers to some of the far-reaching decisions we're going to make as we apply these new systems and techniques for information warfare in the future."

Information dominance as warfighters

The Navy says its information dominance strategy, initiated when it first combined its top officer billets for intelligence and for communications into the job Branch currently holds, is based on the idea that it ought to be able to synthesize skill sets its sailors already hold in various communities across the service into a single warfighting capability.

The eventual goal, Branch said, is to have information dominance leaders sitting at the same table, at the same level as other decision makers in, for example, a carrier strike group.

"We will have arrived when we have our internal audience, the information dominance corps, thinking of themselves as warfighters," he said. "And probably more importantly, when the rest of the guys, the kinetic guys, the trigger-pullers start thinking of the information dominance corps as warfighters, we'll get there."

Table of Contents

Shelton Announces New Space Situational Awareness Satellite Program

By Senior Airman Zachary Vucic, Air Force News Service, February 24, 2014

ORLANDO, Fla. (AFNS) -- The commander of Air Force Space Command announced a new satellite program during a speech about the importance of space and cyberspace at the Air Force Association Air Warfare Symposium and Technology exposition, Feb. 21, here.

General William Shelton told the audience about the new Geosynchronous Space Situational Awareness Program with two satellites being launched on the same launch vehicle later this year.

“GSSAP will present a significant improvement in space object surveillance, not only for better collision avoidance, but also for detecting threats,” Shelton said. “GSSAP will bolster our ability to discern when adversaries attempt to avoid detection and to discover capabilities they may have, which might be harmful to our critical assets at these higher altitudes.”

According to a new fact sheet on GSSAP posted on the AFSPC website, the program will be a space-based capability operating in near-geosynchronous orbit, supporting U.S. Strategic Command space surveillance operations as a dedicated Space Surveillance Network sensor. GSSAP will allow more accurate tracking and characterization of man-made orbiting objects, uniquely contribute to timely and accurate orbital predictions, enhance knowledge of the geosynchronous orbit environment, and further enable space flight safety to include satellite collision avoidance.

Shelton announced the program during a speech that conveyed concern about the increasingly complex and contested space and cyber environments. He said space and cyberspace are very much a part of everything we do. The dependence on, and demand for, space and cyberspace is higher than it’s ever been, he said, noting the changes that have occurred over the years, with 170 countries now having a tangible interest in space to include 11 countries with indigenous launch capability.

He said there are no midterm alternatives to the capability provided by space.

“If we’re going to be a global power, we want global coverage, we want global access and we want it at a time and a place of our choosing,” Shelton said.

Speaking specifically about space, Shelton said despite the increased dependence, the declining budget creates challenges to meet the rising demand. The demand for space includes surveillance, tracking and communication.

In addition the focus and actions the Air Force and the nation are taking on space situational awareness, he discussed need for survivability and resilience of our satellite constellations. With the additional challenge of declining budgets, Shelton said, “What we’re really looking for is the nexus of required capability, affordability and resilience” for the nation’s space systems.

“The study work we are doing right now will be effectual for new solutions in the mid 2020 timeframe,” he said. “But we’ve got to get that work done now.”

Shelton closed the space portion of his presentation by talking about the Space Security and Defense Program, a vital program that helps find ways to protect the Air Force’s spacecraft. SSDP looks at available intelligence and adversary counter space programs, and recommends solutions. He said the program has been a “big plus” for situational awareness and has tangible results in many other areas, even in its early stages.

“(Air Force Space Command) is working very hard to get it right for the future,” he said. “(Space) is a vital capability for the nation, for the joint force. We can’t let them down, and we won’t.”

Moving on to cyberspace, the general said it is very different than any other domain as it’s man-made and unlike the physical domains people have learned to use over time. Cyberspace more and more defines modern life in the 21st century.

He said cyberspace creates a big advantage in regards to how many people the military has to put in harm’s way, however the country’s adversaries know cyberspace is the nation’s lifeline. Because of this, high-end operators are constantly threatening U.S. systems.

