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. 03 (March - April 2014)

The Chinese People's Liberation Army and Information Warfare

By Larry Wortzel, U.S. Army War College Strategic Studies Institute, 5 March 2014

On November 23, 2013, China's Ministry of National Defense spokesman announced that a new air defense intercept zone (ADIZ) will be established by the government to include the Diaoyu, or Senkaku Islands. Sovereignty over these islands is disputed by Japan, China, and Taiwan. Pundits and policy analysts quickly engaged in a broad debate about whether China's expanded ADIZ is designed to create tension in Asia, or is part of a broader plan to impose a new definition of China's territorial space in the Asia-Pacific region. Meanwhile, to deal with cyber penetrations attributed to the Chinese People's Liberation Army (PLA), the U.S. Departments of Justice, Homeland Security, and State are devising new means to protect intellectual property and secrets from the PLA's computer network operations.

The ADIZ announcement by China is an example of the PLA General Political Department engagement in what it calls "legal warfare," part of the PLA's "three warfares." In expanding its ADIZ, China is stretching International Civil Aviation Organization regulations to reinforce its territorial claims over the Senkaku Islands. On another level, the Chinese government will use the ADIZ as a way to increase the airspace it can monitor and control off its coast; the Chinese government is already suing the navy and maritime law enforcement ships to enforce these claims at sea. Additionally, the PLA and the Chinese government have sent a major signal to Taiwan, demonstrating another aspect of the "three warfares." When the Chinese Ministry of National Defense put its expanded ADIZ into effect, the new zone carefully avoided any infringement into Taiwan's ADIZ, signaling that in addition to the improved economic ties with Taiwan, there is room for political improvement across the Taiwan Strait.

The PLA spent more than a decade examining U.S. military publications on network-centric warfare and the evolution of American doctrine on information warfare. After observing American information operations in the Balkans and the first Gulf War, the PLA saw the effect of modern information operations on the battlefield and in the international arena. The PLA then began to implement its own form of information warfare. The Chinese military has adopted information warfare concepts suited to its own organization and doctrine—blending its own traditional tactics, concepts from the Soviet military, and U.S. doctrine to bring the PLA into the information age. At the same time, the PLA has modernized and improved upon its own psychological warfare operations and expanded the role of its legal scholars in justifying military action and territorial claims.

The PLA's command, control, communications, computers, intelligence, surveillance, and reconnaissance programs support the ground forces, navy, air force, missile forces, nuclear doctrine, and space warfare. China's military doctrine depends on incorporating information technology and networked information operations. The PLA's operational concepts for employing traditional signals intelligence and electronic warfare have expanded to include cyber warfare; kinetic and cyber attacks on satellites; and information confrontation operations across the electromagnetic spectrum. As this monograph explains, the PLA used innovative means to expand on Cold War Soviet doctrine on "radio-electronic combat," which called for a combination of jamming and precision air, missile, and artillery strikes on North Atlantic Treaty Organization forces. The Chinese military, however, apparently intends to conduct these activities at the tactical, operational, and strategic levels of war, envisioning attacks on an enemy's homeland critical infrastructure and points of embarkation.

Along with these more technical aspects of information operations, the PLA's combination of psychological warfare; the manipulation of public opinion, or media warfare; and the manipulation of legal arguments to strengthen China's diplomatic and security position, or what China calls "legal warfare," join together in a comprehensive information operations doctrine. This monograph explains how the PLA is revising its operational doctrine to meet what it sees as the new mode of "integrated, joint operations" for the 21st century. An understanding of the PLA's new concepts is important for U.S. and allied military leaders and planners.

NOTE: Download complete publication at http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1191 (3.4Mb)

Table of Contents

There's No Real Difference between Online Espionage and Online Attack

By Bruce Schneier, the Atlantic, Mar 6 2014

Back when we first started getting reports of the Chinese breaking into U.S. computer networks for espionage purposes, we described it in some very strong language. We called the Chinese actions cyber-attacks. We sometimes even invoked the word cyberwar, and declared that a cyber-attack was an act of war.

When Edward Snowden revealed that the NSA has been doing exactly the same thing as the Chinese to computer networks around the world, we used much more moderate language to describe U.S. actions: words like espionage, or intelligence gathering, or spying. We stressed that it's a peacetime activity, and that everyone does it.

The reality is somewhere in the middle, and the problem is that our intuitions are based on history.

Electronic espionage is different today than it was in the pre-Internet days of the Cold War. Eavesdropping isn't passive anymore. It's not the electronic equivalent of sitting close to someone and overhearing a conversation. It's not passively monitoring a communications circuit. It's more likely to involve actively breaking into an adversary's computer network—be it Chinese, Brazilian, or Belgian—and installing malicious software designed to take over that network.

In other words, it's hacking. Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs.

The abbreviation-happy U.S. military has two related terms for what it does in cyberspace. CNE stands for "computer network exfiltration." That's spying. CNA stands for "computer network attack." That includes actions designed to destroy or otherwise incapacitate enemy networks. That's—among other things—sabotage.

CNE and CNA are not solely in the purview of the U.S.; everyone does it. We know that other countries are building their offensive cyberwar capabilities. We have discovered sophisticated surveillance networks from other countries with names like GhostNet, Red October, The Mask. We don't know who was behind them—these networks are very difficult to trace back to their source—but we suspect China, Russia, and Spain, respectively. We recently learned of a hacking tool called RCS that's used by 21 governments: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan.

When the Chinese company Huawei tried to sell networking equipment to the U.S., the government considered that equipment a "national security threat," rightly fearing that those switches were backdoored to allow the Chinese government both to eavesdrop and attack US networks. Now we know that the NSA is doing the exact same thing to American-made equipment sold in China, as well as to those very same Huawei switches.

The problem is that, from the point of view of the object of an attack, CNE and CNA look the same as each other, except for the end result. Today's surveillance systems involve breaking into the computers and installing malware, just as cybercriminals do when they want your money. And just like Stuxnet: the U.S./Israeli cyberweapon that disabled the Natanz nuclear facility in Iran in 2010.

This is what Microsoft's General Counsel Brad Smith meant when he said: "Indeed, government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."

When the Chinese penetrate U.S. computer networks, which they do with alarming regularity, we don't really know what they're doing. Are they modifying our hardware and software to just eavesdrop, or are they leaving "logic bombs" that could be triggered to do real damage at some future time? It can be impossible to tell. As a 2011 EU cybersecurity policy document stated (page 7):

> *...technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyberwarfare can well be cyberespionage initially or simply be disguised as such.*

We can't tell the intentions of the Chinese, and they can't tell ours, either.

Much of the current debate in the U.S. is over what the NSA should be allowed to do, and whether limiting the NSA somehow empowers other governments. That's the wrong debate. We don't get to choose between a world where the NSA spies and one where the Chinese spy. Our choice is between a world where our information infrastructure is vulnerable to all attackers or secure for all users.

As long as cyber-espionage equals cyber-attack, we would be much safer if we focused the NSA's efforts on securing the Internet from these attacks. True, we wouldn't get the same level of access to information flows around the world. But we would be protecting the world's information flows—including our own—from both eavesdropping and more damaging attacks. We would be protecting our information flows from governments, nonstate actors, and criminals. We would be making the world safer.

Offensive military operations in cyberspace, be they CNE or CNA, should be the purview of the military. In the U.S., that's CyberCommand. Such operations should be recognized as offensive military actions, and should be approved at the highest levels of the executive branch, and be subject to the same international law standards that govern acts of war in the offline world.

If we're going to attack another country's electronic infrastructure, we should treat it like any other attack on a foreign country. It's no longer just espionage, it's a cyber-attack.

Table of Contents

Information Warfare: The Iridium Hotspot

From Strategy Page, 7 March 2014

March 7, 2014: The U.S. Department of Defense has arranged for satellite telephone service provider Iridium to supply small (300 gr/10.3 ounce and the size of a small paperback) battery powered Iridium GO! devices that can connect to the Iridium satphone network and provide a local wifi hotspot. Up to five users with a wifi devices within about 30 meters (a hundred feet) of the Iridium GO! can have Internet access. That means smartphones or tablets can use texting, Skype to make phone calls or a browser for web search and limited downloading. All of this uses military encryption. The Iridium Go! devices will cost the Department of Defense $800 each and the Iridium service is taken care of by the contracts the Department of Defense has had with Iridium for over a decade. Currently the Department of Defense (which also provides other government agencies with satphone service) is Iridiums largest customer accounting for about 20 percent of revenues.

This tight relationship between Iridium began back in 2000. The Iridium satellite system was put up in the 1990s at a cost of $5.5 billion. Alas, not enough customers could be obtained for the expensive satellite telephone service, and in 2000 the company was not only broke but no one wanted to take over its network of 79 satellites. The situation was so dire that the birds were going to be de-orbited (brought lower so they would burn up in the atmosphere.) Then the Department of Defense stepped in with an offer. For $3 million a month the Department of Defense would get unlimited use of up to 20,000 devices (mostly phones, but also pagers and such.) That was enough for someone to come in and take over the satellite system (which cost more than $3 million a month to operate) and make a go of it. The new owners didn't have the $5.5 billion in debt to worry about and were able to lower prices enough that they were able to sign up 80,000 other customers (civilian and military.)

The Department of Defense paid about $150-$200 a month per satellite phone account under the 2000 contract. Civilian customers paid more and the company thrived. Now Iridium is about to launch a new generation of satellites that will provide faster and cheaper service.

Iridium survived in large part because of the Pentagon business that grew larger after September 11, 2001. In 2013 the Department of Defense signed a five year, $400 million contract with Iridium. There are currently over 51,000 Department of Defense and other U.S. government Iridium users.

Back in 2000 the plan was that each combat brigade would have over 500 satellite phone accounts. That was never needed, in part because the air force and navy wanted lots of satphones as well and the army began using portable satellite dishes to obtain high-speed service from military and commercial communication satellites.

The Iridium and other satellite communications capability was the key to making the battlefield Internet work, although the army has found that it's more efficient (and cheaper) to use military radios and other wireless devices to network with each other and get Internet access via satellite dishes connected with the military satellite communications system. But for many small units out in the bush Iridium is still the way to go.

Table of Contents

Playing by Putin's Tactics

By Molly K. McKew and Gregory A. Maniatis, Washington Post, 9 Mar 2014

References to Vladimir Putin's invasion of Crimea as some sort of "19th-century behavior" misjudge the enormity of recent events. He hasn't miscalculated; Putin is redefining 21st-century warfare.

Before Putin invaded Georgia in August 2008, he spent months deploying the traditional machinery of war. He rebuilt railroads and highways to move tanks and thousands of troops. He sent warplanes menacingly over Georgian territory. He also used state propaganda to muddle the narrative about who started the war.

But Putin is no longer bound by the constraints of nation-state warfare. Years of confrontations with separatists, militants, terrorists and stateless actors influenced his thinking. In Crimea, Putin debuted a pop-up war — nimble and covert — that is likely to be the design of the future.

First, the hidden army appeared out of nowhere. Soldiers-of-no-nation were outfitted for troublemaking and street-fighting. These troops, denied by Putin, are also seemingly unconstrained by the laws, rules and conventions governing warfare — Putin's biggest brush-off yet to international order. They are Putin's hybrid of soldiers and terrorists: hidden faces, hidden command-and-control, hidden orders, but undoubtedly activated to achieve state objectives.

The lack of an identified leader gums up the international community's response. There is no general with whom to negotiate a cease-fire or surrender; if violence erupts, there is potentially no way to end it short of stopping each gunman.

These irregular forces are also a psychological menace for the local population and Ukrainians nationwide, who don't know where else the hidden army awaits.

The second component of Putin's 21st-century warfare is cyber. Calling it propaganda diminishes the insidious and poisonous nature of this information battle.

Cybertactics have been streamlined to Putin's latest purpose: interrupting the communications of legislators and governance, even as the stream of Russian-language misinformation heralding the new war on "fascisti" continues to flow.

Putin has manufactured a version of reality to propagate the narrative he needs to destabilize Ukraine. He decided an ethno-lingual division was needed to achieve his objectives — and then cast parts. Now the story is being acted out on hundreds of fronts and posted on social media, a virtual live-stream of content for Putin's argument of oppression, victimization and fear in Russian-speaking Ukraine.

Reality plays no role in all this. Itar-Tass ran a story last weekend, later picked up by Forbes and others, that 675,000 Ukrainians had recently sought political asylum in Russia. Recall that in August 2008, Moscow claimed that 2,000 civilians had been killed in South Ossetia, a region of Georgia into which it sent and still maintains troops. Human Rights Watch investigators later found that only 44 civilians had died. But Western news agencies cover Putin's fake news as if it were worthy of debate. His distortions and the resulting intimidation slow responses to his actions and dilute the resolve of those who would stand against him.

Third, Putin is using financial markets as a polemical tool. With a personal net worth said to be in the tens of billions, he understands financial might. Russia's wealth has allowed it to forge "partnerships" based on mutual financial interest, and Putin is relying on that web of connections.

Putin has familiarity with such tactics; in 2007, a cyberattack crippled Estonian financial markets for days after a dispute with Russia. Last week, after Russian markets plummeted more than 10 percent amid fears of war, Putin held a news conference scripted to calm investors. Consider how much money he might have lost, and regained, between Monday and Wednesday. Once he perfects his manipulation of markets, Putin can increase his personal wealth and further supplement the web of money that he believes makes him untouchable. It's a self-propagating, invisible weapon.

Ultimately, these tactics create a chaos that he controls, a status quo that allows him to influence the politics and policies of Ukraine.

Putin moved into Crimea partly because it was a low-stakes way to test out his new warfare. Home to significant Russian military assets and a somewhat sympathetic population, Crimea is geographically isolated from the rest of Ukraine; Putin could confidently predict that there would be no physical response to his invasion by a globally exhausted West.

For years, Putin relied on the heavy, Soviet-style hammer. His recent actions suggest that traditional military and intelligence are no longer the means by which he feels he has to fight. While the West is focusing on the best response to his recent steps, Putin is most likely on to the next stages: determining which, if any, international protocols apply to his actions and how his tactics can be used elsewhere.

It's time to give up the decadent belief that continental wars are over. Going forward, the terms by which the world is playing are Putin's — a reality we all must recognize and for which we need an effective response.

Table of Contents

New Attack On HTTPS Crypto Might Reveal If You're Pregnant Or Have Cancer

By Dan Goodin, ars technica, Mar 6 2014

As the most widely used technology to prevent eavesdropping on the Internet, HTTPS encryption has seen its share of attacks, most of which work by exploiting weaknesses that allow snoops to decode cryptographically scrambled traffic. Now there's a novel technique that can pluck out details as personal as someone's sexual orientation or a contemplation of suicide, even when the protection remains intact.

A recently published academic paper titled "I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis" shows how even strongly encrypted Web traffic can reveal highly personal information to employers, Internet service providers, state-sponsored spies, or anyone else with the capability to monitor a connection between a site and the person visiting it. As a result, it's possible for them to know with a high degree of certainty what video someone accessed on Netflix or YouTube, the specific tax form or legal advice someone sought from an online lawyer service, and whether someone visiting the Mayo Clinic website is viewing pages related to pregnancy, headaches, cancer, or suicide.

The attack works by carefully analyzing encrypted traffic and taking note of subtle differences in data size and other characteristics of the encrypted contents. In much the way someone holding a wrapped birthday present can tell if it contains a book, a Blu-ray disk, or a box of candy, an attacker can know with a high degree of certainty the specific URL of the HTTPS-protected website. The transport layer security and secure sockets layer protocols underpinning the Web encryption specifically encrypt the URL, so until now, many people presumed an attacker could only deduce the IP address of a site someone was visiting rather than specific pages belonging to that site.

"The message motivating the technical points and techniques presented in the paper is that, in the case of many HTTPS deployments, maintaining the privacy of which pages a user views within a site matters," Brad Miller, a PhD candidate at the University of California at Berkeley and the lead author of the paper, wrote in an e-mail. "To see why, consider (1) the range of intermediary parties which can access user traffic and (2) what can be inferred from the pages you view within a website."

The researchers targeted 10 websites, including those belonging to the American Civil Liberties Union, Bank of America, Kaiser Permanente, Legal Zoom, the Mayo Clinic, Netflix, Planned Parenthood, Vanguard, Wells Fargo, and YouTube. To create a body of training data, they carefully measured the characteristics of specific URLs of each by visiting them ahead of time. They then monitored other encrypted Web sessions on those sites and used the characteristics to determine when those pages were visited. With an average accuracy rate of 89 percent, they were able to determine the individual pages within those sites. A small sampling on the subject matters, along with the corresponding URLs included:

- Abortion
- Cancer Screenings
- Sexual Orientation
- Sexual Orientation of Child (Google translation here)
- HIV/AIDS
- Unexpected Pregnancy
- Infertility
- Considering Pregnancy
- Morning After Pill
- Suicide
- Pregnancy
- Headaches
- Fingernails

Gauss what?

The researchers relied on Gaussian distribution to find similarities between the traffic observed during the training period and the HTTPS-protected communications traveling between test machines and the websites they visited. To return to the earlier metaphor, the technique is similar to studying the weight, shape, and size of the contents inside a wrapped present. Something small, square, and light is likely to be a Blu-ray disk. Something long, heavy, and showing the outline of a bicycle is probably a bike.

The researchers' job was made much harder by the common use of Web caching and browser cookies, which often remove or modify the contents contained in encrypted traffic from what was observed in the training data. Miller explained:

In the context of the bicycle analogy, imagine trying to figure out if somebody is building a unicycle, bicycle or a tricycle based on individually wrapped parts they receive. Without caching, you can just count the number of wheel shaped objects and you know what is being built. With caching, it could be the case that somebody already has a wheel or two in the garage, so even if you just see one wheel it could be a unicycle, bicycle or tricycle. The upshot is that you have to pay closer attention to the rest of the objects and be able to pick up on smaller details.

The technique should be of concern to privacy advocates, since it could be used by employers to determine if a worker is planning to get pregnant, or by repressive governments to know when people are viewing videos or other content deemed subversive. The paper is another reminder that the mere fact that data is encrypted doesn't mean it doesn't reveal highly personal information. The researchers also provide several countermeasures website operators can employ to prevent leakage, including a technique they dubbed Burst. The paper and its recommendations should be required for any site that provides privacy assurances to its visitors.

Table of Contents

Google is Encrypting Search Globally. That's bad for the NSA and China's Censors.

By Craig Timberg and Jia Lynn Yang, Washington Post, March 12 2014

Google has begun routinely encrypting Web searches conducted in China, posing a bold new challenge to that nation's powerful system for censoring the Internet and tracking what individual users are viewing online.

The company says the move is part of a global expansion of privacy technology designed to thwart surveillance by government intelligence agencies, police and hackers who, with widely available tools, can view e-mails, search queries and video chats when that content is unprotected.

China's Great Firewall, as its censorship system is known, has long intercepted searches for information it deemed politically sensitive. Google's growing use of encryption there means that government monitors are unable to detect when users search for sensitive terms, such as "Dalai Lama" or "Tiananmen Square," because the encryption makes them appear as indecipherable strings of numbers and letters.

China — and other nations, such as Saudi Arabia and Vietnam, that censor the Internet on a national level — will still have the option of blocking Google search services altogether. But governments will have more difficulty filtering content for specific search terms. They also will have more trouble identifying which people are searching for information on sensitive subjects, experts say.

The development is the latest — and perhaps most unexpected — consequence of Edward Snowden's release last year of National Security Agency documents detailing the extent of government surveillance of the Internet. Google and other technology companies responded with major new investments in encryption worldwide.

Chinese officials did not respond to questions about Google's decision to routinely encrypt searches there, but the move threatens to ratchet up long-standing tensions between the American tech powerhouse and the world's most populous nation.