“We’ve got a lot of cyber enabled weapons these days,” he said. “If an adversary can get in and make that weapon system ineffective at the worst possible time – think about that.

“As we’ve grown our dependence on cyberspace for all the right reasons, it has become an increasingly contested environment for all the wrong reasons. The threats have grown in both sophistication and in number.

A laptop, the right skill set and an internet connection is all one needs to become a player in cyber warfare, making the low “cost of admission” a major complication.

“We can spend a great deal of treasure on defenses, only to be overtaken by the exquisite talents of a high-end cyber operator who has very little capital invested,” Shelton said, noting anonymity makes attribution of these attacks difficult.

Though the cyber domain is different from any other domain, the application of standard military process is doing well to mitigate a lot of the risk, he said. Air Force Space Command is developing several tools to conduct cyberspace operations including the potential for offensive cyber capability.

“Our Airmen and industry partners are facing up to these cyber challenges each and every day, and they are ensuring the mission gets done in the ‘wild west’ of cyberspace,” Shelton said. “We’ve come a long way in space and cyber these last few years. We continue to provide game-changing capabilities to the warfighter … I think the future of warfare really depends on us having the best, most secure and most capable space and cyber systems.”

U.S. Cyber Command recently established a cyber-mission force concept to conduct full-spectrum cyber operations across the Department of Defense, he said. Over the next three years, the Air Force will provide 39 teams, roughly 2,200 Airmen, to contribute to this cyber mission force.

“We must be prepared as a nation to succeed in increasingly complex and contested space and cyber environments, especially in these domains where traditional deterrence theory probably doesn’t apply,” he said. “We can’t afford to wait … for that catalyzing event that will prod us to action.”

Table of Contents

Cyber in Waffle House land

By Jan Kallberg, C4ISR & Networks, 27 Nov 2013

The epicenter of cyber is Washington, D.C., and the discourse radiates from the national capital outward. The question is how far from the Beltway it reaches. Does the rest of this nation care about the national security threat that is embedded in future adversarial cyber operations?

One of my major cyber concerns for the next 10 years is how to disseminate the cyber knowledge into small-town America. The vast majority of the utilities, plants and local government facilities are located in small towns and communities. The United States has 3,500 counties, 18,000 state and local police departments, and 50,000 water utilities of various sizes — just to give you an idea of the scale of local government. This disconnect between the federal level and the local communities is nothing unique for cyber. Implementation is a challenge for every public program just because the sheer size of the volume of information and guidance that have to be communicated, disseminated and checked.

Cyber is unique because it allows states to engage in a conflict within another country and engage the target with limited ability for the targeted nation to identify, intercept and prevent the attack. This increases the number of potential targets astronomically and it also affects the society at all levels and locales when every part of our society can be cyber attacked.

I live in a small town with two Waffle Houses, one IHOP and one post office where you are greeted as family, but it also has three major food-processing plants, a rubber factory, a larger energy utility and a sizeable sawmill. Cyber security is naturally a part of the operating procedures for the major corporations, but is not

really on most people's mind. Here lies the challenge: How can we change the mindset so cyber is seen as a local problem and not an issue to be handed off to the federal government?

The critical infrastructure and the manufacturing base of America are located in thousands of these small towns. If the drive for increased cyber security and ability to reach national cyber resilience do not reach these communities, these incentives are pointless exercises.

Table of Contents

Cyber Beyond Computers - The Environmental Aspect

By Jan Kallberg, C4ISR & Networks, Feb. 7, 2014

A forgotten aspect on cyber and cyber conflicts impact on our society is the fact that tampering with our control systems can lead to industrial processes running amok - and lead to environmental damages. Threats to our environment are taken very serious by the population and pollution and contamination of our living space trigger drastic reactions.

We are surrounded by materials and liquids that could be harmful if released or mixed. An example is the sizeable U.S. chemical industry. Manufacturing plants and storage facilities store large quantities of industrial chemicals. The U.S. chemical industry produces chemical products to a value of $759 billion in 2011. More than 96 percent of all manufactured products in the U.S. are relying on chemical input material.

The U.S. is responsible for 15 percent of the world's chemical production. In the U.S., each year is 847 million tons of chemicals transported on railways, highways, and freight ships. The transportation routes are near to creeks, rivers, ground water aquifers, urban areas, and agricultural land. These chemical fluids can, once released, create contamination that require long-term mitigation, restoration, and in some cases land subsidence equal to an EPA Superfund site.

Environmental hazards that lead to loss of life, and dramatic long-term loss of quality of life for citizens, trigger a demand for the government to act. If the population questions the government's ability to protect and safeguard, the government's legitimacy and authority will suffer.

One example is the Three Mile Island accident, which had an impact, even decades after the incident, on how citizens perceived the government's nuclear policies and ability to ensure that nuclear power was a safe energy source. Harold R. Denton, the Director of the Office of Nuclear Reactor Regulation, was able to calm the public and reduce the fear during the Three Mile Island accident. During the duration of the events Harold R. Denton was President Jimmy Carter's personal representative at the site. It was essential for President Carter to show and project ability to handle the incident and to restore confidence in the general public for the government's energy policies. The public notion of environmental risk is driven not only by logic, but also emotions, foremost by uncertainty and fear of the future. A population that fears the future has lost confidence in government.

The difference with the Three Mile Island incident and cyber attacks on our infrastructure creating environmental damage is that the Three Mile Island incident was local, and it could be contained and understood.

For an adversarial nation that seeks to influence our population and inject fear, cyber-created environmental damages have a high payoff -- especially if the cyber operations are covert and unlikely to be attributed. Is it legal by international law? No, of course not, but these adversarial countries are often not bothered by legal "technicalities," and the question is rather their perception of the risk of detection and strength of a potential U.S. retaliation.

If an adversarial nation can inject fear in fraction of our population they have an option they can use at their discretion. Therefore cyberdefense must go beyond the information systems and look at the broader picture.

Table of Contents

Kiwi Spies Taught 'Honey Trap' Tricks - Snowden Documents

From TVNZ, February 26, 2014

Kiwi spooks were briefed on setting honey traps and internet "dirty tricks" to "control, infiltrate, manipulate, and warp" online discourse, documents leaked by Edward Snowden reveal.

Government Communications Security Bureau (GCSB) agents - part of the Five Eyes intelligence network - were briefed by counterparts from the ultra-secret Joint Threat Research Intelligence Group. A slide-show presentation, called "The Art of Deception: Training for Online Covert Operations", was given at a top secret spy conference in 2012.

It outlined sex and dirty tricks cyber operations used by JTRIG, a unit of the British Signals intelligence agency GCHQ which focused on cyber forensics, espionage and covert operations. GCHQ described the purpose of the unit as "using online techniques to make something happen in the real or cyber world," including "information ops (influence or disruption)."

According to the slides, JTRIG conducted "honey traps," sent computer viruses, deleted the online presence of targets and engaged in cyber-attacks on the "hacktivist" collective Anonymous.

One carried the title "Cyber offensive session: pushing the boundaries and action against hacktivism" revealing the agency was going after online political activists.

Reputation destroying tactics

The presentation outlined tactics to destroy the reputation of targets online. It detailed how agents could get another country to "believe a secret" by placing information on a compromised computer or making it visible on networks under surveillance.

A JTRIG tool, called AMBASSADORS RECEPTION, involved sending a virus to someone's computer to stop it functioning. It would delete emails, encrypt files, make the screen shake, deny service or stop log-ins.

Other methods were deployed to "stop someone communicating," bombarding their phone with text messages and calls - in some cases every 10 seconds, deleting their online presence and blocking up their fax machines. According to the presentation these tactics were used in Afghanistan "significantly disrupting Taliban Operations."

Changing a profile photo on social networking sites "can take paranoia to a whole new level." A honey trap was described as "a great option" and "very successful when it works." Writing false blogs, pretending to be a "victim" of a target worked in "serious crime ops" and in Iran, the conference was told.