"No matter what the cause is, this will help Chinese netizens to access information they've never seen before," said Percy Alpha, the co-founder of GreatFire.org, an activist group that monitors China's Great Firewall. "It will be a huge headache for Chinese censorship authorities. We hope other companies will follow Google to make encryption by default."

Alpha, who like other members of the group uses a pseudonym to evade Chinese authorities, noted that Google began encrypting searches in the country more than two months after GreatFire.org publicly challenged the company to do so in an opinion piece published by Britain's Guardian newspaper in November.

That piece came in response to a speech by Google's executive chairman, Eric Schmidt, in which he said, "We can end government censorship in a decade" through expanding encryption. GreatFire.org said the company didn't need to wait 10 years; it could encrypt all searches in China far more quickly.

Google denied that the group's agitation had anything to do with the rollout of encryption technology in China, saying that it began in February for unrelated reasons. All searches made from most modern browsers will be

encrypted in the coming months. The completion date for the worldwide rollout is not yet clear, the company said.

“The revelations of this past summer underscored our need to strengthen our networks. Among the many improvements we’ve made in recent months is to encrypt Google Search by default around the world,” spokeswoman Niki Christoff said in an e-mailed statement. “This builds on our work over the past few years to increase the number of our services that are encrypted by default and encourage the industry to adopt stronger security standards. ”

Google largely pulled out of mainland China in 2010, moving many of its operations to the quasi-autonomous base of Hong Kong after refusing to comply with orders to censor searches or redirect them to preferred sites — something that competitors who remained behind still do.

Since then, the company’s share of the search market in China has dwindled to as low as five percent, according to Beijing-based market-research firm Marbridge Consulting. The vast majority of Internet users there use the Chinese search engine Baidu, even on phones running Google’s Android operating system.

This means that the effect of Google’s increased use of encryption could be limited in its reach since those who use Google in China — typically tech-savvy and young — often already know ways past the Great Firewall.

“Those who are technically sophisticated don’t really need another tool to get around censorship,” said Jason Q. Ng, author of “Blocked on Weibo: What Gets Suppressed on China’s Version of Twitter (and Why).

Google began offering encrypted search as an option for some users in 2010 and made the protection automatic for many users in the United States in 2012. The company began encrypting traffic between its data centers after The Washington Post and the Guardian, relying on documents provided by Snowden, reported last year on the massive extent of Internet spying by the National Security Agency and its allies. Microsoft and Yahoo soon followed with similar initiatives.

Encrypted search has come more slowly in other parts of the world, and especially to those using older browsers. Firefox, Safari and Google’s own Chrome browser support automatic encryption, but older generations of Microsoft’s Internet Explorer — still popular in China and much of the world — do not. Internet Explorer 6, which was first released in 2001 and does not support encrypted Google searches, is used for 16 percent of Chinese Internet traffic, according to NetMarketShare.com, which tracks usage.

The move to routine encryption could spark backlash from Chinese authorities, who constantly tweak their Great Firewall to block the flow of unwanted content and also to maintain the ability to monitor Internet users in China.

“The Great Firewall is entirely a moving target,” said Richard Clayton, a computer security researcher for the University of Cambridge, in England, who has studied Chinese Internet filtering. “They are tweaking it all the time.”

The censorship poses an obstacle to Chinese businesses that are trying to expand internationally because they lack reliable access to sites with global audiences, such as Facebook. It can be hard to determine what the government will block on any given day.

“In China, a lot of things are like this,” said Jiang Tao, founder of CSDN, a Chinese software developer community. “You don’t know what you can do, what you can’t do. No one tells you.”

Google’s growing use of encryption could prompt China to block Google searches altogether or even all services offered by the company. Though Google has a much smaller market share in China than elsewhere in the world, it is still widely used by international firms and some others, meaning there could be economic consequences to an outright block.

Another option would be what experts call a “man-in-the-middle attack” that would allow Chinese censors to intercept encrypted traffic and decode it before it reaches Google servers. For many users, such an attack would be obvious because their browsers would warn that the communication had been accessed before reaching its intended recipient. Users would be free to proceed with the query, even in the face of a man-in-the-middle attack, but the protection offered by Google’s encryption would be lost.

Privacy advocates, who long have criticized Google, said its expanded use of encryption will do nothing to curb the company’s own tracking of the Web site visits, e-mails and search queries of its users. Such information helps the company target advertising, the key source of revenue for the company.

“It’s a good move to encrypt as much as possible, but I really think Google is grandstanding here,” said Jeff Chester, executive director of the Center for Digital Democracy, an advocacy group based in Washington.

Table of Contents

I was Putin's Pawn

By Elizabeth Wald, Politico Magazine, 21 May 2014

I knew I had to quit. I'd been a correspondent for RT—the English-language international cable network funded by the Russian government—for about two and a half years. I'd looked the other way as the network smeared America for the sake of making the Kremlin look better by comparison, while it sugarcoated atrocities by one brutal dictator after another. I'd been thinking about leaving for a long time, but was trying to hang in there until I figured out my next move.

Then Russia invaded Ukraine, and I came to see just how dangerous a propaganda tool the network was. I couldn't be a part of it any longer. I decided, somewhat arbitrarily, that March 5th would be my last day. And when that day came, after some particularly egregious coverage of the Ukraine crisis, I knew my resignation had to be public; I couldn't just silently disappear. That afternoon, I went to the bathroom to scribble down some thoughts before making my dramatic exit. During the 5 p.m. broadcast, after the coverage of Ukraine wrapped up, I made my closing statements:

"I cannot be part of a network funded by the Russian government that whitewashes the actions of Putin," I said. "I am proud to be an American and believe in disseminating the truth. And that is why, after this newscast, I am resigning."

My heart racing, I took my earpiece out and got up from the anchor chair. As I gathered my belongings, the news director said he wanted to have a word with me in his office. He asked me why I did it, as though I had some reason other than the one I had just announced on live TV. I explained that it really was because of the propaganda RT was pushing about Ukraine. Then I left the building and walked a couple blocks to a restaurant to sit down and let the reality of what I did settle in.

Fifteen minutes later, my phone started ringing.

***

I first arrived on the job at the Washington, D.C., bureau in September 2011. I came ready to take on the "stories the mainstream media ignores" and to do hard-hitting news that really matters. That's the job I signed on for, anyway.

When RT first contacted me, I was working as a reporter and anchor 8,000 miles away on the island of Saipan, in the U.S. Commonwealth of the Northern Mariana Islands, a 40-minute plane ride from Guam. I had been there for about two years, reporting for the local news station on topics like immigration and local political corruption. Before making the move across the globe, I had freelanced at a local news station in my home state of Connecticut, and had done several internships in broadcast news, including at NBC and Fox.

Island life was a blast, but around the time I decided I was ready to move back to the mainland, RT emailed me out of the blue. Apparently the news director had seen one of my reports—on how Saipan was preparing to handle possible radiation exposure after the Fukushima disaster—on YouTube and thought I'd be a good addition to RT.

The news director, who was Russian, pitched the network as an alternative news source that dared to challenge conventions. "Question More" was the network's slogan. During our Skype interview and on subsequent emails, there was little talk about Russia, or any indication the news would be influenced by Russian politics. I had some misgivings and asked about editorial independence. He scoffed, and asserted that the network was providing alternative news that mainstream outlets didn't want to hear. I wondered why the network was interested in me since I'm not Russian and have no ties to the country, but I checked out RT America's online videos and saw that almost all of the on-air correspondents were from the United States.

I was a little skeptical about the whole thing, but I couldn't find much concrete information on the Internet about the station and its mission and I didn't know anyone who'd ever worked there. I figured there are other networks that do respected journalism while getting some form of government funding. Also, the Cold War was over. Weren't we supposed to be mending ties? It's not like it was North Korea.

Here was an opportunity to move to D.C. and work on stories of national and international significance. I knew my other options would likely require moving to some Podunk town to cover rescued kittens and the Fourth of July parade.

Maybe I ignored some red flags. Maybe I should have asked tougher questions. But from my post in the Pacific, RT looked like a good opportunity.

I took the job.

***

The first few days were … interesting. The top guys were all Russian, but most of my co-workers were American. Some colleagues warned me that I'd need to let go of any preconceived notions and journalistic principles. I wasn't exactly sure what they meant.

It was during this first week that the Occupy Wall Street movement began with a group of protesters in New York's Zuccotti Park. The day after the demonstration started, the Russian news director announced at our morning meeting that this was the top story and we would take it on with full force. It was Occupy all day, every day, from coast to coast.

I spent a lot of time interviewing Occupy protestors in D.C.'s McPherson Square. Some had legitimate grievances: the rising role of money in politics, frustration over taxpayers footing the bill for bailing out big banks and crippling student-loan debt. But others were just hippies who were camping out, barefoot and beating drums, and had jumped at the opportunity to come together in solidarity against The Man.

Of course the coverage made the United States look terrible. Video of outraged protesters, heavy-handed police and tents pitched in parks portrayed America as a country in the midst of a popular uprising—it was the beginning of the inevitable decline of a capitalistic world power.

Occupy was our lead story for weeks and then months, even as the number of protesters dwindled and tents cleared out. We sucked that story completely dry.

Eventually, it was accepted that a revolution was not upon us.

Meanwhile, in Moscow thousands of demonstrators took to the streets protesting alleged election fraud and corruption, with most of their outrage directed at Russian leader Vladimir Putin, who announced his intention to run for president for a third term. There was little, if any, talk in our newsroom or on our newscasts of the dissent in Russia.

* * *

Soon our attention shifted to the 2012 presidential election. In RT's eyes, only one candidate mattered: Ron Paul. I don't remember Paul ever speaking to RT during campaign season, but that didn't stop our obsessive coverage of the "rock star" candidate. After a while the bosses' fixation with him seemed bizarre. Why were they pushing non-stop coverage of this long shot? Something tells me it wasn't his message of freedom and liberty but his non-interventionist stance and consistent criticism of U.S. foreign policy. His message fit RT's narrative—that the United States is a huge bully.

The network's coverage of foreign leaders was just as slanted, and more disturbing. After the death of Libyan leader Muammar Qadhafi, about a month into my time at RT, I was assigned to do a segment on how the dictator was once best buddies with the United States. I wasn't sure how to turn that into a full-scale reported package, but I was told to make it work by including photographs of the late dictator shaking hands and schmoozing with Western leaders. Add a couple mainstream media clips of talking heads celebrating his death and—boom—there's a story. The theme, the producer made clear, was U.S. hypocrisy … how dare Americans meddle in a conflict when Sen. John McCain once dined with the country's leader?

It was a theme the network returned to over and over. Mahmoud Ahmadinejad? The West was simply stoking fears of the Iranian president's plans to create a nuclear weapon as a pretense to go to war. Plus, the guy had some good points. Speaking at the U.N. General Assembly in 2010, Ahmadinejad said the biggest threat facing the world is U.S. domination.

Bashar Assad? Syria's bloody civil war was characterized by violence on both sides. The chemical attack near Damascus that killed hundreds of civilians was yet another excuse for the United States and its allies to swoop in, attack and support regime change. One particularly appalling article on the RT website, titled "Footage of chemical attack in Syria is a fraud," cited statements from a Catholic nun in Syria who asked "where parents of the supposedly dead children are."

I was disgusted and disappointed by the whitewashing of brutal dictators—and glad to be covering domestic issues. I tried to pitch stories I felt were important and underrepresented. From time to time, I would report on something I found worthwhile, and feel a little better about the cognitive dissonance I was suffering from. I went inside the country's largest jail in Cook County, Chicago, to expose how mental health patients flooded the correctional facility, highlighted the victims of the so-called War on Drugs who were unjustly incarcerated for decades for petty drug crimes and consistently covered the Bradley Manning trial in Fort Meade, Md. But I knew the stories would only fly if they fit the network's narrative that America is a crumbling nation plagued with problems.

Another troubling thing about RT was its popularity among fringe extremists. Abby Martin, who uses her platform on the network to advocate an anti-Western ideology, has a cult following among 9/11 "truthers" who believe the attack was an inside job orchestrated by a small group of political elites. The Russian bosses

love her lack of restraint in catering to a paranoid audience and blaming the mainstream media for conspiring to deliver the U.S. government agenda. Many of her fans say the Sandy Hook shooting was a hoax and that smoke left by aircraft are “chemtrails” containing chemical or biological agents the government is using for sinister reasons ranging from psychological warfare to population control. The more deranged the conspiracy theory, the more the Russian managers seemed to love it.

When Martin went off-script condemning Russia invading, I was proud of her. The Russian bosses, stumped on how to handle the situation, suggested sending her on a trip to Crimea. She didn’t go, knowing full well that it would be a “vetted PR experience,” as she called it. RT then used her brief moment of dissent to their advantage, asserting, “Contrary to the popular opinion, RT doesn’t beat its journalists into submission, and they are free to express their own opinions, not just in private but on the air. This is the case with Abby’s commentary on the Ukraine.”

But it was the very next day that the biased, Kremlin-driven coverage of Ukraine was pushed on the newscast, with propaganda and censorship like I’ve never seen it before. That added to my conviction that I had to resign, and do it publicly. RT was trying to use Martin to lend credibility to the network when I knew they were pushing lies. I wanted the viewers and the public to know what the station is really about.

There was one exception to the hostile-toward-the-West approach: pornography. Anything erotic was encouraged. Sexbots, the regulation of the porn industry—any excuse to get a porn star on the show made the head Russian honchos excited. I assumed the goal here was to stimulate the viewership, which largely consisted of young men who tuned into RT America, mostly online.

***

Throughout my time at the network, I heard colleagues repeat various justifications for continuing to work there ranging from “we’re providing a different perspective,” to “everyone has an agenda” to “it’s a job.” I resolved to only report facts, and I fell out of favor with the Russian managers for pushing back when they wanted me to push an angle I wasn’t comfortable with. (There’s a reason why many of the employees there are young and inexperienced.)

But when the turmoil in Ukraine deepened, the justifications no longer sufficed for me. The coverage of Ukraine was about promoting a Putinist agenda as Russia shamelessly invaded the country. When reports of armed military personnel at the airports surfaced, we were told to downplay them. When it became clear that troops on the ground in Crimea were Russian, RT dubbed them “self-defense forces.”

Producers booked clearly pro-Russian, anti-American guests, and I was instructed to egg them on. I was told to play up the extremist elements of the opposition, painting the new government as driven by neo-Nazi nationalists. But I also did my own research, and the more I learned about the uprising, the more my eyes opened to how the network was being used as a tool to push Putin’s agenda. It was a complex situation, sure, but there was at least one simple, irreducible fact: Russia had invaded Ukraine and lied about it.

I stopped to think about who I was and what I was doing. On my father’s side, both of my grandparents were immigrants from Hungary. My grandfather arrived in the U.S. around the end of World War II. My grandmother arrived 10 years later as a refugee from the 1956 Hungarian uprising, a nationwide revolt against Soviet forces that eventually forced Hungary into submission.

My grandmother, her brother and their mother managed to escape by bribing guards on the border with brandy and cash. The guards warned them that they would have to shoot around them to make it look like they were shooting to kill. They ran for the Austrian border as the guards fired a hail of bullets. It was a gamble: Sometimes the guards would take the bribes and shoot people anyway. When my grandmother made it across the border, she realized she had made it to safety but wasn’t sure if her brother and mother were alive. Eventually they found each other amid the smoke and dust and broke down crying. They were greeted by Red Cross personnel, taken to a refugee camp and granted passage to America.

I decided I could not work for a station that was spewing lies to justify Russian military intervention in a sovereign country. For months, I had wanted to quit, but decided I could not delay any longer. Nothing was worth being part of the Putin propaganda machine.

On the Wednesday I planned to be my last day, every story relating to Ukraine seemed designed to push Putin’s warped view toward the country. I had a pre-taped interview that day with none other than Ron Paul. The news director emailed me a list of questions like this one: “Isn’t it fascinating how US officials and the mainstream media are able to quickly arrive at a moral judgment condemning foreign interventionism on the part of Russia while, at the same time, blocking out of their minds all the foreign interventionism on the part of the US government for the past many decades?”

I didn't ask Paul all the questions I was given, and I substituted some of my own, including what the United States should do in light of Russia invading. How should Washington respond? Later, I saw the video editor cutting out "Russia invading" after, he said, higher-ups ordered him to do so. (Russia is not characterizing its actions as an invasion.) The uncensored version of the interview was posted online briefly before it was taken down and replaced with the edited one.

I decided that not only did I have to quit, I had to let viewers know why—to tell them the truth about RT and its misleading coverage. I went to the bathroom, wrote down some heartfelt notes and prepared for my exit a couple hours later. It was then that I contacted Jamie Kirchick, a writer with The Daily Beast, and told him my resignation was imminent. I first reached out to Kirchick a few months ago after he criticized Russia's anti-gay laws on the RT airwaves. I told him it was a bold move and I was willing to eventually come forward with the truth about RT. I informed him that the time had come and how I planned to do it. He published the exclusive story. Little did I know just how far word of my resignation would go.

***

The response has been unbelievable. I was flooded with interview requests from national and international news organizations. The clip went viral quickly, with millions of hits on YouTube.

I've received thousands of messages from people around the world voicing their support.

"I am from a group of Judaism called Hasidim where females are not particularly seen as brave and smart," one of the most touching messages said. "So after seeing the video of your resignation I asked my wife and 3 daughters to sit down with me and watch it together to show them how brave and smart a woman can be."

But I also received some hateful messages. RT's official response was that my actions were a "self-promotional stunt." Critics accused me of "selling out to the mainstream media."

After I went on CNN and mentioned the way my Ron Paul interview was edited, RT then reposted the original version. (There are now two versions online, one with and one without the edited question). The network later asked Paul for a comment about the interview—misleading him to believe that I quit because his message was censored—and posted Paul's response:

"Wahl's questions were all legitimate," Paul stated. "I would say that it essentially all got in there in a fair and balanced manner but she implied they edited something I said that might have benefited her position. I don't recall any of that. I thought the report and the essence of what they put on TV was exactly the message I was trying to get out."

That response and the way RT misrepresented the situation led to a deluge of hate tweets from Paul's supporters accusing me of lying about the interview, and saying that it was proof that my resignation was fraudulent.

I asked Paul's people to set the record straight. I explained what happened, even providing two versions of the video as proof that it was the editing of my question that I took issue with. His media representative responded to my concerns by saying: "We are actually on hiatus until the 24th. I don't want to rush to respond to your request or the details in your email but I will discuss this with my colleagues and will present this to Dr. Paul when it is appropriate."

I also got a long voicemail from someone named Kevin Gosztola, who represented himself as a journalist with First Look Media, Pierre Omidyar's new organization, though it turns out he's not employed there. "We're going to be putting forward some allegations about you and your time at RT," the message said. After about two minutes of accusations and rambling, he concluded: "If you have something to say for this story to defend yourself before we go ahead and publish, you have about 24 hours."I never called him back. (He left a similarly long harassing message to The Daily Beast, which checked with First Look, only to find that he was not an employee.)

Gosztola never published an attack on me. But nearly two weeks later, one of Abby Martin's close friends (whom she invited to the RT holiday party, where the two of them posed for a picture giving the middle finger to Israeli Prime Minister Benjamin Netanyahu) wrote a story on the website Truthdig that claimed to "uncover" that my resignation was part of a greater conspiracy, stating, "Behind the coverage of Wahl's dramatic protest, a cadre of neoconservatives was celebrating a public relations coup." It was surreal to read such an elaborate and far-fetched story about me.