The documents were presented to the GCSB, NSA and agents from Australia and Canada.

Author and journalist Glen Greenwald worked with MSNBC to reveal the documents. On "The Intercept" website he wrote that the agencies were "attempting to control, infiltrate, manipulate and warp online discourse, and in doing so are compromising the integrity of the internet itself."

Table of Contents

Army Issues Guidance on Cyberspace Operations

From Federation of American Scientists blog, 20 Feb 2014

For the first time the U.S. Army has produced official doctrine on military activities in cyberspace, including offensive, defensive and network operations.

A new Army field manual “provides overarching doctrinal guidance and direction for conducting cyber electromagnetic activities (CEMA)…. It provides enough guidance for commanders and their staffs to develop innovative approaches to seize, retain, and exploit advantages throughout an operational environment.”

It is “the first doctrinal field manual of its kind.” See FM 3-38, Cyber Electromagnetic Activities, February 2014.

The manual introduces the fundamentals of cyber operations, or “cyber electromagnetic activities” (CEMA), defining terms and identifying important operational factors and constraints.

“Today’s Army must operate in cyberspace and leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested.”

However, “execution of CEMA can involve significant legal and policy considerations.” Also, “possibilities of unintended or cascading effects exist and may be difficult to predict.”

Several years ago, any official discussion of offensive cyber operations was considered classified information. That is no longer the case, and the new Army manual — which itself is unclassified — treats the subject as a normal part of military conflict.

“Army forces conduct OCO [offensive cyberspace operations] across the range of military operations by targeting enemy and hostile adversary activity and related capabilities in and through cyberspace,” the Field Manual says.

Cyberspace attacks in support of offensive operations “may be directed at information resident in, or in transit between, computers (including mobile phones and personal digital assistants) and computer networks used by an enemy or adversary.”

“Cyberspace attacks may employ capabilities such as tailored computer code in and through various network nodes such as servers, bridges, firewalls, sensors, protocols, operating systems, and hardware associated with

computers or processors. Tailored computer code is only one example of a cyberspace capability… designed to create an effect in or through cyberspace."

"Cyberspace attacks may employ manipulation which includes deception, decoying, conditioning, and spoofing to control or change information, information systems, and networks."

The Army manual also presents doctrine on defensive cyberspace operations and on information network operations. "[Defensive] countermeasures in cyberspace should not destroy or significantly impede the operations or functionality of the network they are being employed against, nor should they intentionally cause injury or the loss of life."

The manual devotes some attention to the legal framework governing cyber operations, which "depends on the nature of the activities conducted." Under all circumstances, the manual says, "Army forces conducting CO [cyberspace operations] will comply with the law of war."

Ordinarily, the manual states, the U.S. Army should not be conducting offensive cyber operations against U.S. targets. "Unless approved by appropriate authorities, Army assets cannot be used to perform attack or exploit operations on U.S. entities."

"Commanders must ensure that the legal, constitutional, and privacy rights of U.S. citizens are protected throughout the planning and execution of [cyber operations]."

Table of Contents

Inside the Army's First Field Manual for Cyber Electromagnetic War

By Patrick Tucker, DefenseOne, February 26, 2014

The Pentagon long has made a big effort to showcase its budding cyberwarfare capabilities. But the military has been less forthcoming about a key, more tangible component of cyber - electronic warfare - until now.

The Army just publically released its first-ever Field Manual for Cyber Electromagnetic Activities. The manual covers operations related to cyberspace and the electromagnetic spectrum, highlighting that for the Army electronic warfare is every bit as important as the cyber threat we hear so much about in abstract.

Electromagnetic spectrum, or ES, is the entire field of electromagnetic radiation that surrounds all of us, including infrared, radar, TV and radio waves. It's what allows for cellphone and radio communication. The Army's field manual describes a variety of its electronic warfare, or EW, operations - from sending confusing signals and messages that degrade the enemy's communication capability on the battlefield to finding enemy equipment and destroying it with big bursts of electromagnetic radiation. (Remember Goldeneye?) The manual does not explain how to conduct specific EW attacks, but it does provide guidance to soldiers on what these sorts of operations look like in terms of protocol, terminology, and command and control. And it comes right as the number of potential electronic warfare operations is growing with every new radio or internet-dependent device that the military buys.

Want to fly a drone? Get directions from the Global Positioning System? Drop a smart bomb? Use radar to land your plane, communicate with a forward operating base on a mountaintop in Afghanistan, find an improvised explosive device or, better yet, detonate one? Then you'll need access to the electromagnetic spectrum. Even door locks that use radio-frequency ID, requiring the chipped common access (CAC) ID card that Army employees carry, use electromagnetic radiation.

The military has been fighting to maintain spectrum dominance since the days of World War II radio jamming. But reliance on the spectrum is going to grow considerably in the future and take a variety of forms. The lower ends of the spectrum are useful for radio and cell communication, including Bluetooth exchanges. The frequencies at the higher end of the spectrum have applications for things like cruise missile targeting and lasers. Extremely sophisticated (and expensive) military equipment like the Army's proposed laser truck, which would shoot down enemy drones, might use spectrum frequencies in a wide number of different ways.

But the spectrum doesn't just represent a weapon. It's also a gaping vulnerability. The U.S. doesn't have a monopoly on the atom-sized units of energy that make up electromagnetic radiation. In the last few years, off-the-shelf pieces of wireless communications equipment have allowed everyone from hobbyists to terrorists to access the spectrum cheaply and easily. In the past decade, as more wireless consumer electronics flooded the marketplace, that vulnerability has taken the form of IEDs on the battlefields of Iraq and Afghanistan (as well as the streets of Boston during the 2013 marathon bombing).

To patch the hole, the Army established a new career field dedicated to electronic warfare in 2009. Unfortunately, the military's reliance on the spectrum might be growing faster than our ability to keep hold of it.

"The American military is scrambling to develop new tools and techniques that will help it preserve its electromagnetic edge," according to Wired's Brendan Koerner. "But that edge continues to shrink by the day, and very soon our inability to completely control the spectrum might result in a different kind of war."

It's an issue that the Defense Department publicaly addressed again last week with the release of its Electromagnetic Spectrum Strategy. There's a push to use the spectrum much more efficiently as the military seeks to access much more of it. That's either an irreconcilable conflict of wants and available resources or a very delicate balancing act. DOD contends it's the later. "We are not certainly making the assumption that DOD will have to make do with less spectrum," said the Pentagon's chief information officer, Teri Taki.

On the cyber side, the manual offers detailed descriptions of who responds to whom in an cyber-operation and how the various roles differ; priority lists for unit activities (hint: defend first, then attack); functions of cyberspace operations; how to prepare the intelligence battlefield; what to attack in order to achieve what goals; and the multinational and legal considerations for various actions.

Both cyber operations and spectrum warfare fall under the category of electronic communication. But experts who saw the manual disagreed, somewhat, on the decision to group the two together in one field guide. Do IEDs and denial-of-service attacks really have that much in common?

"There has been some debate about how traditional EW capacity will play with newer cyber operations. While there are strong similarities, cyber operations have a broader range of capacities than the traditional EW strategic role, and can support a wider range of operations. Similarly, the counter-EW capacity has a more limited scope than the huge needs to defend our military infrastructure from cyber exploitation and disruption," Allan Friedman, co-author of the book Cybersecurity and Cyberwar: What Everyone Needs to Know told Defense One.

Retired Lt. Gen. Robert Elder, a George Mason University research professor and former Air Force cyber officer, argues that electronic warfare and cyber warfare indeed are closely related and should be treated as such. "The new [field manual] makes it clear that conducting these activities independently may detract from their efficient employment," he said. "This provides a useful mechanism for the traditional and [cyber electromagnetic activities] communities to effectively communicate with one another."

The overlap between EW operations, related to drones, communications, and improvised explosive devices on the battlefield, and cyberwarfare, which we commonly think of as being about ones, zeros and spam, shows that the Army is evolving its view of both fields.