Some of the vitriol came from within RT. One of my former colleagues tweeted the Truthdig link along with this message: "it's a pity when someone claiming to be committed to 'disseminating the truth' turns out to be a big ball of lies." And others were quoted in the article itself describing me as "an apolitical, deeply disgruntled employee seeking an exit strategy."

But from what I can tell it's a small handful of RT loyalists behind the hate. Several current and former employees have sent me messages commending me for finally blowing the whistle on this sketchy organization that poses as legitimate news.

More than anything, I feel like a weight has been lifted since I resigned. The outpouring of support has reaffirmed my belief in seeking and spreading the truth. As for my "self-promotional publicity stunt," if telling truth leads to better opportunities, some of my faith in humanity will be restored.

Table of Contents

Human Resources Command Stands Up Cyber Branch

By Lt. Col. Chevelle Thomas, HRC Public Affairs Office, March 24, 2014

FORT KNOX, Ky. (March 24, 2014) -- U.S. Army Human Resources Command established a provisional Cyber Branch Thursday, to provide career management, development and readiness to the Army's cyber forces.

The establishment of the branch will ensure the Army maintains visibility of Soldiers with unique cyber skills and talents, according to officials with Human Resources Command, or HRC. The new branch will perform career management services and provide Soldiers with cyber skills a "focal point" within HRC, said Maj. Gen. Richard P. Mustion, commanding general, HRC.

"While there are a significant number of decisions yet to be made on the future of the Army cyber force, we must establish an element dedicated to the assignment and career management of cyber Soldiers," said Col. Robert E. Duke, chief of Operations Support Division, Officer Personnel Management Directorate, HRC. "We will retain enough flexibility in our approach at HRC to adjust to changes as cyber proponency matures, and [as] this force evolves to meet mission requirements."

"As the Army develops cyber capability and establishes a Cyber Electromagnetic Branch, HRC remains aligned by providing capable and dedicated personnel support to this emerging workforce," said Duke. "We are establishing a Branch that consolidates enlisted, warrant officer and officer management and combines functional or designation focus with an organizational focus."

This is different from traditional branch management where one branch manages officers and an entirely different branch manages enlisted personnel. The Cyber Electromagnetic Branch, or CEM, branch will be a hybrid that consolidates and holistically manages the efforts of the entire Army cyber population under one entity, HRC officials said.

"This will enhance stabilization and the ability to gain depth into the specialized field," said Lt. Col. Candice E. Frost, Operations and Plans chief of Officer Readiness Division, OPMD, HRC. "As the Army's Cyber Center of Excellence stands up, the management of movement into and out of the cyber force rests upon Army Cyber's leadership and HRC's approval."

This closely aligned relationship will allow the Cyber or CEM Branch to better support a small, highly skilled, high-demand population in order to maintain personnel readiness in line with Army priorities, said Duke.

"The process is designed to ensure cyber force leadership has visibility of Soldiers with unique cyber skills and mechanisms in place to ensure a stable force capable of executing cyber missions," said Lt. Col. Kurt Connell, Military Intelligence Enlisted Branch chief, Enlisted Personnel Management Directorate, HRC. "What we don't want to do is create inadvertent turbulence in the cyber formation. So, as we set the conditions for incoming and outgoing Soldiers, control mechanisms are collectively agreed upon for each personnel action or assignment to meet both the needs of the Soldier and the Army."

A key part of managing the force is identifying the distinct groups that make up the population in constructing the branch, officials said. The initial organization is established around a set population of military occupational specialties, known as MOSs, additional skill identifiers, or ASIs, and current positions held by individuals in the cyber field.

The CEM branch centers on Functional Area 29, Area of Concentration 29A, MOS 29E and 290A. Additionally, it supports individuals in cyber operations, and those who function as cyber planners or defenders and receive an ASI or Skill Identifier of E4. Awarding this ASI is done by Army Cyber Command and is based on the individual Soldier, unit and mission, HRC officials said. It is not MOS dependent, they said.

"Development of an ASI/SI to identify those who provide support to cyber is underway," Frost said.

Factors such as population management, current and future requirements, training necessities, and growth and maturity within the field may also influence cyber assignments, HRC officials said.

"The personnel requirements are greater than the number of people available to fill them," Duke said. "Developing a mature force able to meet all Army requirements will take time; many assignments can require

technical training and a lot of lead time. Training an individual throughout the entire process from recruiting, accessing, entry-level training and other professional military educational objectives to the point of where they can function within the career field of operations is sometimes extensive."

Table of Contents

As U.S. War Ends, Russia Returns To Afghanistan with Series of Investment Projects

By Kevin Sieff, Washington Post, March 21, 2014

KABUL — To the white-bearded Afghan machinists, it felt like the Cold War era had suddenly returned.

After 25 years of working in a sprawling Soviet-built factory — a vestige of a war and occupation long extinguished — they suddenly spotted a new shipment of gleaming Russian equipment arriving last fall on an 18-wheeler.

The factory was abuzz. The Russians were back.

As the U.S.-led war winds down and Russia reasserts itself in Ukraine and the Middle East, Moscow is also ramping up its investment in Afghanistan. It is rebuilding the relics of the Soviet occupation and promoting its own political and cultural prowess.

“You see Russia’s interest in Afghanistan rising. It’s visible,” said Stepan Anikeev, the spokesman for the Russian Embassy in Kabul. “We want to enlarge our role in the region. It’s not only for Afghanistan, but for our own goals.”

Russia’s recent incursion into its neighbor, Ukraine, and its annexation of Crimea reflect its intent to maintain influence in some former Soviet republics. It also reaching out to old allies further afield. Last month, President Vladimir Putin received Egyptian army chief Abdel Fatah al-Sissi, whose relations with Washington have been strained since a coup last summer, and expressed support for the military man’s expected presidential bid.

Moscow is also negotiating a major arms deal with Sissi and agreed in 2012 to sell Iraq $4.3 billion in weapons. In Syria, Putin is strongly backing the government of President Bashar al-Assad as he seeks to crush a rebellion that has received support from the West.

In Afghanistan, Russian officials point to their development activities as a counterexample to U.S. aid projects, which many Afghans criticize as wasteful and misguided.

“The mistake of the last 12 years is that people were eager to give money, but without the proper strategy,” said Russian Ambassador Andrey Avetisyan, who was also based in Kabul as a young diplomat in the 1980s.

Many Afghans, including President Hamid Karzai, praise the Soviet model even though they fought a bloody 10-year war against the country’s army, which invaded in 1979 to support an unpopular communist government.

“The Soviet money went to the right place. They were efficient in spending their money and doing it through the Afghan government,” Karzai said in an interview with The Washington Post this month.

The new warmth between the Kremlin and Afghanistan was visible this week when the Afghan government released a message from Putin marking the Persian new year. It was the only such message made public, and was released at a time when the United States and European governments are imposing sanctions on Russia for its expansion into Ukraine.

“I am certain that friendly ties and cooperation between Russia and Afghanistan in the future will add to the goodness and welfare of our people,” Putin said in the message to Karzai, which was translated into Dari, the local language.

The Russian government has compiled a list of 140 Soviet-era projects that it would like to rehabilitate, according to the embassy. The Kabul Housebuilding Factory, the country’s largest manufacturing facility, was the first to receive assistance last fall: $25 million in new equipment.

A few miles away in Kabul, the Russian government is spending $20 million to renovate the Soviet House of Science and Culture, constructed in 1982. The building, whose jutting angles exemplify Soviet industrial design, was torn apart by bullets and rockets and became crowded with Afghan drug addicts. It is to reopen this fall as the Russian Cultural Center, a beacon for those with interest in Russia.

“We want to expand our culture here,” Anikeev said of the center.

Aid that's appreciated

Afghanistan is still peppered with reminders of both the Soviet Union's war and its infrastructure projects. Soviet land mines continue to kill and injure dozens of Afghan civilians every year. But its bread-making factory still produces thousands of loaves every day. Its housing complexes are among the country's most desirable (and the only ones with central heating).

"I hated the Soviets. I fought against them. They killed my father. But this is still the best place to live," Gen. Labib Raeed said in his apartment in the Microryan, a Soviet-built complex which translates to "housing block" in Russian.

Raeed is an officer in the U.S.-backed Afghan army, but he's quick to criticize the U.S. development effort — more than $100 billion spent on non-military aid, including roads and schools.

"The Americans were generous to donate so much money, but they gave it to the wrong people," he said.

The Microryan looks like it has been transplanted from a small Russian city. It is gray and unadorned, a stark contrast to the flashiness of Kabul's new homes and wedding halls. The four-bedroom apartments are cramped and austere, but they sell for more than $100,000.

Projects such as the Microryan were constructed during the height of the Cold War. The Soviet Union continued building even as it waged war in the country throughout the 1980s. And then, on Feb. 15, 1989, it was all over. The Soviets withdrew and their projects — the factories, schools, swimming pools atop Kabul hills — were left largely unattended.

Many of those projects managed to survive a civil war and the Taliban regime relatively intact. The house-building factory made the prefabricated walls from which Taliban officials, including top leader Mohammad Omar, built their homes and offices. Last year, it produced the walls for one of Afghanistan's biggest prisons.

The machinists who were in their 20s when they were trained by Soviet engineers are now middle-aged, but they're still working on the same equipment, with instructions in fading Cyrillic characters. The new Russian technology is expected to be installed in the coming months.

Many Afghans question why Russia seems so interested in development here now, just as the West's assistance tapers off. The aid program seems to many a calculated move reminiscent of the Great Game, the contest between the Russian and British empires for influence in central Asia in the 19th century.

Russian officials say that supporting Afghanistan makes sense, given their regional interests. Afghanistan shares borders with three former Soviet states that still receive considerable funding — and direction — from Moscow. And Afghanistan continues to be a major source of narcotics that pour into Russia. Economic development, along with a Russian-funded counternarcotics program, could curb that illicit trade, officials hope.

Still, the timing of Russia's development effort has raised eyebrows. That country's most significant economic partnership with Afghanistan in recent years, a joint commission on "trade and economic cooperation," wasn't launched until 2012, the year the U.S. withdrawal began.

There are other signs of a Russian revival here.

The number of students studying Russian at Kabul University has doubled in the past two years. Russia, in turn, has doubled the number of scholarships it offers to Afghan students. The cultural center, when it reopens this fall, will hold a vast library of Russian literature and offer language courses.

Russia has refused to send soldiers to support the NATO mission and has provided limited military aid. Although there is talk of equipping Afghan forces with more Russian-made Kalashnikov assault rifles, that plan has not been finalized and civilian projects remain the focus of the development effort.

"What the Soviets did here was really fundamental. They were thinking about the long term," said Ahmad, the head engineer of the house-building factory, who like many Afghans uses only one name.

For 30 years, Ahmad has walked past the same inscription every day on his way to the office.

"This factory," the inscription reads, "was built by the friendly government of the Soviet Union and was presented to the Afghan nation as a gift." The year "1962" is carved into the stone.

In the 1980s, as Afghanistan's war with the Soviet Union raged, the word "friendly" stood out as bitterly ironic. Now, with Russia's promise to return the factory to its days of productivity, the adjective is starting to resonate.

"We don't differentiate between the Americans and the Russians. Whoever wants to help us," said Ahmad. "We welcome the Russians back."

Table of Contents

Cyber Supports Red Flag for First Time

By 2nd Lt. Meredith Hein, 24th Air Force Public Affairs, March 14, 2014

JOINT BASE SAN ANTONIO-LACKLAND, Texas (AFNS) -- For the first time in Red Flag's nearly 40-year history, the 24th Air Force played a significant role in the Cyber Mission Force, or CMF, at the Air Combat Command-sponsored exercise held at Nellis Air Force Base, Nev. Jan. 27 through Feb. 14.

Red Flag, an Air Combat Command-sponsored exercise held four times annually, combines a series of complex scenarios and a robust simulated Integrated Air Defense Systems, which challenge exercise participants to collaboratively plan and execute missions in support of operational and tactical objectives, said Michael Connolly, the director of operations with the 90th Information Operations Squadron here.

The goal for 24th Air Force, the Air Force's component to U.S. Cyber Command, was to demonstrate Air Forces Cyber's progress in implementing U.S. Cyber Command's CMF construct through the employment of combat mission teams, or CMTs and cyber protection teams, or CPTs.

CMTs provided full-spectrum cyber capability for combatant commanders. This was the first time that CMTs were used in this configuration for Red Flag. On the other hand, CPTs protect a specific target and provide mission assurance. In the case of Red Flag, the CPTs protected the combined air operations center at Nellis AFB.

"This is an asymmetric capability that we're scratching at the surface to employ," said Brig. Gen. Robert J. Skinner, the AFCYBER deputy commander. "We are more engaged with Red Flag, allowing more opportunities to provide mission effects at the point of our choosing and at the drop of a hat for joint force commanders to use."

In addition to the CMTs and CPTs various squadrons from the 24th Air Force acted as the cyber defense service provider, which located general threats against the network and practiced enterprise protection.

One of the other key cyber components for Red Flag was the 318th Cyberspace Operations Group, Detachment 2, whose daily mission is to establish cyber operations as credible, replicable combat capability across air, space and cyberspace domains.

The detachment worked with the U.S. Air Force Warfare Center to integrate cyber into the Red Flag scenarios, which allowed cyber operators to fully participate in the exercise. In order for this to happen, effective ranges were built to represent the operating environment for U.S. and coalition forces and intelligence was created to fulfill the needs of the exercise.

The detachment worked closely with providers such as the 346th Test Squadron to build a replica of the Air Force Network for the "blue team" to defend during the exercise, as well as create targets for the "red forces" to attack.

In addition, the Det. 2 worked with intelligence units, such as the 547th Intelligence Squadron at Nellis AFB to create a realistic back story for the cyber operators to work under.

Red Flag is truly an integration exercise, said Maj. Robert Biggers, the 318th COG, Det. 2 commander.

"Operators participated from planning to execution, and all forces, air, space and cyberspace, worked as a collective body to understand how each of their actions affects one another and the mission," he said.

The warfare center fundamentally changed how Red Flag is being carried out this year in an effort to fully integrate non-kinetic operations and intelligence, surveillance and reconnaissance capabilities.

Changes to the Red Flag construct, which now links scenarios across several days, allowed intelligence to be gathered in a more realistic world setting. This Red Flag was also the first time 24th AF has been fully integrated with the Air Force Intelligence, Surveillance and Reconnaissance Agency.

"Developments happening with cyber and ISR are all in preparation for operations in a contested environment," said Capt. Andrew Caulk, a spokesman for AFISRA. "We train like we fight."

According to Biggers, the red forces and blue forces engaged in a campaign plan against one another responding and adjusting to each other as they would in a real-world conflict.

"Lessons were learned and operators applied what they learned from day to day to refine how we can most effectively operate together," Biggers said. "This is exactly the type of advanced training cyberspace operators need today."

The Air Force was not the only service that provided cyber support to Red Flag. Army Cyber Command and coalition forces participated as well.

"Not only did each country bring their own weapon systems to be integrated into the fight, but they brought unique perspectives and expertise," Biggers said. "The reality is that we fight alongside our coalition brothers

and sisters every day. I am glad we are training together at this level, in the Air Force's largest and most advanced exercise."

The integration of these different units, branches and partner nations has far-reaching effects.

"We use Red Flag for advanced training to hone our skills, and we continue to learn great lessons to employ in the next one," Skinner said. "You can see us taking advantage of operations to become better, faster and leaner. The expertise, professionalism and teamwork displayed throughout the activities, teams that don't normally work together, watching them be an integrated team shows how far we have come to provide effects for our mission and operations."

Table of Contents

This is Information Warfare

By Joel Harding, To Inform is to Influence (blog), March 26, 2014

This is the first information war since the US developed the concept of information warfare back in the early 1990s. Since then the term was watered down to become politically correct, into information operations. Someone asked me today what the difference was between this and the Cold War where the Soviets and the US lobbed propaganda back and forth in the hopes of somehow causing a popular uprising, affecting some random decision or hopefully a leader.

First, notice I used the term propaganda. Both the Soviet Union and the US produced massive amounts of propaganda to support their point of view. I grew up in the 60s and 70s and when I worked in China and Russia only a few years ago, I realized my concept of both countries had been severely skewed by this information.

Fast forward to today and I deal with VOA, RFE/RL, RFA and other international news outlets. I can honestly say, in my expert opinion, that the news they broadcast is as close to the truth as I have ever seen and is definitely not propaganda. One of the first targets of pro-Russian commenters was to label VOA and others as propaganda purveyors and as CIA fronts. This is interesting because that is definitely not the case.

In the early 1990s the Cold War ended and a concept named Command and Control Warfare popped up, quickly replaced by Information Warfare and finally the worst plain vanilla expression in the world: Information Operations. Quickly, Information Operations became overwhelmed with warfare in cyberspace. State sponsored hackers popped up and the news focused on hackers. Hackers became the new cool kids. Then, finally, the term "Information Warfare" was dropped from the lexicon of official terms. Life, somehow, has a way of reminding us that just dropping a term does not stop it from being correct. Senior staffers in the Information Operations office in the Pentagon use Information Warfare as if it is right, and who am I to argue? Dr. Dan Kuehl, formerly the titular leader of Information Operations at National Defense University for years argued that Information Warfare was and is the proper term. He's right and always has been.

Which brings us to today and the difference between what we are seeing today and saw yesterday. There are two huge pieces missing from this little conflict: the use of massive cyber attacks and conventional warfare but we see massive and the highly effective use of information against leaders as well as the population.

Yes, this is just like the Cold War. For the past 25 years, however, volleys of electrons, cyber spitballs, were flung back and forth between potential enemies. Probing, pinging, attempts to overwhelm (DDOS), silly website defacements – all efforts deemed short of war. Cries of "Digital Pearl Harbor" rang out and the US has spent billions of dollars and devoted thousands of their best and brightest to this new field of cyberwarfare. People have made fortunes and careers have been established based solely on one concept. Cyberwarfare was forever inextricably linked to warfare. Cyber became the end game, information and influence were overlooked. Here, the Russians pulled up to a communications bunker and simply unhooked Crimea from the rest of the world and 'game over'. Cyber is not a player. Sure, there are website defacements and DDOS attacks but twitter and social media have overcome those minor inconveniences. Yes, it's still cyber, but in this case, is only being used for communications and the information and influence is the dominant effect.

Not since the 1980s have we seen information, misinformation, disinformation and outright lies flung back and forth between Russia and the rest of the world. Propaganda is being churned up like chum in a global fishing tournament. We are seeing symbology unlike any other time, pointed directly at world leaders. Putin bare-chested and doing traditionally manly things. Obama wearing mom jeans and riding a silly bicycle contrasted against the Russian bear. Russian stories of them needing to protect ethnic Russians. Stories of Russian tradition. Masked soldiers controlling Crimea. From the West we hear of international laws being broken, of banks being closed down, of a rapidly spiraling Russian economy. We see videos done by a young female

leader of an uprising – instantly viewed around the world by millions. Within hours we see a Russian response. We see massive amounts of reportedly paid commentors on social media.

No more paper posters. No more pamphlets. No more Life magazine. No more waiting for Walter Cronkite to tell us what to think. No more old white men in smokey rooms planning out what we see.

This is the first information war where the repercussions are immediately felt, almost globally. The instantaneous effects have necessitated new tactics, planning and strategies by our world leaders. This is an entirely new information war where everybody has the potential of being on the front line and being a victim as well as a soldier.

Table of Contents

The United States Secretly Built 'Cuban Twitter' to Stir Unrest

By Desmond Butler, Jack Gillum and Alberto Arce, Associated Press, 3 April 2014

WASHINGTON — In July 2010, Joe McSpedon, a U.S. government official, flew to Barcelona to put the final touches on a secret plan to build a social media project aimed at undermining Cuba's Communist government.

McSpedon and his team of high-tech contractors had come in from Costa Rica and Nicaragua, Washington and Denver. Their mission: to launch a messaging network that could reach hundreds of thousands of Cubans. To hide the network from the Cuban government, they would set up a byzantine system of front companies using a Cayman Islands bank account, and recruit unsuspecting executives who would not be told of the company's ties to the U.S. government.

McSpedon didn't work for the CIA. This was a program paid for and run by the U.S. Agency for International Development, best known for overseeing billions of dollars in U.S. humanitarian aid.

According to documents obtained by The Associated Press and multiple interviews with people involved in the project, the plan was to develop a bare-bones "Cuban Twitter," using cellphone text messaging to evade Cuba's strict control of information and its stranglehold restrictions over the Internet. In a play on Twitter, it was called ZunZuneo — slang for a Cuban hummingbird's tweet.

Documents show the U.S. government planned to build a subscriber base through "non-controversial content": news messages on soccer, music, and hurricane updates. Later, when the network reached a critical mass of subscribers, perhaps hundreds of thousands, operators would introduce political content aimed at inspiring Cubans to organize "smart mobs" — mass gatherings called at a moment's notice that might trigger a Cuban Spring, or, as one USAID document put it, "renegotiate the balance of power between the state and society."

At its peak, the project drew in more than 40,000 Cubans to share news and exchange opinions. But its subscribers were never aware that it was created by the U.S. government, or that American contractors were gathering their private data in the hope that it might be used for political purposes.

"There will be absolutely no mention of United States government involvement," according to a 2010 memo from Mobile Accord, one of the project's contractors. "This is absolutely crucial for the long-term success of the service and to ensure the success of the Mission."

The program's legality is unclear: U.S. law requires that any covert action by a federal agency must have presidential authorization. Officials at USAID would not say who had approved the program or whether the White House was aware of it. McSpedon, the most senior official named in the documents obtained by the AP, is a midlevel manager who declined to comment.

USAID spokesman Matt Herrick said the agency is proud of its Cuba programs and noted that congressional investigators reviewed them last year and found them to be consistent with U.S. law.

"USAID is a development agency, not an intelligence agency, and we work all over the world to help people exercise their fundamental rights and freedoms, and give them access to tools to improve their lives and connect with the outside world," he said.

"In the implementation," he added, "has the government taken steps to be discreet in non-permissive environments? Of course. That's how you protect the practitioners and the public. In hostile environments, we often take steps to protect the partners we're working with on the ground. This is not unique to Cuba."

But the ZunZuneo program muddies those claims, a sensitive issue for its mission to promote democracy and deliver aid to the world's poor and vulnerable — which requires the trust of foreign governments.

"On the face of it there are several aspects about this that are troubling," said Sen. Patrick Leahy, D-Vt. and chairman of the Appropriations Committee's State Department and Foreign Operations subcommittee.

“There is the risk to young, unsuspecting Cuban cellphone users who had no idea this was a U.S. government-funded activity. There is the clandestine nature of the program that was not disclosed to the Appropriations subcommittee with oversight responsibility. And there is the disturbing fact that it apparently activated shortly after Alan Gross, a USAID subcontractor who was sent to Cuba to help provide citizens access to the Internet, was arrested.”

The Associated Press obtained more than 1,000 pages of documents about the project’s development. The AP independently verified the project’s scope and details in the documents — such as federal contract numbers and names of job candidates — through publicly available databases, government sources, and interviews with those directly involved in ZunZuneo.

Taken together, they tell the story of how agents of the U.S. government, working in deep secrecy, became tech entrepreneurs — in Cuba. And it all began with a half a million cellphone numbers obtained from a Communist government.

—

ZunZuneo would seem to be a throwback from the Cold War, and the decades-long struggle between the United States and Cuba. It came at a time when the historically sour relationship between the two countries had improved, at least marginally, and Cuba had made tentative steps toward a more market-based economy.

It is unclear whether the plan got its start with USAID or Creative Associates International, a Washington, D.C., for-profit company that has earned hundreds of millions of dollars in U.S. contracts. But a “key contact” at Cubacel, the state-owned cellphone provider, slipped the phone numbers to a Cuban engineer living in Spain. The engineer provided the numbers to USAID and Creative Associates “free of charge,” documents show.

In mid-2009, Noy Villalobos, a manager with Creative Associates who had worked with USAID in the 1990s on a program to eradicate drug crops, started an IM chat with her little brother in Nicaragua, according to a Creative Associates email that captured the conversation. Mario Bernheim, in his mid-20s, was an up-and-coming techie who had made a name for himself as a computer whiz.

“This is very confidential of course,” Villalobos cautioned her brother. But what could you do if you had all the cellphone numbers of a particular country? Could you send bulk text messages without the government knowing?

“Can you encrypt it or something?” she texted.

She was looking for a direct line to regular Cubans through text messaging. Most had precious little access to news from the outside world. The government viewed the Internet as an Achilles’ heel and controlled it accordingly. A communications minister had even referred to it as a “wild colt” that “should be tamed.”

Yet in the years since Fidel Castro handed over power to his brother Raúl, Cuba had sought to jump-start the long-stagnant economy. Raúl Castro began encouraging cellphone use, and hundreds of thousands of people were suddenly using mobile phones for the first time, though smartphones with access to the Internet remained restricted.

Cubans could also text message, though at a high cost in a country where the average wage was a mere $20 a month.

Bernheim told his sister that he could figure out a way to send instant texts to hundreds of thousands of Cubans — for cheap. It could not be encrypted though, because that would be too complicated. They wouldn’t be able to hide the messages from the Cuban government, which owned Cubacel. But they could disguise who was sending the texts by constantly switching the countries the messages came from.

“We could rotate it from different countries?” Villalobos asked. “Say one message from Nica, another from Spain, another from Mexico?”

Bernheim could do that. “But I would need mirrors set up around the world, mirrors, meaning the same computer, running with the same platform, with the same phone.”

“No hay problema,” he signed off. No problem.

—

After the chat, Creative hired Bernheim as a subcontractor, reporting to his sister. (Villalobos and Bernheim would later confirm their involvement with the ZunZuneo project to AP but decline further comment.) Bernheim, in turn, signed up the Cuban engineer who had gotten the phone list. The team figured out how to message the masses without detection, but their ambitions were bigger.

Creative Associates envisioned using the list to create a social networking system that would be called “Proyecto ZZ,” or “Project ZZ.” The service would start cautiously and be marketed chiefly to young Cubans, whom USAID saw as the most open to political change.

“We should gradually increase the risk,” USAID proposed in a document. It advocated using “smart mobs” only in “critical/opportunistic situations and not at the detriment of our core platform-based network.”

USAID’s team of contractors and subcontractors built a companion website to its text service so Cubans could subscribe, give feedback, and send their own text messages for free. They talked about how to make the website look like a real business. “Mock ad banners will give it the appearance of a commercial enterprise,” a proposal suggested.

In multiple documents, USAID staff pointed out that text messaging had mobilized smart mobs and political uprisings in Moldova and the Philippines, among others. In Iran, the USAID noted social media’s role following the disputed election of then-President Mahmoud Ahmadinejad in June 2009 — and saw it as an important foreign policy tool.

USAID documents say their strategic objective in Cuba was to “push it out of a stalemate through tactical and temporary initiatives, and get the transition process going again towards democratic change.” Democratic change in authoritarian Cuba meant breaking the Castros’ grip on power.

USAID divided Cuban society into five segments depending on loyalty to the government. On one side sat the “democratic movement,” called “still (largely) irrelevant,” and at the other end were the “hard-core system supporters,” dubbed “Talibanes” in a derogatory comparison to Afghan and Pakistani extremists.

A key question was how to move more people toward the democratic activist camp without detection. Bernheim assured the team that wouldn’t be a problem.

“The Cuban government, like other regimes committed to information control, currently lacks the capacity to effectively monitor and control such a service,” Bernheim wrote in a proposal for USAID marked “Sensitive Information.”

ZunZuneo would use the list of phone numbers to break Cuba’s Internet embargo and not only deliver information to Cubans but also let them interact with one another in a way the government could not control. Eventually it would build a system that would let Cubans send messages anonymously among themselves.

At a strategy meeting, the company discussed building “user volume as a cover … for organization,” according to meeting notes. It also suggested that the “Landscape needs to be large enough to hide full opposition members who may sign up for service.”

In a play on the telecommunication minister’s quote, the team dubbed their network the “untamed colt.”

—

At first, the ZunZuneo team operated out of Central America. Bernheim, the techie brother, worked from Nicaragua’s capital, Managua, while McSpedon supervised Creative’s work on ZunZuneo from an office in San José, Costa Rica, though separate from the U.S. embassy. It was an unusual arrangement that raised eyebrows in Washington, according to U.S. officials.

McSpedon worked for USAID’s Office of Transition Initiatives (OTI), a division that was created after the fall of the Soviet Union to promote U.S. interests in quickly changing political environments — without the usual red tape.

In 2009, a report by congressional researchers warned that OTI’s work “often lends itself to political entanglements that may have diplomatic implications.” Staffers on oversight committees complained that USAID was running secret programs and would not provide details.

“We were told we couldn’t even be told in broad terms what was happening because ‘people will die,’ ” said Fulton Armstrong, who worked for the Senate Foreign Relations committee. Before that, he was the U.S. intelligence community’s most senior analyst on Latin America, advising the Clinton White House.

The money that Creative Associates spent on ZunZuneo was publicly earmarked for an unspecified project in Pakistan, government data show. But there is no indication of where the funds were actually spent.

Tensions with Congress spiked just as the ZunZuneo project was gearing up in December 2009, when another USAID program ended in the arrest of the U.S. contractor Alan Gross. Gross had traveled repeatedly to Cuba on a secret mission to expand Internet access using sensitive technology typically available only to governments, a mission first revealed in February 2012 by AP.

At some point, Armstrong says, the foreign relations committee became aware of OTI’s secret operations in Costa Rica. U.S. government officials acknowledged them privately to Armstrong, but USAID refused to provide operational details.

At an event in Washington, Armstrong says he confronted McSpedon, asking him if he was aware that by operating secret programs from a third country, it might appear like he worked for an intelligence agency.

McSpedon, through USAID, said the story is not true. He declined to comment otherwise.

—

On Sept. 20, 2009, thousands of Cubans gathered at Revolution Plaza in Havana for Colombian rocker Juanes' "Peace without Borders" concert. It was the largest public gathering in Cuba since the visit of Pope John Paul II in 1998. Under the watchful gaze of a giant sculpture of revolutionary icon Ernesto "Che" Guevara, the Miami-based Juanes promised music aimed at "turning hate into love."

But for the ZunZuneo team, the concert was a perfect opportunity to test the political power of their budding social network. In the weeks before, Bernheim's firm, using the phone list, sent out half a million text messages in what it called "blasts" to test what the Cuban government would do.

The team hired Alen Lauzán Falcón, a Havana-born satirical artist based in Chile, to write Cuban-style messages. Some were mildly political and comical, others more pointed. One asked respondents whether they thought two popular local music acts out of favor with the government should join the stage with Juanes. Some 100,000 people responded — not realizing that the poll was used to gather critical intelligence.

Paula Cambronero, a researcher for Mobile Accord, began building a vast database about the Cuban subscribers, including gender, age, "receptiveness," and "political tendencies." USAID believed the demographics on dissent could help it target its other Cuba programs and "maximize our possibilities to extend our reach."

Cambronero concluded that the team had to be careful. "Messages with a humorous connotation should not contain a strong political tendency, so as not to create animosity in the recipients," she wrote in a report.

Falcón, in an interview, said he was never told that he was composing messages for a U.S. government program, but he had no regrets about his involvement.

"They didn't tell me anything, and if they had, I would have done it anyway," he said. "In Cuba they don't have freedom. While a government forces me to pay in order to visit my country, makes me ask permission, and limits my communications, I will be against it, whether it's Fidel Castro, (Cuban exile leader) Jorge Mas Canosa, or Gloria Estefan," the Cuban American singer.

Carlos Sánchez Almeida, a lawyer specializing in European data protection law, said it appeared that the U.S. program violated Spanish privacy laws because the ZunZuneo team had illegally gathered personal data from the phone list and sent unsolicited emails using a Spanish platform. "The illegal release of information is a crime, and using information to create a list of people by political affiliation is totally prohibited by Spanish law," Almeida said. It would violate a U.S.-European data protection agreement, he said.

USAID saw evidence from server records that Havana had tried to trace the texts, to break into ZunZuneo's servers, and had occasionally blocked messages. But USAID called the response "timid" and concluded that ZunZuneo would be viable — if its origins stayed secret.

Even though Cuba has one of the most sophisticated counter-intelligence operations in the world, the ZunZuneo team thought that as long as the message service looked benign, Cubacel would leave it alone.

Once the network had critical mass, Creative and USAID documents argued, it would be harder for the Cuban government to shut it down, both because of popular demand and because Cubacel would be addicted to the revenues from the text messages.

In February 2010, the company introduced Cubans to ZunZuneo and began marketing. Within six months, it had almost 25,000 subscribers, growing faster and drawing more attention than the USAID team could control.

—

Saimi Reyes Carmona was a journalism student at the University of Havana when she stumbled onto ZunZuneo. She was intrigued by the service's novelty, and the price. The advertisement said "free messages," so she signed up using her nickname, Saimita.

At first, ZunZuneo was a very tiny platform, Reyes said during a recent interview in Havana, but one day she went to its website and saw that its services had expanded.

"I began sending one message every day," she said, the maximum allowed at the start. "I didn't have practically any followers." She was thrilled every time she got a new one.

And then ZunZuneo exploded in popularity.

“The whole world wanted in, and in a question of months I had 2,000 followers who I have no idea who they are, nor where they came from.”

She let her followers know the day of her birthday, and was surprised when she got some 15 personal messages. “This is the coolest thing I’ve ever seen!” she told her boyfriend, Ernesto Guerra Valdes, also a journalism student.

Before long, Reyes learned she had the second-highest number of followers on the island, after a user called UCI, which the students figured was Havana’s University of Computer Sciences. Her boyfriend had 1,000. The two were amazed at the reach it gave them.

“It was such a marvelous thing,” Guerra said. “So noble.” He and Reyes tried to figure out who was behind ZunZuneo, since the technology to run it had to be expensive, but they found nothing. They were grateful, though.

“We always found it strange, that generosity and kindness,” he said. ZunZuneo was “the fairy godmother of cellphones.”

—

By early 2010, Creative decided that ZunZuneo was so popular Bernheim’s company wasn’t sophisticated enough to build, in effect, “a scaled down version of Twitter.”

It turned to another young techie, James Eberhard, CEO of Denver-based Mobile Accord. Eberhard had pioneered the use of text messaging for donations during disasters and had raised tens of millions of dollars after the January 2010 earthquake in Haiti.

Eberhard earned millions in his mid-20s when he sold a company that developed cellphone ringtones and games. His company’s website describes him as “a visionary within the global mobile community.”

In July, he flew to Barcelona to join McSpedon, Bernheim, and others to work out what they called a “below the radar strategy.”

“If it is discovered that the platform is, or ever was, backed by the United States government, not only do we risk the channel being shut down by Cubacel, but we risk the credibility of the platform as a source of reliable information, education, and empowerment in the eyes of the Cuban people,” Mobile Accord noted in a memo.

To cover their tracks, they decided to have a company based in the United Kingdom set up a corporation in Spain to run ZunZuneo. A separate company called MovilChat was created in the Cayman Islands, a well-known offshore tax haven, with an account at the island’s Bank of N.T. Butterfield & Son Ltd. to pay the bills.

A memo of the meeting in Barcelona says that the front companies would distance ZunZuneo from any U.S. ownership so that the “money trail will not trace back to America.”

But it wasn’t just the money they were worried about. They had to hide the origins of the texts, according to documents and interviews with team members.

Brad Blanken, the former chief operating officer of Mobile Accord, left the project early on, but noted that there were two main criteria for success.

“The biggest challenge with creating something like this is getting the phone numbers,” Blanken said. “And then the ability to spoof the network.”

The team of contractors set up servers in Spain and Ireland to process texts, contracting an independent Spanish company called Lleida.net to send the text messages back to Cuba, while stripping off identifying data.

Mobile Accord also sought intelligence from engineers at the Spanish telecommunications company Telefónica, which organizers said would “have knowledge of Cubacel’s network.”

“Understanding the security and monitoring protocols of Cubacel will be an invaluable asset to avoid unnecessary detection by the carrier,” one Mobile Accord memo read.

Officials at USAID realized, however, that they could not conceal their involvement forever — unless they left the stage. The predicament was summarized bluntly when Eberhard was in Washington for a strategy session in early February 2011, where his company noted the “inherent contradiction” of giving Cubans a platform for communications uninfluenced by their government that was in fact financed by the U.S. government and influenced by its agenda.

They turned to Jack Dorsey, a co-founder of Twitter, to seek funding for the project. Documents show that Dorsey met with Suzanne Hall, a State Department officer who worked on social media projects, and others. Dorsey declined to comment.

The State Department under then-Secretary Hillary Rodham Clinton thought social media was an important tool in diplomacy. At a 2011 speech at George Washington University, Clinton said the U.S. helped people in "oppressive Internet environments get around filters." In Tunisia, she said people used technology to "organize and share grievances, which, as we know, helped fuel a movement that led to revolutionary change."

Ultimately, the solution was new management that could separate ZunZuneo from its U.S. origins and raise enough revenue for it to go "independent," even as it kept its long-term strategy to bring about "democratic change."

Eberhard led the recruitment efforts, a sensitive operation because he intended to keep the management of the Spanish company in the dark.

"The ZZ management team will have no knowledge of the true origin of the operation; as far as they know, the platform was established by Mobile Accord," the memo said. "There should be zero doubt in management's mind and no insecurities or concerns about United States Government involvement."

The memo went on to say that the CEO's clean conscience would be "particularly critical when dealing with Cubacel." Sensitive to the high cost of text messages for average Cubans, ZunZuneo negotiated a bulk rate for texts at 4 cents a pop through a Spanish intermediary. Documents show there was hope that an earnest, clueless CEO might be able to persuade Cubacel to back the project.

Mobile Accord considered a dozen candidates from five countries to head the Spanish front company. One of them was Francoise de Valera, a CEO who was vacationing in Dubai when she was approached for an interview. She flew to Barcelona. At the luxury Mandarin Oriental Hotel, she met with Nim Patel, who at the time was Mobile Accord's president. Eberhard had also flown in for the interviews. But she said she couldn't get a straight answer about what they were looking for.

"They talked to me about instant messaging but nothing about Cuba, or the United States," she told the AP in an interview from London.

"If I had been offered and accepted the role, I believe that sooner or later it would have become apparent to me that something wasn't right," she said.

—

By early 2011, Creative Associates grew exasperated with Mobile Accord's failure to make ZunZuneo self-sustaining and independent of the U.S. government. The operation had run into an unsolvable problem. USAID was paying tens of thousands of dollars in text messaging fees to Cuba's communist telecommunications monopoly routed through a secret bank account and front companies. It was not a situation that it could either afford or justify — and if exposed it would be embarrassing, or worse.

In a searing evaluation, Creative Associates said Mobile Accord had ignored sustainability because "it has felt comfortable receiving USG financing to move the venture forward."

Out of 60 points awarded for performance, Mobile Accord scored 34 points. Creative Associates complained that Mobile Accord's understanding of the social mission of the project was weak, and gave it 3 out of 10 points for "commitment to our Program goals."

Mobile Accord declined to comment on the program.

In increasingly impatient tones, Creative Associates pressed Mobile Accord to find new revenue that would pay the bills. Mobile Accord suggested selling targeted advertisements in Cuba, but even with projections of up to a million ZunZuneo subscribers, advertising in a state-run economy would amount to a pittance.