For U.S. soldiers, according to this new manual, cyber and electronic are the same. Eventually the term cyberwar may soon become obsolete. It might be time to just call it war.

Table of Contents

This Is the App That's Fueling the Uprising in Venezuela

By Patrick Tucker, DefenseOne, February 24, 2014

Entrepreneur Bill Moore was in his Austin, Texas, office last Thursday, watching explosive growth for his company's walkie-talkie app, Zello, inside Venezuela. Zello had become the favorite app of protest organizers there after recently hitting the mark as the most popular app in Ukraine. Over the past few days in Venezuela, the protests ballooned following rapidly rising food prices, controversy over President Nicolas Maduro's economic policies, public dissatisfaction over crime and multiple other factors.

Moore was finding that in Venezuela that popularity had a price. Shortly after 9 p.m., his Twitter feed blew up with messages from users inside the country. The government-owned Internet service provider, CANTV, which hosts 90 percent of Venezuela's Internet traffic, was blocking the app as well as access to Zello's website. Downloads were dropping off considerably.

Zello sent out the following Tweet: "If you are in Venezuela and familiar with network diagnostics tools, please respond, we need your help to understand the block applied."

As Moore describes it, the response, like the protests themselves, was immediate and enormous. People inside Venezuela and many more from around the world wrote in with advice. Moore, Alexey Gavrilov, Zello's co-founder and chief technical officer, and the company's programmers worked feverishly through the night on a new version of the app to get around the CANTV blockade. "This was the most important thing in the company," Moore told Defense One. "We said, 'How do we get this done?'"

Finally, at about 5 p.m. the following day, an updated version was ready to go. The company released this tweet: "Android users in Venezuela, who cannot access the app. Please try this version and report back results."

Despite the efforts of the Maduro government, protests in Venezuela are continuing and so are downloads of Zello, one fueling the other. It's a cycle that's reminiscent of the very early days of the Arab Spring in 2010 and 2011, in which students and other protestors used social networks like Twitter and Facebook to help organize, promote and communicate through protests, eventually forcing the ouster of nondemocratic governments in places like Tunisia and Egypt.

The lesson from the events in Tunisia in particular seemed to be that when you combine an educated student class with the power of social networks and press the return key, the outcome can be democracy. But when the machine malfunctions, the result can look like a protracted war with the potential to embroil U.S. forces. The protests in Libya, in contrast, resulted in a civil war costing more than $1 billion to the U.S. and NATO. When the machine breaks down completely, the result looks like Syria, or possibly Iran, where the regime has been extremely successful shutting the opposition out of the Internet.

To Moore, Venezuela looks like digital trench warfare with governments working feverishly to outmaneuver software makers and vice versa.

Founded in Austin in 2011, Zello allows individuals to communicate to one another walkie-talkie style via a simple broadband connection. The app interface looks a like button on your phone. You press it to speak to people on a particular channel. The channels can be as small as two people or as big as hundreds of thousands. The largest in Venezuela is about 450,000, but only 600 can be active on a channel at one time, Moore said. The feel of the app is similar to the now defunct Nextel push-to-talk service, which was shut down last summer. Zello is free for individuals but companies can purchase a plan to allow more users on a single channel for $10 a month.

Zello has been downloaded some 50 million times. In addition to playing a big role in the recent Ukraine protests, it was also extremely popular during last year's unrest in Turkey.

Moore never imagined that what he was making could become a politically destabilizing force. He knew only that he wanted to make a social network around the idea of Internet-based radio. "The human voice carries so much more information than typing. We knew that was the basis of something great. If you listen to these channels you realize that it's a way for people to make friends. The surprise was that that it exploded in Turkey almost a year ago to become the number one app in Turkey around the issues that they had, and then in Venezuela."