By March 2011, ZunZuneo had about 40,000 subscribers. To keep a lower profile, it abandoned previous hopes of reaching 200,000 and instead capped the number of subscribers at a lower number. It limited ZunZuneo's text messages to less than 1 percent of the total in Cuba, so as to avoid the notice of Cuban authorities. Though one former ZunZuneo worker — who spoke on condition of anonymity because he was not authorized to speak publicly about his work — said the Cubans were catching on and had tried to block the site.

—

Toward the middle of 2012, Cubans began to complain that the service worked only sporadically. Then not at all.

ZunZuneo vanished as mysteriously as it had appeared.

By June 2012, Cubans who had access to Facebook and Twitter were wondering what had happened.

"Where can you pick up messages from ZunZuneo?" one woman asked on Facebook in November 2012. "Why aren't I receiving them anymore?"

Users who went to ZunZuneo's website were sent to a children's website with a similar name.

Reyner Aguero, a 25-year-old blogger, said he and fellow students at Havana's University of Computer Sciences tried to track it down. Someone had rerouted the website through DNS blocking, a censorship technique initially developed back in the 1990s. Intelligence officers later told the students that ZunZuneo was blacklisted, he said.

"ZunZuneo, like everything else they did not control, was a threat," Aguero said. "Period."

In incorrect Spanish, ZunZuneo posted a note on its Facebook page saying it was aware of problems accessing the website and that it was trying to resolve them.

"¡Que viva el ZunZuneo!" the message said. Long live ZunZuneo!

In February, when Saimi Reyes, and her boyfriend, Ernesto Guerra, learned the origins of ZunZuneo, they were stunned.

"How was I supposed to realize that?" Guerra asked. "It's not like there was a sign saying 'Welcome to ZunZuneo, brought to you by USAID.' "

"Besides, there was nothing wrong. If I had started getting subversive messages or death threats or 'Everyone into the streets,' " he laughed, "I would have said, 'OK, there's something fishy about this.' But nothing like that happened."

USAID says the program ended when the money ran out. The Cuban government declined to comment.

The former web domain is now a placeholder, for sale for $299. The registration for MovilChat, the Cayman Islands front company, was set to expire on March 31.

In Cuba, nothing has come close to replacing it. Internet service still is restricted.

"The moment when ZunZuneo disappeared was like a vacuum," Guerra said. "People texted my phone, 'What is happening with ZunZuneo?'

"In the end, we never learned what happened," he said. "We never learned where it came from."

Table of Contents

Information Warfare: Twitter Becomes a Battlefield

From Strategy Page, 3 April 2014

April 3, 2014: Islamic terrorists have been early and energetic adopters of social media on the Internet. But the terrorists soon found that the messaging went two ways and those who disagreed with them had no trouble, or inhibitions about responding to terrorist messages. This was particularly the case with Twitter. Here even the U.S. State Department found it effective to assign people to respond to terrorist tweets. The State Department had people who spoke Arabic and other languages Islamic terrorist fanboys used and had the culture awareness to become very annoying for the true-believers.

Interrogations of captured terrorists or terrorism suspected revealed that the responses, especially those from a government agency, had an impact. It scared off many potential terrorist recruits and angered true believers, often to the point where they would reveal things they should have kept to themselves. This sort of backtalk because such a problem that terrorist leaders began warning followers to ignore these infidel taunts and insults and to not respond. The Internet being what it is, most pro-terrorist twitter users found themselves unable or unwilling to heed this advice.

This interference has become a growing problem for Islamic terrorist organizations. That's because the continued use of international media to keep people (largely disaffected Moslems and Western leftists looking for a new lost cause) informed about how the terrorist group is still around was being diminished by this interference. Maintaining such visibility is essential for recruiting. Al Qaeda has always recruited from the least educated and most desperate Moslem men out there. Religious fervor was not crucial but the willingness to suffer and die was. These recruits are attracted to the image of al Qaeda as being constantly active, no matter what damage they suffer. Also important was maintaining support from older, more affluent, and less desperate supporters. It was to keep these rich men willing to help out with cash or access to needed resources. The new recruits and other contributions were only forthcoming if al Qaeda could demonstrate that it was active. Thus there is a constant need for new "actions" (assassinations, bombings, prison breaks, and other media-worthy events) to remind wealthy fans of Islamic radicalism that cash keeps it all going.

The core terrorist leadership has always contained some technically adept people who recognized how the media worked and appreciated how new technology was changing how you reached and maintained those supporters. So it should not be surprising that al Qaeda and other terrorist organizations became heavy users of Twitter and other social media sites. Even though many of these sites do not welcome al Qaeda, the Islamic

terrorists keep at it and maintain a presence in high-traffic areas. Much of this is made possible by Internet-savvy volunteers who don't want to blow themselves up but are willing to risk (and it is not a big risk) arrest by working from home to serve the cause and keep al Qaeda visible on the Internet and thus in the mass media. Now all that is being compromised by the growing pushback by individuals and organizations hostile to terrorism.

There are other problems. For example several times in January 2014 Hamas, a Palestinian Islamic terrorist group that rules the Gaza Strip had its Twitter accounts suspended for violating the Twitter terms of service. Hamas was constantly advocating genocide and the use of terrorism against civilians. Hamas makes no secret about its desire to destroy Israel and kill any Jews who did not leave the region. Twitter points out that since Hamas has been designated (since 1997) as a Foreign Terrorist Organization it is against U.S. law for American firms to provide it with any kind of support. This is not always enforced, unless the terrorists seem to be making effective use of something and then the company in questioned is reminded of the law by the U.S. government. Hamas has long been using the Internet to get its message out, as well as to raise money and seek out recruits. Apparently they were becoming too blatant with getting their message out using accounts operated by Hamas. At the same time there were more and more non-Moslem media monitoring groups that were publicizing what Arab language media (of Hamas and other Islamic radical groups) were saying about their goals. While these groups moderate their message in English, they are more blunt and scary in Arabic. This is not a translation issue, Hamas leaders want to kill lots of Jews and are not happy about their lack of success.

Hamas is not the only Islamic terrorist group to have had their Twitter accounts shut down. This sort of thing has become more frequent as Twitter turned into another form of mass media. In 2013 Somali Islamic terrorist group Al Shabaab had its twitter account shut down several times for violating Twitter terms of service. Twitter management was particularly upset when al Shabaab used twitter to announce and discuss its involvement in a horrendous terror attack on a Nairobi, Kenya shopping mall that killed over 60 civilians. For that al Shabaab had its twitter account shut down on September 6th. Despite that the terrorist group started a new account on September 10th that was also shut down. Earlier in 2013 (February) al Shabaab began using a new Twitter account and criticized Twitter for shutting down al Shabaab's original (since 2011) account on January 20th because the Islamic terrorists had used Twitter to make specific threats against several people on January 16th. This is not allowed by the Twitter terms of service. The al Shabaab account had over 20,000 followers.

The Hamas account had more than twice as many. Both groups are still active on Twitter using accounts that do not feature the name of the groups. Hamas also tries to distance itself from the nasty stuff said in its name by claiming it's all the fault of a "militant wing" of Hamas.

Table of Contents

U.S. Tries Candor to Assure China on Cyberattacks

By David Sanger, New York Times, 06 Apr 2014

WASHINGTON — In the months before Defense Secretary Chuck Hagel's arrival in Beijing on Monday, the Obama administration quietly held an extraordinary briefing for the Chinese military leadership on a subject officials have rarely discussed in public: the Pentagon's emerging doctrine for defending against cyberattacks against the United States — and for using its cybertechnology against adversaries, including the Chinese.

The idea was to allay Chinese concerns about plans to more than triple the number of American cyberwarriors to 6,000 by the end of 2016, a force that will include new teams the Pentagon plans to deploy to each military combatant command around the world. But the hope was to prompt the Chinese to give Washington a similar briefing about the many People's Liberation Army units that are believed to be behind the escalating attacks on American corporations and government networks.

So far, the Chinese have not reciprocated — a point Mr. Hagel plans to make in a speech at the P.L.A.'s National Defense University on Tuesday.

The effort, senior Pentagon officials say, is to head off what Mr. Hagel and his advisers fear is the growing possibility of a fast-escalating series of cyberattacks and counterattacks between the United States and China. This is a concern especially at a time of mounting tensions over China's expanding claims of control over what it argues are exclusive territories in the East and South China Seas, and over a new air defense zone. In interviews, American officials say their latest initiatives were inspired by Cold-War-era exchanges held with the Soviets so that each side understood the "red lines" for employing nuclear weapons against each other.

“Think of this in terms of the Cuban missile crisis,” one senior Pentagon official said. While the United States “suffers attacks every day,” he said, “the last thing we would want to do is misinterpret an attack and escalate to a real conflict.”

Mr. Hagel’s concern is spurred by the fact that in the year since President Obama explicitly brought up the barrage of Chinese-origin attacks on the United States with his newly installed counterpart, President Xi Jinping, the pace of those attacks has increased. Most continue to be aimed at stealing technology and other intellectual property from Silicon Valley, military contractors and energy firms. Many are believed to be linked to cyberwarfare units of the People’s Liberation Army acting on behalf of state-owned, or state-affiliated, Chinese companies.

“To the Chinese, this isn’t first and foremost a military weapon, it’s an economic weapon,” said Laura Galante, a former Defense Intelligence Agency cyberspecialist. She now works for the Mandiant division of FireEye, one of the largest of the many cybersecurity firms seeking to neutralize attacks on corporations from China and other countries, as well as criminal groups and hackers.

Administration officials acknowledge that Mr. Hagel, on his first trip to China as defense secretary, has a very difficult case to make, far more complicated than last year. The Pentagon plans to spend $26 billion on cybertechnology over the next five years — much of it for defense of the military’s networks, but billions for developing offensive weapons — and that sum does not include budgets for the intelligence community’s efforts in more covert operations. It is one of the few areas, along with drones and Special Operations forces, that are getting more investment at a time of overall Pentagon cutbacks.

Moreover, disclosures about America’s own focus on cyberweaponry — including American-led attacks on Iran’s nuclear infrastructure and National Security Agency documents revealed in the trove taken by Edward J. Snowden, the former agency contractor — detail the degree to which the United States has engaged in what the intelligence world calls “cyberexploitation” of targets in China.

The revelation by The New York Times and the German magazine Der Spiegel that the United States has pierced the networks of Huawei, China’s giant networking and telecommunications company, prompted Mr. Xi to raise the issue with Mr. Obama at a meeting in The Hague two weeks ago. The attack on Huawei, called Operation Shotgiant, was intended to determine whether the company was a front for the army, but also focused on learning how to get inside Huawei’s networks to conduct surveillance or cyberattacks against countries — Iran, Cuba, Pakistan and beyond — that buy the Chinese-made equipment. Other cyberattacks revealed in the documents focused on piercing China’s major telecommunications companies and wireless networks, particularly those used by the Chinese leadership and its most sensitive military units.

Mr. Obama told the Chinese president that the United States, unlike China, did not use its technological powers to steal corporate data and give it to its own companies; its spying, one of Mr. Obama’s aides later told reporters, is solely for “national security priorities.” But to the Chinese, for whom national and economic security are one, that argument carries little weight.

“We clearly don’t occupy the moral high ground that we once thought we did,” said one senior administration official.

For that reason, the disclosures changed the discussion between the top officials at the Pentagon and the State Department and their Chinese counterparts in quiet meetings intended to work out what one official called “an understanding of rules of the road, norms of behavior,” for China and the United States.

The decision to conduct a briefing for the Chinese on American military doctrine for the use of cyberweapons was a controversial one, not least because the Obama administration has almost never done that for the American public, though elements of the doctrine can be pieced together from statements by senior officials and a dense “Presidential Decision Directive” on such activities signed by Mr. Obama in 2012. (The White House released declassified excerpts at the time; Mr. Snowden released the whole document.)

Mr. Hagel alluded to the doctrine a week ago when he went to the retirement ceremony for Gen. Keith B. Alexander, the first military officer to jointly command the N.S.A. and the military’s Cyber Command. General Alexander was succeeded last week by Adm. Michael S. Rogers, who as the head of the Navy’s Fleet Cyber Command was a central player in developing a corps of experts who could conduct cyberwarfare alongside more traditional Navy forces.

“The United States does not seek to militarize cyberspace,” Mr. Hagel said at the ceremony, held at the N.S.A.’s headquarters at Fort Meade, Md. He went on to describe a doctrine of “minimal use” of cyberweaponry against other states. The statement was meant to assure other nations — not just China — that the United States would not routinely use its growing arsenal against them.

In Beijing, the defense secretary “is going to stress to the Chinese that we in the military are going to be as transparent as possible,” said Rear Adm. John Kirby, the Pentagon press secretary, “and we want the same openness and transparency and restraint from them.”

Experts here and in China point out that a lot was left out of Mr. Hagel’s statement last week. The United States separates offensive operations of the kind that disabled roughly 1,000 centrifuges in Iran’s nuclear program, America’s best-known (and still unacknowledged) cyberattack against another state, from the far more common computer-enabled espionage of the kind carried out against the Chinese to gather information about a potential adversary.

“It’s clear that cyberspace is already militarized, because we’ve seen countries using cyber for military purposes for 15 years,” said James Lewis, an expert at the Center for Strategic and International Studies. “The Chinese have had offensive capabilities for years as well,” he said, along with “more than a dozen countries that admit they are developing them.”

Table of Contents

The Ukrainian Crisis – A Cyber Warfare Battlefield

By Simon Tsipis, Defense Update, 5 Apr 2014

Russia has managed to hit almost all Ukraine government websites and it was able to take control and to put on surveillance and monitoring all the Internet and telephone communications lines, before the invasion and occupation of Crimea by its military. Russian Special Forces managed to derail all important communications systems through direct physical impact on them by combined field and high-tech operation.

Cyber espionage is an integral part of military strategy and foreign policy of Russia towards the countries of the former Soviet Union. Being able to access information systems of diplomatic, government and military organizations for many years, since the USSR collapse, giving Russia a huge advantage in predicting their tactics, actions and analyzing the thinking of their neighbours.

The largest military cyber attack was the attack implemented by the Russian Military Intelligence (GRU) on the armed forces of Ukraine, as reported by BBC. According to the law enforcement agencies of Ukraine, Russian cyber attacks collapsed the communication systems of almost all Ukrainian forces that were based in Crimea that could pose danger to the invading Russian troops. Attacks of a lesser scale were directed at government websites, news and social networks. Similar handwriting and set of actions has been committed by the Russian military during the war against Georgia, a fact which suggests that the invasion operation in the Crimea has been carefully planned in advance. The Head of the Security Service of Ukraine, Valentin Nalevaychenko admitted, that mobile communication systems of members of the Ukrainian government were attacked in order to neutralize and disrupt communication between government agencies. As the Ukrainian company Ukrtelecom announced, unmarked gunmen penetrated into their infrastructure objects and the optical fiber and conductor units were knocked out, which in turn led to the collapse of all communication. Despite this, western experts say that Russian forces were relatively moderate in their actions and are able to engage much more global cyber-attacks.

Being able to access information systems of diplomatic, government and military organizations for many years, since the USSR collapse, gave Russia a huge advantage in predicting their tactics, actions and analyzing the thinking of their neighbours

According to a former senior officer of the CIA’s Special Operations department Marty Martin, the more extreme attacks will be held by the Russians in case of greater escalation of the conflict. “Sometimes it is useful to keep some lines of communication working, in order to be able to monitor and control, than completely derail them and deprive yourself from intelligence sources.” says Martin. In fact, experts say, no one in the world so far, including the CIA, is not able to assess the possibility of Russian cyber-capabilities as large-scale conflict with its participation yet haven’t been at place.

Additional obstacle to Western intelligence agencies, in the definition of “friend or foe” and who on which side, was the fact that both sides are communicating virtually on the same language, writing scripts by the similar rules and often attack each other with similar IP addresses.

A founder of U.S. cyber security consulting company “Red Branch Consulting” Paul Rozenshveyg argues that Russia is quite strong in cyber, but he warns that we should not overestimate the cyber-space as a place of major future wars, in comparison with ground operations, if the situation gets out of control. “Cyber attacks will not bring much damage,” Paul said “when the tanks will get on course.”

According to the director of the California based privet cyber-security company “CrowdStrike” Dmitri Alperovitch, there have been observed a great amount of cyber attacks and surveillance activity in Ukraine

cyberspace during the crisis. Dmitry also said that despite the fact that both the Ukrainian and Russian hackers came out of the same "schools", the difference in the capabilities of Russia and Ukraine is essential. Russia, he said, ranks among world leaders for its cyber capabilities, while Ukraine "doesn't even come close to a third …"

Another expert in this field, the director of the initiative group "Atlantic Council on the State of Cyber-management" and former adviser on cyber-security issues of the White House, for the Bush administration, Jason Harley, argues that today we are witnessing a different approach to cyber warfare from the Russian side, rather than in the conflicts in Georgia and Estonia. Moscow, he says, applied in the Ukrainian case, higher level of "hands-on" attacks. This is, an old school Cold War tactics. Physical contact with cyber equipment in hostile territory is an old, and far not ineffectual way, the Russian security services used to work in the past. In the near future, we will see more large-scale operations by such means, he added. In the case of Ukraine, there was absolutely no difficulty for Russian special forces to penetrate any military or strategic facility in Ukraine, since the equipment and facilities were built by the same experts when the two countries were under one rule. The Russian intelligence services are possessing all the required documents and location maps of all the important objects in the territory of the former Soviet Union, as well as specialists, some of whom participated in the construction of these objects and are today reside in Russia. Thus, says Harley, any kind of intervention or sabotage in the former Soviet Union territories, can be quickly and efficiently suppressed by Russian security services, which makes such attempts almost meaningless. Today, all cyber-space mainly based on remote attacks such as denial-of-service (DDoS), while if physical penetration and chopping off or putting under control of telephone and Internet communication is possible, remote attacks lose most of its effect.

One of the techniques used by the Russians for cyber espionage was the "Snake", also known as Ouroboros and Uroburos. It was developed in Russia at least four years ago, with some elements of software created in 2005. Its name, Urobos has been taken from Greek mythology and it is capable of inducing chaos in communication system, and this is exactly what it did in Ukraine. What's interesting about it is the fact, that it is able to combine two in one. It is able to be used as stealthy means for network surveillance and data collection, it can also carry out a 'warhead' – able to physically destroy computer networks specifically targeted by its operators. The use of Urobos, along with the physical attacks against networks therefore combined both "old school" operations with modern, cyber warfare techniques to gain the desired impact.

While Russian cyber operations in Ukraine were based on the experience and lessons learned from previous attacks on Estonia and Georgia, they haven't left 'fingerprints' leading to the sources. Todays cyber wars are waged in a domain that lacks rules of war, what could bring a country threatened by such all-out cyber offensive to turn to physical retaliation, in the absence of effective international legal and cyber security tools.

As for the Ukraine, some details on the use of cyber-means in the country are now been disclosed. The extents of the corruption of the Yanukovych's government, after his overthrow, are crawling out. It became known that in December 2013, when the confrontation on Independence square (the Maydan) were gaining strength, Ukrainian hackers have posted online information about some senior members of the government that appealed to them with requests to crack Internet sites and other resources of the State Government Organizations for personal means. Thus, on the night of December 23 2013, all sites of Ukrainian government were hacked by the cyber-activists. However, hackers have published the stolen information in the public domain, admitting that they were forced to do so, as they had not been paid for hacking the databases. Furthermore, according to those hackers, First Deputy Chairman of the Verkhovna Rada of Ukraine and the former chairman of the State Customs Service of Ukraine Igor Kalyetnik addressed them, requesting access to the Unified State Register of Voters of Ukraine. He asked for "full control over more than a hundred public mailboxes of government members. In addition, hackers received a request to access the e-mail of the Chairman of the Verkhovna Rada of Ukraine Volodymir Rybak and Minister of Internal Affairs of Ukraine Vitaliy Zakharchenko. It is important, that in addition to mail-boxes, Kalyetnik wished to establish control over personal mobile devices of the aforementioned officials. According to cyber criminals, there is still a lot of information at their disposal, and they intend to publish the data of the Ministry of Finance, bank account numbers and other details of the Treasury of Ukraine.

Cyber events during the Russia-Ukraine conflict

December 16, 2003: Ukrainian hackers group "KiberBerkut" direct an attack against several NATO websites, their actions were attributed to the presence of "the NATO occupiers" on Ukraine territory.

March 7, 2014: Attacks are directed against Russian news and media websites, the Ukrainian hackers group "Kibersotnya" claimed to be responsible for the collapse of the site "Russian newspaper". Another cyber attack has undergone news agency Lenta.ru, administration.

March 9, 2014: Indian government confirms that a military documents concerning Indo-Russian negotiations over fighter aircraft were compromised by unknown hackers. The assumption is that someone, not necessarily Ukraine, trying to explore the possibilities of Russian Air Forces, through hacking databases with such information that are available in other country's air-forces whose systems are much less secure than the Russia's.

March 14, 2014: Russian armed forces were able to intercept and seize American reconnaissance and strike UAV over Crimea. The drone, an Israeli built MQ-5B 'Hunter', one of 18 operated by the US Army's 66th Military Intelligence Brigade. The unit regularly stationed in Bavaria, Germany was transferred to Ukrainian Kirovograd in early March, from where the UAVs performed reconnaissance raids over Ukraine, Crimea and the Russian border regions.

March 14, 2014: Multiple Distributed Denial of Service (DDoS) attacks, allegedly by Ukrainian hackers, are directed at Russian government and commercial websites. Targets include the Mr. Putin's presidential website, the official government website and the Central Bank of Russia, Portals of the Russian Ministry of Foreign Affairs and energy consortium Gazprom. As suggested by the FSB, all the attacks committed by Ukrainian hackers or hackers hired by Ukrainian opposition but, Russian law enforcement agencies also do not rule out the fact that in those attacks may have been involved foreign individuals or entities as well.

March 17, 2014: VTB and the Alpha bank, two of the largest Russian banks, suffer major cyber attacks damaging the on-line banking service and credit organization. An anonymous Caucasus hacker group took responsibility for those attacks.

Table of Contents

Researcher: Finnbay Activities May Be Part of Psychological Warfare

By Laura Halminen and Niina Woolley, Helsinki Times, 07 Apr 2014

Finnbay's activities have similarities to information operations, which aim to stir and confuse public debate, says Mika Aaltola, a researcher at the Finnish Institute of International Affairs.

Last Saturday, the English-language news service Finnbay published an article claiming that Finland would continue collaboration with Russia, regardless of the stance of the United States and the EU. The Finnish ambassador in Russia, who dubbed the website a "fake news site", was threatened with a court case by Finnbay.

"Typically an information operation's strategy involves establishing a cover activity that is not too transparent. The idea is to pass communication that aims to nudge public debate to the desired direction amid true information," explains Aaltola.

In this case, Aaltola says the desired direction is to cause confusion in the public debate.

"The news will keep circulating, whether true or not. The idea is to give an impression that Finland is in a conflicting situation and turning to Russia for support. At the same time, the threat posed by Russia is mentioned, creating a picture that Finns are feeling confused."

Aaltola uses the US and Israel as examples of countries who use carefully considered formulations and wording in their information operations, which can make it difficult to figure out the source of the misinformation.

"The operations are multi-layered making it difficult to find who provides the funding."

Ilta-Sanomat, Helsingin Sanomat and Yleisradio all published reports on Finnbay's activities yesterday after which the news service announced on their website that they do not have a Finnish business ID because the organisation is run by volunteers and its turnover does not exceed the allowed limit. Finnbay also claimed that Yle published "racist content".

"White-washing is part of the normal operation model. It would not be surprising if they published something sensational tomorrow as a distraction," says Aaltola.

On its website, Finnbay gives the idea that it publishes a newpaper called Helsinki Novosti, which has been granted funding by an association supporting Russian citizens living outside Russia, according to information received by Helsingin Sanomat. The association was founded by the Russian Ministry for Foreign Affairs and Rossotrudnitshestvo, an advocacy agency for Russians abroad. Helsingin Sanomat did not yet have further information on the link between Finnbay and Helsinki Novosti.

“Information operations typically involve several operators,” says Aaltola. “The website is just one part of the operation. Often some the parties involved are funded by associations, and some of those involved are just ‘useful idiots’ who disseminate the information. Intelligence services can also be directly involved.”

Table of Contents

Information Warfare: Very Dangerous Videos

From Strategy Page, 7 April 2014

April 7, 2014: One of the things that worries North Korean leaders the most is the realization that decades of propaganda, which kept most North Koreans believing they were better off than South Koreans, has been undone by videos illegally brought in on CDs, DVDs and memory sticks that revealed what was really going on in the south. In the last decade this has undone all that energetic and expensive propaganda work.

In South Korea there have been so many North Koreans arriving in the last decade that it has become possible for polling companies to conduct surveys that provide an accurate view of attitudes up north. For example over 90 percent of North Koreans know the South Koreans have a higher standard of living. One defector attributed that insight to the fact that while he was in the army his unit was shown a propaganda film depicting the depraved conditions in South Korea. Once scene showed a neighborhood that had all sorts of night clubs and bars, complete with many bright lights (as are common in most East Asian cities). For many of the soldiers this did not indicate South Korea was depraved (which has a certain appeal to young men everywhere) but rich. Most of these young troops had never seen so many lights at night. The only city that has a lot of outdoor lighting at night in North Korea is the capital. Space satellite pictures show clearly what was happening. Most of North Korea is dark in these photos, except for the capital and small blips of light at some other cities. In contrast South Korea is lit up like any Western country. Refugees from the north, on seeing these photos, are not surprised because they lived in the dark spaces for years.

The surveys also indicate that despite the difficulty adjusting to life in the fast-paced south, most of the northern refugees are adapting and most want to save money to pay the bribes required to get their families out of North Korea. The northern refugees also agree that North Korea is close to economic and government collapse.

Collapse in North Korea makes South Korea and China nervous and, according to opinion surveys more South Koreans are agreeing with China taking over up there. That’s because since the 1990s South Korean reunification experts have been studying what happened in Germany (after the communist East Germany was absorbed by the democratic West Germany). That cost the West German taxpayers over two trillion dollars. Estimates of what it will cost South Koreans to absorb North Korea are now over five trillion dollars. Then there was the fact that Germany had a GDP four times that of South Korea, meaning that the average South Korean will have to pay ten times what the average West German paid to rebuild their lesser half. This could cost South Koreans up to ten percent of their GDP for a decade or more. Many South Koreans fear that rebuilding the north could wreck the South Korean economy. No one knows, and everyone is scared. But someone will have to pay, and the most likely candidate is the South Korean taxpayer. Unless, of course, China is allowed to take over. This is something China is not only willing to do but is kind of insisting on.

Meanwhile South Korea is seeking ways to deal with the discrimination issue. This was a problem when communist East Germany was absorbed by democratic West Germany. Most South Korean see North Koreans as different, more passive and less economically successful. This was not unexpected by government planners. This social distance was a big problem when East and West Germany were reunited in the early 1990s. The easterners had lived under communism for 45 years, and that made them different, and not in good ways. The western Germans often avoided, or mocked eastern Germans. These tensions still exist more than two decades after the unification.

For a long time it was popular to believe that reunification with the north could be done gradually, by making peace with the communist dictatorship up there, and gradually merging the two economies. But the northern communists have proved unreliable, incompetent and seemingly out-of-touch with reality. So now, South Korea believes that unification will come in the wake of economic and political collapse in the north. In other words, the worst case. South Koreans tend to agree on one thing, that the cost of cleaning up after a collapse will be huge. Leaving China to take over and turn North Korea into an extension of northeast China, while practical, bothers a lot of South Koreans. That because for a long time the southerners will be accused of abandoning their fellow Koreans in the north. Korea has a long tradition of resisting Chinese aggression and control. As a result there are no easy outcomes to this mess for all Koreans.

Table of Contents

Cyber Warfare Research Institute to Open at West Point

By Joe Gould, Army Times, Apr. 7, 2014

The Army's academy has established a cyber warfare research institute to groom elite cyber troops and solve thorny problems for the Army and the nation in this new warfighting domain.

The U.S. Army Military Academy at West Point, N.Y., plans to build a cyber brain trust unprecedented within the service academies, filling 75 positions over the next three years — including scholars in technology, psychology, history and law, among other fields.

The chairman of the organization, called the Army Cyber Institute, will be retired Lt. Gen. Rhett Hernandez, the first chief of Army Cyber Command, according to Col. Greg Conti, the organization's director.

The institution, which aims to take on national policy questions and develop a bench of top-tier experts for the Pentagon, will be defining how cyber warfare is waged, to steer and inform the direction of the Army.

"It's a very exciting time," Conti said. "It feels a bit like we're at the birth of the Air Force, like we're that kind of historic era."

The institute's interdisciplinary approach will join civilian doctorate-level experts in cybersecurity and cyber operations with psychologists, attorneys, policy experts, mathematics experts and historians within its walls.

"I think we're building a unique team that's never been done before," Conti said. "People think of technology, and maybe policy, but it's never been done before in this holistic way."

Cyber experts from the operational cyber force would rotate through the institute as students and faculty, bringing hands-on experience and emerging with a broader perspective, better equipped as leaders, Conti said.

The institute will strive to connect to the "constellation" of expertise in academia, industry and national labs, with its own "fresh, agile organization," Conti said.

The plan is to recruit and hire about 25 people per year when competition is hot to hire cyber experts, but Conti was confident West Point's reputation and relationships would attract the right people.

There is no shortage of questions for personnel at the institute to noodle over. How does a unit "maneuver" in cyberspace? How do troops fight and win in a large scale cyberwar? What would a cyber Ranger School look like?

"We want to get ahead of doctrine," Conti said.

West Point has offered cyber education for years under various names, including information assurance or information warfare, but it launched a small dedicated cyber security program in 1999 that has grown significantly since. Graduates and faculty worked to launch Army's cyber four years ago.

Though Conti said the interdisciplinary model for the Army Cyber Institute is novel, officials there looked to the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, the Georgia Tech Information Security Center, Stanford Center for Internet and Society, among others.

Army senior leaders 18 months ago approved the expansion of the Army cyber center to take on national-level problems and develop a bench of top-tier experts for Army. It follows the creation of Army Cyber Command and comes amid the command's ongoing reorganization and the consolidation of the Army signals school into the Army Signal Center of Excellence, at Fort Gordon, Ga.

The idea for the institute comes after Odierno emphasized the importance of cyber in a National Press Club talk on Jan. 7, saying cyber would, "impact future warfare." He said it is in the national security interest to resolve fundamental legal and policy issues.

"As a national issue, this is about our ability to protect our financial networks, our infrastructure, and it's an important issue," he said. "We have to recognize this is a new way for people to potentially influence what's going on in the United States, so it's incumbent upon us to improve our capability."

Table of Contents

China's President Xi Urges Greater Military Use of Space

By Ben Blanchard, Reuters, 14 April 2014

BEIJING (Reuters) - Chinese President Xi Jinping urged the air force to adopt an integrated air and space defence capability, in what state media on Tuesday called a response to the increasing military use of space by the United States and others.

While Beijing insists its space program is for peaceful purposes, a Pentagon report last year highlighted China's increasing space capabilities and said Beijing was pursuing a variety of activities aimed at preventing its adversaries from using space-based assets during a crisis.

Fears of a space arms race with the United States and other powers mounted after China blew up one of its own weather satellites with a ground-based missile in January 2007.

A detailed analysis of satellite imagery published in March provided additional evidence that a Chinese rocket launch in May 2013, billed as a research mission, was actually a test of a new anti-satellite weapon.

Visiting air force headquarters in Beijing, Xi, who is also head of the military, told officers "to speed up air and space integration and sharpen their offensive and defensive capabilities", Xinhua news agency said late on Monday.

It gave no details of how China expects to do this.

China has to pay more attention to its defensive capabilities in space, the official China Daily said on Tuesday.

"The idea of combining air and space capability is not new to the Chinese air force, as a host of experts have underscored the importance of space," it said.

Wang Ya'nan, deputy editor-in-chief of Aerospace Knowledge magazine in Beijing, said Xi's call for integrated air and space capability is to answer the need of the times.

"The United States has paid considerable attention and resources to the integration of capabilities in both air and space, and other powers have also moved progressively toward space militarization," Wang Ya'nan was quoted as saying.

"Though China has stated that it sticks to the peaceful use of space, we must make sure that we have the ability to cope with others' operations in space."

The United States was the first country to develop anti-satellite weapons in the 1950s, but currently has no known weapons dedicated to that mission.

China has been increasingly ambitious in developing its space programs for military, commercial and scientific purposes. Xi has said he wants China to establish itself as a space superpower.

But it is still playing catch-up to established space superpowers the United States and Russia. China's Jade Rabbit moon rover has been beset by technical difficulties since landing to great domestic fanfare in mid-December.

Table of Contents

‘Dangerous’ Era of Dissent May Have Begun

By Andrei Lankov, NK News, April 8th, 2014

It seems that the “era of dangerous talks” has, at last, begun. Reports coming from numerous unrelated and generally trustworthy sources point to a significant, albeit not necessarily quantifiable, change in North Korean society. Educated North Koreans, including junior members of the elite, have begun to privately and seriously discuss political issues – and these discussions do not usually follow the officially prescribed line. This is a new development: the first signs of this deviance have become visible only since around 2011.

This does not mean that North Korean college teachers, mid-ranking police officers and market vendors are now dreaming of revolution. Nonetheless, they are increasingly aware that their country is lagging behind China, not to mention South Korea, they are becoming more and more inclined to blame their own government and their country’s economic and political system, rather than the notorious U.S.-instituted blockade or other twists of fate – and they are willing to talk about this.

“They are becoming more and more inclined to blame their own government and their country’s economic and political system”

In the past, some educated North Koreans also understood that everything was not right in their land, but only recently it seems that a significant number of them have become willing to raise these topics in private conversations, including conversations with relatively trustworthy foreigners. The latter is not all that surprising, many elite North Koreans are probably well aware that foreigners are among the safest people to share political misgivings with. After all, they have no reason to report you.

So far, it seems that dissatisfied North Koreans do not have much in the way of expectations. In most cases, their dream is for their country to emulate China’s reforms and economic miracle. They also might dislike the late Kim Jong Il, but most of the time they seemingly hope that his young son, the incumbent Supreme Leader will somehow fix things. And, of course, they still usually have great adoration and respect for Kim Il

Sung, the founder of the Kim dynasty, even though the policies of the late strongman are actually the main reason why they are in this mess.

WHY NOW?

This change of mind has come about as the result of a combination of factors – most of which have been around for around 20 years. First, the spread of information about the outside world is important, and such information has spread in North Korea through a multitude of channels. Second, it helps that North Korea under Kim Jong Il was much less repressive than that of his father Kim Il Sung. Third, the growth of the black market economy and endemic corruption have made people both more independent of the government and more critical of it. Last but not least, a palpable improvement of living standards over the last 10-15 years also means that people are less stressed and have more time to think about politics and other lofty issues (contrary to what is often believed, revolutions seldom happen when people are really desperate and cornered).

Reports about changes in the behavior of educated North Koreans are too numerous now to be dismissed as merely incidental or anecdotal. However, we should not see it as a sign that the North Korean state is now on the verge of collapse. Of course, collapse may well happen soon, but if we keep in mind the experiences of other communist states, we should not probably not start getting ready for our road trip to Pyongyang from Seoul. In the Soviet Union, for instance, the length of time it took for the emergence of relatively uninhibited political talk to lead to the collapse of the country was some 30 years.

“The talk one can now hear from educated North Koreans is quite reminiscent of the talk that could be heard in Moscow from the mid-1960s”

Indeed, the talk one can now hear from educated North Koreans is quite reminiscent of the talk that could be heard in Moscow from the mid-1960s. In the Soviet Union, this was also a time of moderate economic expansion and relative stability, this was also when the state stopped terrorizing its people (there were very few people going to prison for political crimes after 1953). Needless to say, the liberalization of the Soviet Union after 1956 was far more dramatic than what happened in North Korea after Kim Jong Il took over. The number of political prisoners in the Soviet Union decreased some 700-fold between 1953 and 1964 while in North Korea of the last decade this number merely halved.

Amid this post-Stalin political relaxation, the Soviet Union of the 1960s also began to become more open to the outside world. More Soviets going abroad to travel, more foreigners came to the Soviet Union, and increasing numbers of Soviet citizens began listening to foreign radio stations. The Soviet people began to realize what was all too obvious to their Western visitors: the Soviet Union was increasingly lagging behind the developed world. This spurred many of the Soviet intelligentsia to take up the issue of the country’s socio-economic plight over the kitchen table.

REFORM BUT NOT OPENNESS

People who have reported of growing discontent among their North Korean contacts often emphasize the fact that North Koreans are loathe to discuss revolution or the replacement of the Kim family. Usually, they express hope for reforms, and they are also afraid that in the current political climate, the North Korean government will be unwilling to implement necessary changes. This does not sound all that radical – what the most opposition minded North Koreans seemingly want is the introduction of Chinese-style developmental minded dictatorship, not the switch to a liberal democracy, the wonders of which they do not necessarily appreciate. Indeed, one can even hear North Koreans say that the present-day China is dangerously and unnecessarily liberal and permissive.

In one case, a North Korean businesswoman even said that “North Korea needs Chinese-style reforms but not Chinese-style openness.” She was assuming that proper patriotic discipline should still be instilled into North Koreans and that the North Korean media should provide the people with a wholesome ideological diet, rather than with the frivolous melodramas so frequently seen on Chinese TV.

This does not sound terribly radical, but one should keep in mind that Soviet intellectuals of the late 1960s were also not known for their anti-communism. Most of them wanted a more permissive and efficient government, not a complete or even partial switch to the capitalist market economy. The ideal Russian state as seen from a Moscow kitchen around 1970 would still be overwhelmingly socialist in its nature and would quite probably still be run by the Communist Party. Only in the 1980s would the Soviet public begin to entertain grave doubts about the viability of the entire state socialist project.

“It seems that the North Korean people are now at the beginning of a long and winding road of political self-doubt”

So, it seems that the North Korean people are now at the beginning of a long and winding road of political self-doubt. It is also possible that the Kim Jong Un government will find a way to return a level of repression not seen since the Kim Il Sung era. If this is going to happen, it will put an abrupt end to all politically dangerous talk. Fortunately, however, such a revival of old-school Stalinist terror seems to be quite unlikely because the government does not have the commitment or resources to realize such a project.

Nonetheless, even if history is allowed to take its course, one will probably have to wait quite a few years before one sees the discontented junior members of the elite being able to change the country's future. At any rate, things are beginning to change, and with the passage of time, the North Korean government is more and more likely to face pressures from within.

Table of Contents

Information Operations Is Just another Media Format Vying for the Eyes of the Audience

Contributor: The Platform, DefenceIQ, 04/08/2014

The following article has been written by a senior producer/director and Information Operations specialist at The Platform, a neutral strategic communications, media services and information management business working in stressed territories around the world.

"You can design and create, and build the most wonderful place in the world. But it takes people to make the dream a reality" - Walt Disney.