In emails, multiple protestors said that they saw Zello as an essential tool for coordinating movement, collecting intelligence on the location of government forces, and organizing responses. In other words, Zello has clear military potential. The company reports that it has received interest from the U.S. National Guard and the United States Army Reserve Command

But Zello, which has been downloaded more than 600,000 times in Venezuela in just a few days, has seen multiple uses, some of these extend beyond calling for marches and launching maneuvers to evade the authorities. They include organizing guarimbas, blockades of burning trash, to thwart National Guard and police movements. The erection of the guarimbas represents a clear escalation in protestor tactics away from simple peaceful marches and some report that the blockades have contributed to the casualty count, which officially hit 11 over the weekend. The use of guarimbasis controversial among the protestors and has been met with extremely harsh responses from troops as demonstrated in this video.

The openness of the Zello platform explains why it's become so useful across Venezuela, but this ease of use has also led to a digital fog of war with confusion about who is using the network for what purpose. According to protestors, the government and government-supporting militia groups, or colectivos, will listen in on protestor channels on Zello to get information about upcoming movements or marches, distribute disinformation, or learn the identities of people on the other side. This has led to calls from protestor groups on Twitter to abandon use of the walkie-talkie app.

Moore, who says his company has no direct stake in Venezuelan politics, said there's a simple fix to these problems: the platform allows users to create one-way communication channels, multiple communication channels, or closed channels where users must be granted to access to join. It can work like a giant open microphone, a conference call, or a radio-station.

Abelardo Jesus Marquez, a Venezuelan technology consultant and blogger sympathetic to the protest movement, said in an email that part of the problem was that too many Zello users were simply unaware of the most secure and effective ways to use the service. "The logical question would be, why [don't] they use closed channels protected by passwords? They ignore the security implications."

The confusion among protestors using the app as well as the government shutdown of Zello and the company's quick response, speak to the fact that digital revolution is more complicated in Venezuela today than it was in Tunisia in 2011.

“During the Arab spring we saw the power of social media to organize people around freedom. Governments have caught on to understand that their ability to restrict this information is important. These governments will continue to restrict these [services],” said Ryan Dochuk, founder of a Toronto-based company called TunnelBear that offers Internet encryption services. Dochuk said TunnelBear has seen an enormous uptick in usage in Venezuela in the last few days, primarily through Twitter.

TunnelBear’s encryption service hides the way the user is accessing the Internet, what websites he or she is visiting and what is being downloaded. It offers what’s called a virtual private network, or VPN, within a larger Internet service provider. (Another example is TOR.) When a VPN is working, it functions as an invisibility cloak. In Venezuela, it’s allowing people to access banned Web sites and apps, such as Zello.

TunnelBear offers a free service for moderate data usage and two other plans for more heavy usage. In response to user demand, the company has made TunnelBear completely free inside Venezuela.

The decision was not an easy one. “When you decide to open up your network for free, there’s financial decisions at play. There’s emotional decisions at play. You open your inbox on a Friday morning and you see dozens of stories of people requiring assistance,” Dochuk said. “We’ll support these efforts where we can, but it’s by no means full proof.”

Dochuk, like Moore, has no direct interest in Venezuelan politics. But he’s opposed to censorship on principle. And TunnelBear already had a lot of users in Venezuela. When he heard that the government was trying block Internet access, he knew that he had to make the service free where it was needed most. But the company would really prefer not to get overly involved in conflict areas, and so the rising death toll in Venezuela is worrisome. Also, he knows that there’s only so much an encrypted network can do. In places where government censorship operations are sophisticated, like in China, Syria or Iran, TunnelBear is non-existent. (Dochuk recommends users in these countries try TOR.)

The national security implications of app wars in conflict areas can’t be understated. Whether Venezuela will follow the path of Tunisia, Libya, Syria or Iran remains to be seen. The outcome depends on multiple factors. But one is how well different sides in the emerging conflict leverage technologies like Zello and TunnelBear to achieve their objectives. Though it sounds hyperbolic, the future of Venezuela, and U.S. involvement in that country, may depend on which side makes better use of this sort of technology in the coming days and weeks. Dochuk is guardedly optimistic.

“Technology can move much faster than these governments, and I think over time, these groups will be successful getting information and freedom out.”

Table of Contents