As far as I know, Walt Disney isn't often cited in articles about information operations, but, having borrowed the anthem of the Seven Dwarves for the title of my article, it seemed but a short hop to allude to the sentiments of their creator. However, there's editorial method in the madness.

Politicians, soldiers, strategists, advertising agencies and PR men are all adept at conjuring compelling visions of utopia – or at least peace and prosperity – for afflicted societies. But, as Walt Disney said, 'it takes people to make the dream a reality'. Beyond the world of cartoons and magic kingdoms, the same is true. Ordinary people are the real agents of change, and information operations are intended to help inform, influence and inspire those people toward making the decisions and adopting the behaviours that ensure the dream becomes a reality.

To talk of 'dreams' may imply something fantastical or ostentatious, but in the stressed territories where information operations are often applied, people's dreams are surprisingly modest: peace, security, a job, a future. Very few people in the world do not share this basic suite of ambitions, and information operations can exert great emotional power when acting upon these desires.

My interest in influence operations is as a practitioner. However, I'm not a soldier, civil servant or academic, though I've worked alongside all of those groups. I'm part of a small coterie of professional people whose impact upon information operations is often taken for granted, but whose direct influence is out of all proportion to their number and status.

As a television producer/director, I and my colleagues interpret strategic intent and bring it to life. Without producers, directors, editors, cameramen and sound recordists, the campaigns and strategies, however eloquently described and however persuasively sold, remain confined to the gaudy realm of the Powerpoint presentation. This is not to downplay the role of the strategist, campaign manager or anyone else, but simply to highlight the importance of the television maker's art in this field and to underline the point that upon the success or failure of the television product, may depend the success of the strategy. The product itself, whether it be a short news feature, a youth entertainment programme or a full blown documentary, is the vital nexus between target audience and strategy. If the product fails, so does the strategy, and so does the effort to influence.

The purpose of this article is to explore influence operations from the standpoint of the IO Producer, giving an insight into what he/she does, and explaining why the right people with the right skills and experience are critical to the overall success or failure of any information operation, and, moreover, are vital to the future of IO.

In this article I intend to convey my own experience, instinct and conviction as someone who not only worked in prime-time broadcast television for over a decade, but who, in the last five years of concentrated activity, has written, produced or presided over somewhere between 750 and perhaps as many as 1000 television influence products across various territories and various genres. I hope this piece will be a valuable summary of lessons learned from the recent past and offer some bold propositions for the future.

In writing this piece, I want to assert some of the principles I apply in creating IO products. I should say at the outset, 99% of my experience is in creating 'un-attributable' television products, and therefore the particular nuances of that field inform this article. My IO experience is in ENG (essentially, short news features), documentary and youth entertainment, amongst other formats. I was never concerned with television commercials, and I'm not going to talk about written material or radio, though some of the same principles may overlap.

I should also add, the bulk of this very concentrated experience is drawn from operations in Iraq, participating in an influence campaign that it's now rather fashionable to dismiss. Some of those who dismiss it are not perhaps acquainted with the intense daily activities of certain organisations, nor aware of the sophistication of some of the work or the innovation, let alone the products themselves. Whilse I certainly agree it's all up for serious review and I would still passionately critique the flaws that I critiqued while I was actually working in Iraq, I would be very cautious about promoting a wholesale dismissal of the advances made and the lessons learnt. Moreover, I would suggest the institutional knowledge gained in Iraq is invaluable.

In my opinion, there are some critical foundations to any IO product:

1. Firstly, whatever the message and whatever the intent, the product's primary challenge is to succeed as a piece of engaging and entertaining television. The clarity and persuasiveness of any strategic message contained in the piece is irredeemably compromised - if not totally lost - if the product doesn't grab the audience. Failure is assured just as certainly as if one scribbled a vital message and entrusted it to a dead carrier pigeon.

The role of the television professional is to capture the audience's attention and hold it, using all the skills of his craft. Not only does he interpret the strategy and breathe life into it, he provides the vital sugar that helps the medicine go down. This is why, in my opinion, you can't make successful IO unless you can make decent television.

2. IO products should aspire to compete with the best quality broadcast television, even if they are un-attributable.

I recognise that this assertion will seem counter-intuitive to some readers, because it's often contested that an un-attributable product should appear similar to locally produced programming in order not to appear conspicuous. That's often interpreted to mean it should look a little amateurish or home-spun. If the product is to deploy on social media and needs to look, 'user generated', that might be a consideration. However, I'd balance this concern about attribution - about products looking 'too good' - with a couple of thoughts.

Firstly, this notion has sometimes been employed cynically to excuse poor quality IO. That's not what the client pays for.

Further, it's folly to assume that all 'foreign telly' looks like Borat. It doesn't. Particularly in the Middle East, high-quality production values are appreciated and frequently seen (editorial or journalistic issues are another dimension, but let's confine ourselves to aesthetics for the time being). Secondly, to sustain the Middle East example, the demographic of the media industries there reflect the general demographics across the region. The Arab TV industry is young, comfortable with technology, multi-skilled, eager to learn and progressive. The TV industry in the Middle East is also influenced by the West - indeed a good many Western media professionals work in these industries now and standards are dramatically improving. Self-taught citizen journalists are moving into the mainstream media, being exposed to new technology and software, mastering it and seeking to excel. It would be complacent to assume that average work will continue to pass muster.

However, aside from professional pride, the overriding reason for making the best television we can possibly make, coincides with point one. It has to be judged at face value: It has to work as good television first. Bad or amateurish television doesn't suddenly 'work' because it's inconspicuous amongst the local programming. It simply means that it's not only bad television, it's bad IO too. My personal opinion is that if a product succeeds as a piece of television, the attribution will be of secondary relevance to the audience - it's the Trojan Horse effect. The audience is too busy consuming the narrative to consider where the message comes from. This is predicated, of course, on the assumption that the message is discreet, and based upon what is reasonable and logical, because though people might repudiate a message because of its assumed source, they can't generally repudiate logic forever.

3. Having talked quality, it's time to consider quantity, and this section assumes a broad, large-scale television campaign. The available funding and the capacity to carpet-bomb an audience with IO products might appear a desirable situation, but if the 'drumbeat' becomes a cacophony, problems emerge.

As a member of the IO community, and moreover, as someone with a mortgage, expressing this caveat might appear fatal to the fortunes of the industry. However, whilse volume might swell corporate coffers in the short

term, increasing output in a given theatre of operations inevitably diminishes returns, particularly where one or two formats are relied upon disproportionately and become conspicuous.

Increased volume creates a necessity for increasing numbers of conduits. Products need to be deployed, and in most territories, there are a limited number of viable broadcasters that cater to the particular target audiences. Over time, and relative to the quality, quantity and subtlety of products, the major domestic broadcasters' desire to deploy material inevitably drops off. But, if the big boys won't play, smaller channels will.

Minor channels, devoid of serious audiences and consequently strapped for cash, will deploy IO products. Presumably, some of these minor channels exist only to deploy IO products. They become a conduit not only for ENGs, but for regular transfusions of life-giving IO Dollars. As deployment of IO products become the major revenue for the channel and more and more jostle for space on the same channels, so audiences drop off even further, and the IO deployed becomes increasingly worthless. In these circumstances, IO merely props up failing channels and distorts the market.

As a wry footnote to this proposition, I recall watching a selection of minor Iraqi channels in around 2009-2010. It was a somewhat bleak epiphany. One channel's output consisted almost entirely of back to back IO products, produced by various cells and exhibiting greater or lesser degrees of virtuosity. The IO products were interspersed with seemingly uncut footage of jubilant dancing sheikhs. I wondered at the time whether these frolicking Arabs might not have been the various channels' owners, convening to celebrate the latest dollar bonanza. I hasten to add, that is no slur on them.

As an émigré from broadcast television, it would seem obvious to me to ask how many people were seeing the IO products I was making – indeed, that became a bitter obsession for me in Iraq. Arguments were advanced that the wafer thin slivers of the audience pie that represented the viewership of a considerable swathe of IO (mainly ENGs), was justified as it represented 'key constituencies'. Above a certain threshold, there might have been some validity to this assertion. However, when certain broadcasters were offering a potential audience of 4% and less[1], it would have been a great deal cheaper to organise a key leader engagement and take enough baklava for everyone. Good products were the least that was being wasted.

In mainstream television, nothing matters more than eyeballs on the product. Given that reality TV ratings and sales of toothpaste are less important than many of the ideas being 'sold' in IO campaigns, we should be a similarly obsessed with audience numbers.

Fewer, higher quality programmes with a greater variety of formats, longer lead time and better deployment would, in my opinion, provide greater value for money, avoid saturation and reduce 'IO fatigue' amongst the audience. [2]

4. The ideal IO product is one that succeeds as an entertaining piece of regularly-broadcast media, securing its own following, and messaging effectively, but seemingly incidentally. It might be a youth orientated magazine programme, a historical documentary, or a news review, but it could equally be any other popular genre; it may be narrated or presenter lead: we're limited only by our skill and our creativity.

Experience tells me that all of the above formats are viable. However, by and large, ENGs are undoubtedly still the default option. I'll advance an alternative model below, but these are my thoughts on the IO workhorse.

ENGs have great utility from a number of points of view. Firstly, they should be relatively cheap to make, and it's possible to turn them round reasonably quickly. A few skilled editors and a similar number of experienced producers have been known to post-produce thirty plus high quality ENGs a month. However, as above, fewer products with greater opportunity to craft and refine, probably represents a better modus operandi. Frequently deployed in the commercial space - sometimes rather too abundantly for discretion – ENGs are still a powerful tool to influence attitudes and change behaviour, if correctly composed.

To work effectively, I believe ENGs should be produced with reference to the following considerations.

ENGs should reflect reality. The producers need, as far as is possible, to understand that reality. Ideally, they'd live amongst the people they're messaging and appreciate the challenges of daily life. Where that isn't possible, they have to make every effort to understand the social and cultural norms which colour the environment. This understanding must necessarily go a lot deeper than rote learning of superficial stereotypes. Producers shouldn't be afraid to acknowledge the negative; it builds credibility and authenticity, and conceding a skirmish might just help to win a messaging battle. Modest claims are better than bold claims, and less likely to backfire. Finally, manage expectations and never message on promises.

ENGs should relay the voice of the people not the voice of the strategist. Sententious voiceover imposes a narrative, where the skillful television producer can draw out that same narrative from interviewees

using carefully crafted journalistic questions. The best ENGs have minimal voiceover, or no voiceover at all, and speak to the audience in the familiar vernacular of everyday people - people to whom the audience can readily relate. This is a powerful means to convey a message.

Finally, stay journalistic, stay objective, stay in touch: don't IO yourself…

Being involved in a long term campaign, especially one where you are removed from the general populace and from life on the street, one's apt to start becoming susceptible to one's own messages. Read everything, watch as much domestic television as possible and consume social media. Products which don't reflect reality just don't work.

So, what's the future? This article isn't merely supposed to be a Bluffer's Guide to IO, it's intended to influence, believe it or not…

IO needs to change. In my opinion, it needs to become more like mainstream television. IO producers and their clients need to proceed from the same professional start point as their cousins in mainstream TV. They need to commence with the question, 'what do people want to watch?' Once they have answered that question, they can think about messaging. It doesn't mean the message is secondary, but simply that for the message to actually reach the audience, the vehicle has to be effective. This applies whether the product occupies the advertising space or otherwise. It cannot be taken for granted that people will watch. But we need to go further than making decent ENGs.

As global audiences become more and more segmented and people graze and multi-task even as they view, IO products will have to work much harder if they're to secure people's attention and perhaps even draw their own audiences. The best products will inform, some will entertain, some will even make people laugh. IO can be produced to exist within every media genre, and to some degree, it already has. It simply needs to be further refined. Moreover, clients need to fully understand what can be achieved by professional television makers. To that end, they need to talk to them directly, to gauge feasibility and cost from the outset of any project.

Considering all the many billions of dollars that have been spent on IO in the last decade, there has been surprisingly little innovation or audacity, and even less attempt to stand back and take a long hard look at the basic propositions upon which messaging is founded.

From my own perspective as an IO producer, my ambition is not to have to foist my products upon the audience, but to have the audience seek out those products. This can be achieved if they are first and foremost successful pieces of television, cleverly conceived and creatively composed. This might seem like a huge additional challenge for the IO community, but when viewed objectively it must be recognised that it's the only hope for IO, if it is to succeed in the multi-platform, multi-genre media world. The one thing consumers of media are not seeking out, is dull, worthy, unsubtle and amateurish film and television. So, unless you have a captive audience, what other options are there but to aspire to the standards and creativity of the mainstream popular media?

The answer to the above proposition might be, 'but that's not what we do!' My riposte would be, 'it needs to be'. Nobody will watch otherwise. A message can be woven into any vehicle, from a cookery show or reality format, to a full blown feature-length documentary. An experienced television producer/director will have spent their whole career following formats, composing narratives, adhering to editorial agendas - that's all 'messaging' is. And is the gulf between popular media and IO so wide? Let's look back.

In 1939, Jan Anstruther's fictionalised account of a wartime British family was published under the title, Mrs Minever. It recounted the tribulations of the eponymous heroine and her family as they braced for war, and subsequently fought it on the home front. The book crossed The Pond and became a huge publishing sensation at a time when America was still neutral, and the public, and many within the establishment, were still opposed to involvement in another European war. The book and the more famous film, which followed in 1942, was credited with engendering empathy for the beleaguered and embattled British, and having a significant influence on American attitudes toward joining the war. FDR credited the film with having hastened US intervention, while Churchill claimed it had been worth, 'six divisions'.

Different times? Well, perhaps. But what about Michael Moore or Morgan Spurlock? Don't they do IO? What about Richard Branson's latest documentary project, Breaking the Taboo, which comprehensively dismantles the strategy behind the war on drugs? Isn't that IO? And very compelling IO?

Admittedly the two documentaries, Fahrenheit 9/11 and Supersize Me, cost $6m and $1m respectively, but it's the ethic, not the budget and scale I'm highlighting here. These were engaging, entertaining narratives which sold complex ideas[3]. We're in the same game; we just have to play it better, using the right people. If there is any gulf between traditional IO and popular media in terms of influencing and motivating, it's only really in terms of relative success.

The point of the above illustration is not to advocate that the IO community goes head to head with Hollywood. But it's not far off. We at least have to see ourselves as competing in the same marketplace for the same audience. That's the critical point.

The ultimate expression of the above model will be a commercial satellite channel which generates its own audiences from a mixture of popular programming - some produced, some bought-in. The schedule would include subtle IO, and the overall editorial agenda would broadly suit the client or clients' needs. It may need to be populist, even tabloid in character, but what it can't be is dull. This model would see deployment issues become an irrelevance, and might even generate revenues. Audacious? Maybe. Possible? We believe so.

The challenge for the IO industry in coming years will be to draw people into it with the right skill set to realise a radical but necessary evolution. Principally, these people need to be experienced television professionals, not PR people, not ad men. Clients need to work closely with people who understand television, understand the possibilities and the constraints and, moreover, understand how you translate an idea directly into a piece of compelling television. A TV format or an editorial agenda is, after all, little different to a campaign strategy. Working directly with TV people from the outset of a campaign better enables clients to plan, assess and realise their goals.

The broadcast TV world has another unique selling point as far as IO and, more importantly, IO budgets are concerned. In the last ten years, as advertising revenues fluctuated and the market fragmented, production companies have had to do more with less. Long gone is the boozy TV lunch and the over-populated production team. The industry has become lean, versatile and efficient. Many good directors are also excellent cameramen; many producers write; many offline television editors can create from very average rushes a gloss and an allure that competes with costly TVCs.

The gold-rush years for IO have undoubtedly passed, at least for the foreseeable future. However, this provides an opportunity for sober reflection and recalibration. Clients need to know that much can still be achieved. In my opinion, the skills, ethics and creativity of the television industry and its versatile professionals can serve the commissioners of IO well – and cost-effectively.

IO needs to be competing for its audience with the best broadcast television and online content. At the end of the day IO is just another media format vying for the eyes of the audience, and it needs to give itself the chance to compete. The industry needs the right people to engender a revolution.

[1] Reliable statistics from December 2009 record the following figures for a selection Iraqi channels deploying IO. With regard Mashriq and Diyar, 1% declared they'd watched the channels yesterday. For Babiliya and Salah a Din it was 3% and 4%, respectively. A further sobering point to note is that these figures only indicate people watching the channel, not the ENG. So viewership for these products was a proportion of 1%, 3% and 4%.

[2] It should be noted that many TV commercials (TVCs) got very good deployment in Iraq. The major state broadcaster, in common with leading regional and provincial channels deployed TVCs prominently, giving them excellent access to audiences. However, my view is that IO fatigue undoubtedly afflicted this genre of products in the same way that ENGs were blighted. However, given consumers' acknowledged resistance to advertising, I'd be interested to explore to what degree a highly conspicuous messaging vehicle such an expensive, glossy TVC is more influential than a cost-effective factual ENG, the narrative of which is led by ordinary, apparently impartial members of the public. If given the same deployment, might not an ENG perform as well for a client – if not for an ad agency's balance sheet?

[3] As a footnote, many will probably be musing, that monthly IO budgets in Iraq could well have accommodated some of the productions mentioned.

Table of Contents

Russian Professor Explains Media Manipulation

By Glenn Kates and Pavel Butorin, Radio Free Europe/Radio Liberty, 16 April 2014

Russian state media has been skewered in the West for its often outlandish coverage of events in Ukraine.

The "misinformation, exaggerations, conspiracy theories, overheated rhetoric and occasionally, outright lies," reverberate "hour after hour, day after day, week after week" on Russian TV, according to "The New York Times" on April 15.

But according to a poll, conducted in late March by the state-funded Public Opinion Foundation, some two-thirds of the Russian population trust government-controlled television more than any other medium.

A lecture by a history professor, apparently recorded in mid-April, sheds some light on Moscow's media strategy and why it seems to work.

"Television determines the agenda," says Valery Solovei, in his hourlong talk at the Moscow State Institute of International Relations (MGIMO). "The methods that I am talking about create a world view, something that's

called a 'reality.' A reality is created for us. If we see this reality the way it is brought to us by television, then we act in accordance with this reality."

Solovei says that in order to create a new reality for Kyiv, Ukraine must look absolutely untenable as a functioning state.

"You will recall the news reports in January when the really bloody events took place, the rapidly changing images of flames, burning tires, running people, alarming music," he says, referring to antigovernment protests in the Ukrainian capital. "What do you think it's for? For dramatic effect? No. There is a much bigger meaning behind it."

"Chaos is the key word," Solovei explains. "All of it is done to create a stable association in our minds: Ukraine is chaos. It is an old mythologem -- Chaos as a protoplasm from which the gods will then create the world. And what is Russia then? Russia is Cosmos, it is order, and it is the foundation of peace and stability."

"If you watch Russian TV you will see that Russia has no problems other than the adaptation of Crimea. We have no inflation, no decreasing incomes. We don't have any of the typical big-city problems. Russia has none of that. Everything is alright in Russia. What is it? It is called the manipulation of the agenda."

An RFE/RL journalist recently observed this prevailing blend of western chaos and Russian calm through a day of Russian TV watching.

At one point, a student, who seems to be offended by Solovei's speech, objects from the back of the room: "Have you seen what's happening there? They're completely out of control!"

"I beg your pardon," the professor responds. "But it absolutely does not matter how much the real picture corresponds with the media picture. An overwhelming majority of television viewers have never been and will never travel there. And they make their judgment based on the television picture and not on what happens in reality."

Table of Contents

Moscow Accuses Ukraine of Electronic Attack on Satellite

By Bill Gertz, Washington Free Beacon, March 17, 2014

Russia is accusing Ukraine of conducting an electronic attack on an orbiting communications satellite and is threatening unspecified retaliation as cyber warfare between the two states heats up over the crisis in Crimea.

Russia's Ministry of Communications and Mass Media revealed Saturday that an electronic attack against a Russian television satellite was traced to Ukraine.

"Appropriate services have detected the exact location of the source in Ukraine's territory," the ministry said, according to state-run ITAR-TASS news agency.

The Russian ministry said the attempt to use "radio-electronic war means against a Russian relay satellite" violated the 1992 International Telecommunication Union charter.

A second Russian state-controlled news agency, Interfax, reported that the Ukrainians attempted to "decay" the orbit of the communications satellite. No details were provided. Some communications satellites can maneuver based on ground signals and apparently the unidentified source of the electronic attack sought to command the satellite to lower its orbit in an attempt to have it reenter the atmosphere and burn up.

James Oberg, a specialist on space issues, said there have been reports in the past of satellites being pirated by non-government groups for political purposes.

"Taking over a satellite to fire its engine and alter its orbit is an entirely different challenge and I know of no examples, nor do I expect any," Oberg said in an email.

Oberg said one explanation for the Russian government statement about the satellite disruption is that it may have been an attempt by someone to fool the Russians into thinking the satellite's orbit had changed and thus create confusion and mistrust of the data it is relaying.

"But here, as in all effective tactics, the target is the enemy's decision loop, not his hardware," he said.

"The people behind this decision should consider the consequences," the Russian ministry warned Ukraine.

Disclosure of the satellite attack comes as both nations reported cyber attacks against government and non-government websites as the first phase of a new Cold War between Russia and Ukraine. The countries are currently embroiled in a conflict over Moscow's invasion of Ukraine's Crimea peninsula and Russia's announced annexation of Crimea following a controversial independence referendum.

Ukrainian government spokesmen and cyber security analysts reported that Ukrainian websites in recent days were subject of sophisticated cyber attacks using malicious software called Snake. The software appears to originate from a nation state, leading to suspicions that Russia was behind the attack.

Snake software gives users covert capabilities to conduct cyber espionage in foreign computers and also can be used to conduct sabotage ranging from disabling networks to destroying data and hardware.

NATO's Brussels headquarters reported experiencing a distributed denial of service attack on several public websites that was believed to be related to the Ukraine crisis. A NATO spokesman said the cyber attack did not disrupt operations of the military alliance. Distributed denial of service cyber attacks are sophisticated strikes that flood websites with requests using pirated computers that force systems to shut down.

Vice Adm. Mike Rogers, the nominee to be next commander of the U.S. Cyber Command, told Congress last week that Russia was conducting cyber attacks against Ukraine. "We clearly see that there's an ongoing cyber element to the challenges in the Ukraine at the moment," the three-star admiral told the Senate Armed Services Committee.

Rogers declined to provide specifics of the Russian cyber attacks but acknowledged that Moscow had developed very sophisticated cyber warfare capabilities and could inflict significant damage on Ukraine's critical infrastructures, such as government and military communications networks and telecommunications networks.

He warned that "clearly cyber will be an element of almost any crisis we're going to see in the future," Ukraine's government reported last week that several websites were affected by the cyber attacks, including the website of Ukraine's National Security and Defense Council that was shut down March 4.

Apparent retaliatory attacks were launched against Russia on Friday. Reports in state-run media described the attacks as "powerful" and affecting the operations of the presidential administration website and Russia's central bank.

A senior Air Force commander warned Congress last week of the growing threat to satellites from an array of attacks, including electronic jamming, cyber attacks, and anti-satellite missiles.

China demonstrated an anti-satellite missile in January 2007, destroying an orbiting weather satellite that left tens of thousands of pieces of debris floating in space.

Air Force Gen. William Shelton, commander of the Air Force Space Command, told a Senate hearing Wednesday that space warfare threats are increasing.

"Counterspace developments by potential adversaries are varied and include everything from jamming to kinetic kill anti-satellite weapons," Shelton said in prepared remarks.

Electronic jammers capable of disrupting Global Positioning Satellites used in navigation and precision guidance for weapons are "widely available" as are satellite communications jammers.

"Also, some nations have developed and successfully demonstrated anti-satellite weapon capabilities which could threaten our satellites in times of conflict," Shelton said in testimony to the Senate Armed Services strategic forces subcommittee. "Unfortunately, all projections indicate these threatening capabilities will become more robust and proliferated, and they will be operational on a shorter than predicted timeline."

Under questioning, Shelton said U.S. missiles and spacecraft are vulnerable to attack.

"Yes, sir. We are going system by system, looking at our cyber vulnerabilities. And we have a large information assurance program that gets into those vulnerabilities and patches them and tries to prevent access. In many cases, these are closed systems. That doesn't mean there aren't vulnerabilities, but they are closed systems, not accessible through the Internet. So it would take insiders, special access, those kinds of things, to get to these closed networks. But nevertheless, we're addressing all those touch points, if you will, in closing off those vulnerabilities best we can."

Shelton said in January that satellite jammers are 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."

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

Table of Contents

Can Military's Satellite Links Be Hacked?

By Mark Clayton, Christian Science Monitor, April 25, 2014

Satellite communication terminals, relied upon by US military aircraft, ships, and land vehicles to move in harmony with one another, are susceptible to cyber-attack through digital backdoors and other vulnerabilities, according to a new report that has sent a tremor through the global satellite telecommunications industry.

The report by IOActive, a Seattle-based cyber-security firm, arrives amid heightened concerns over a surge in cyber-attacks against satellite communications systems and vendors worldwide, industry experts say.

According to the IOActive report, a forensic security analysis of computer code buried inside the circuit boards and chips of the world's most widely used SATCOM terminals found multiple potential hacker entry points. Many terminals use small dishes or receivers that ride on the roof of a military vehicle, the bridge of a ship, or inside a troop transport aircraft, the report said.

Built by a half-dozen of the world's leading SATCOM equipment manufacturers, the SATCOM terminals cited in the report also serve nonmilitary uses, such as data collection from remote oil and gas pumping sites, pipelines, or retail chain stores. All involve sending data from far-flung operations up to large commercial satellite networks and back down again to their respective headquarters.

Industry officials, who generally acknowledged the proliferation of cyber-threats to the communications industry and were aware of the IOActive report, say SATCOM terminals are very secure when security features are turned on and used properly and are not insecure by design.

But what cyber-security researchers found when reverse-engineering the SATCOM terminals' firmware – the core computer code stored on the memory chips that primarily control the equipment – was a shocker, they said.

"IOActive found that malicious actors could abuse all of the devices within the scope of this study," wrote report author Ruben Santamarta, a principal consultant to the company. "These vulnerabilities have the potential to allow a malicious actor to intercept, manipulate, or block communications, and in some cases, to remotely take control of the physical device."

Vulnerabilities in the firmware include digital "backdoors" built into the computer code, as well as "hardcoded credentials," either of which could be used for unauthorized easy access to the devices, according to the report.

In addition, insecure communications protocols (languages) and relatively weak encryption on the system were other key problems, said the report, titled "A Wake-up Call for SATCOM Security."

In at least some cases, an adversary might need only send a text message that included malicious code – one of several options – to take control of the SATCOM terminal, the researchers said. A nation-state adversary or hacker could then fake the locations of aircraft, ships, and ground forces – as well as emergency messages.

"If one of these affected devices can be compromised, the entire SATCOM infrastructure could be at risk," the report says. "Ships, aircraft, military personnel, emergency services, media services, and industrial facilities (oil rigs, gas pipelines, water treatment plants, wind turbines, substations, etc.) could all be impacted by the vulnerabilities."

"The findings," Mr. Santamarta noted, "should serve as an initial wake-up call for both the vendors and users" of current SATCOM technology.

If the US military is concerned that SATCOM systems may be vulnerable to cyber-attack, it's hard to tell.

"The Department of Defense is aware of a multitude of growing threats in cyber-space, that anything connected to the Internet is potentially vulnerable," Lt. Col. Valerie D. Henderson, a Department of Defense spokeswoman, said Thursday in a statement responding to Monitor queries. "We manage all cyber-risks in accordance with one of DoD's primary cyber-space missions: Defense of all DoD information networks. We do not comment on specific operational vulnerabilities or the actions that we take to manage the associated risks, in order to preserve our operational security."

Other experts note that it's often easier to identify a vulnerability than to actually exploit it in the real world.

"No doubt it's a concern, but it's unlikely US aircraft will begin dropping out of the sky anytime soon," says John Bumgarner, research director for the US Cyber Consequences Unit, a cyber-security think tank.

"It's just not very easy to launch some of these attacks, even if you know the vulnerabilities involved," he says in an interview. "Yes, they can happen. But it requires tons of reconnaissance and planning to pull it off."

IOActive's trumpet blast, meanwhile, is hardly the first such warning.

In November 2011, the US-China Economic and Security Review Commission revealed that unknown hackers had infiltrated command links to Landsat-7, a US Geological Survey Earth-imaging satellite launched in 1999, and Terra AM-1, which carried NASA climate change sensors. Neither satellite was damaged, although hackers on June 20, 2008, “achieved all steps required to command” NASA’s Terra, “but did not issue commands,” the commission said.

Soon after, the President’s National Security Telecommunications Advisory Committee reported in 2009 on cyber-threats to satellite networks, noting that “satellite and terrestrial networks share similar cyber-vulnerabilities.”

The IOActive report focused on the world’s most widely used SATCOM terminals that connect with Inmarsat, a British satellite communications provider, and Iridium, a US-based provider.

Even though newer satellites and SATCOM terminals have more secure communications available today than when Landsat or Terra were launched, the soaring demand for satellite bandwidth means US government and military communications are increasingly using commercial satellite data pathways that are somewhat less well protected, satellite communications experts say.

Indeed, proprietary satellite communications have ceded ground in recent years to lower-cost, easier-to-use Internet Protocol or “IP-based” systems that have increased usability – but also the vulnerability of SATCOM systems overall, some experts say.

“Reducing the technical expertise required to connect to a satellite has the unintended consequence of making it easier for hackers to connect to a satellite,” writes Jason Fritz, an Australian cyber-expert at Bond University in Queensland, in an e-mail interview.

SATCOM “vendor brochures often advertise security and encryption,” he notes, “but in some cases it is up to the individual user to enable these features and follow proper procedures.”

Dr. Fritz’s view was confirmed by a satellite industry official who, speaking anonymously to protect his business ties, agrees that there are indeed cyber-security “gaps among some of the more casual users” of SATCOM links. While high-security settings are usually available on such equipment, it is frequently not used or default passwords are not changed – lapses that increase vulnerability to attacks.

“This equipment has been developed and designed to be so secure that if the features that are there in the systems are coherently implemented by the users, they are among the most secure systems in the world,” says the industry official. “The big gap is among more casual users who are not in the middle of a fire-fight.”

But that gap is appearing at the very time that cyber-attackers are intensifying their hunt for vulnerabilities to exploit, SATCOM security experts say.

“The line between SATCOM networks and IT networks have blurred substantially,” said Christopher Fountain, president of Kratos SecureInfo, a Chantilly, Va., cyber-security company. He told Milsat Magazine, a satellite industry trade publication, in July that increased use of Internet-based satellite communications protocols is “bringing additional cyber-security risks. This is against an environment where cyber-attacks and threats continue to increase.”

According to the Kratos SecureInfo website, “cyber-attacks are increasing at an exponential rate and satellite communications are a prime target.”

In response, the satellite industry is ramping up its public face and focus on cyber-threats. In February, the Global VSAT Forum (GVF), which represents the satellite communications industry worldwide, announced a new “cyber-security task force” to address the threat.

“We're working with industry to thwart indicators of cyber-attacks being made on the entire telecommunications sector," says David Hartshorn, GVF secretary general, in an interview. “Our new task force was scrambled to advance and enable best practices throughout the global satellite industry to address these threats.”

While maintaining that satellite systems have long been among the most secure communications systems available, “you can never say everything is just fine,” says Matthew Kenyon, senior director of North American operations for Hughes Network Systems, a provider of broadband satellite network products and a member of the GVF cyber-security task force. “Every community provider, satellite and terrestrial, is constantly working to improve their capabilities.”

Commercial satellite providers like Intelsat and Iridium are seeing a surge in demand due to increased US military activity in North Africa, the Asia-Pacific region, the Horn of Africa, and the Middle East, industry officials say. Satellite communications links are soaring for ISR missions – intelligence, surveillance, reconnaissance – as well as for unmanned aircraft system communications.

Intelsat General Corporation, a Bethesda, Md.-based subsidiary of Intelsat, which has about 50 satellites in its fleet, last year was providing satellite links for more than 60 unmanned aircraft missions and at least 40 manned ISR missions simultaneously, according to Mark Daniels, vice president of engineering and operations.

All that activity has drawn its share of cyber-attacks.

“In the cyber-security area, we have seen significant activity and we have had to take strong action to deal with that,” Mr. Daniels said in a March 2013 interview in Global Military Communications, a trade publication. Intelsat, the parent company, “deals with cyber-attacks on a daily basis.”

For its part, IOActive said it is working with a Department of Homeland Security-affiliated center to inform the SATCOM equipment makers. In a public warning in February, the center noted that “a remote unauthenticated attacker may be able to gain privileged access to the [SATCOM] device.... Additionally, a remote unauthenticated attacker may be able to execute arbitrary code on the device.”

IOActive provided not-yet-released details of the vulnerabilities it says it found in its study to satellite operators Iridium and Innarsat and to SATCOM companies that included Cobham, Hughes, Harris Corporation, Japan Radio Corporation, and Thuraya, a mobile satellite operator.

Monitor e-mails and phone calls requesting comment on the IOActive study elicited several responses from the companies.

“Iridium has been in contact” with the DHS-affiliated center “since they brought these concerns to our attention, and we have taken the necessary steps in the Iridium network to alleviate the issue,” Diane Hockenberry, an Iridium spokeswoman, says in an e-mailed statement. “We have determined that the risk to Iridium subscribers is minimal, but we are taking precautionary measures to safeguard our users.”

“Cobham is aware of the paper by IOActive and its findings,” Greg Alan Caires, a spokesman for the Britain-based company, says in an e-mail. “It is under review. We have no comment to make at this time.”

Hughes’s Mr. Kenyon declined to comment on the IOActive report.

Harris Corporation in Melbourne, Fla., and Japan Radio Corp. did not respond to requests for comment by press time.

Dubai-based Thuraya Telecommunications Company issued a statement that was dismissive of the findings.

“As Thuraya’s equipment was not tested in a real world environment, the results and the conclusions of the whitepaper are theoretical and not a proper assessment of the equipment’s security features,” the company said.

Inmarsat, whose underlying technology was present in several of the systems tested by IOActive, said it had “conducted a preliminary assessment” of the claims as they relate to devices operating over its network.

“We believe that the claims have previously been identified and addressed by Inmarsat and its partners,” Jonathan Sinnatt, an Inmarsat spokesman, writes in an e-mail to the Monitor. “Inmarsat is studying the full report in detail and should any new issues be identified, we will act promptly to address them,” he said.

Table of Contents

Secret Shin Bet Unit at the Front Lines of Israel's Cyber-War

By Tova Dvorin, Arutz Sheva, 4/25/2014

Several weeks ago, a vigilante by the name of "Buddhax" made waves when he exposed the true faces - and names and passwords - of several anti-Israel hackers who participated in the #OpIsrael project to launch a cyber-attack against Israel.

Now, nearly one month later, Channel 2 revealed Friday the existence of another party responsible for keeping Israel's cyberspace safe: a secret unit of the Israeli Security Agency (ISA), or Shin Bet.

Tens of hackers work in S-74, the codename for the Shin Bet unit which protects Israeli cyberspace. For days, they will cluster around their computers, tracking the suspicious movements of "Anonymous" hacktivists around the world. Then, just moments before a hack will disrupt a system, they will strike - without anyone even knowing the Shin Bet was involved.

"We have prepared well in advance, we follow networks around the world closely and collect intelligence through HUMINT and SIGINT [human intelligence and signals intelligence, respectively - ed.]," Alon, an S-74 member, revealed to the daily Friday.

Alon, 39, has been a member of the unit for eight years and is responsible for for teaching institutions who use critical servers how to prevent cyber-attacks. "We approached internet providers, conducted [a simulation

of] the attack with safeguards, and then analyzed the seriousness of the threat. We here in the Shin Bet then opened an operations room and our people ran through a number of simulations of the event before operating against [a cyber-attack] in real-time."

"Timing is critical," he continued. "Your opponent is sitting in advance to make sure a cyber-attack succeeds; all he has to do is press a button and the system begins to fail."

Timing was also crucial before #OpIsrael. Several weeks before, the Shin Bet opened an operations room to explore advanced, unique, and intensive solutions to prevent the lives of Israeli citizens from being disrupted. #OpIsrael had released a list of government sites, including websites in the security sector, and distributed a list of targets which included some 1,300 Israeli websites for its hackers to breach - including the sites for government agencies, banks, defense industries, academic institutions and media organizations.

Following that, S-74 raised the alert level. Employees met with mentors and the unit's best computer experts conducted a series of counter-terrorism simulations repeatedly until they could say, for certain, that "Anonymous" could not succeed.

"The unique thing about Anonymous is their motivation to act openly," Alon noted. "They put out a call to action and recruit thousands [of hackers] to help them [execute] a cyber-attack. The more participants there are, the greater likelihood that someone will force his way into a critical website and cause it to fail."

Research, research, research

Yuval, now 29, began working for the Shin Bet 12 years ago. He works in intelligence and is the co-founder of the SIGINT unit to gather intelligence ahead of a cyber-attack. He rarely speaks about the unit and its abilities to protect Israel.

"In the event of an 'Anonymous' attack, we need to know context about the world of our target," he revealed. "I study and research it, get a report on whether this is an organization or a real terror threat, and as I gather intelligence we begin to manage the process of preventing the future attack."

"This means combining the abilities of [cyber-attack units] SIGINT and HUMINT and attacking the opponent's 'home' - using information about the attacker or his environment to our advantage."

"The cyber-world constantly features glitches - incidents which could either be technical problems or a real cyber-attack," he continued. "It can be very difficult to tell how many people are hacking us at once."

Luckily, Yuval stated, there are ways of reducing the likelihood of a real attack.

"There are a lot of incidents that we can classify as an attack or disruption in the system, and we can test and analyze them to see if they're targeted specifically toward Israel," he said. "For example, Israel's biometric database can be a common target. In the meantime, we have secured the database, [. . .] [but] we do not know who is attempting to look at it."

Intelligence at Large

S-74 was established several years ago and has changed rapidly with the fast-paced changes in technological development, according to the report.

In addition to protecting Israel, the unit collects intelligence to launch its own attacks against Israel's enemies, according to Yuval.

"This is a classified area, normally, but we received special permission to give you a small glimpse into the world of intelligence," Yuval stated.

"In order to make critical decisions about Israel's security, we perform operations across the globe to hack into computers, databases, and networks - including personal computers," he explained. "We collect data from everywhere in every area."

"There are many institutions that work strategically against the State of Israel; we work quietly against them. Then, an intelligence officer will call me and ask me for that information and that can drastically change the character of an operation."

Branching Out

Another dimension is collecting intelligence before physical operations against terrorists. For example, S-74 was involved in collecting much of the relevant information to kill senior Hamas terrorist Hamza Abu Alheja last month in Jenin.

Yet another approach to cyber-intelligence includes education on cyber-safety.

"We have developed tools to identify anomalous networks, abnormal movements, and to isolate and contain them," Alon explained. He stated that he often presents CEOs of major institutions with information on real cyber-attacks to "scare" them into increasing their cyber-security.

"After Israeli entities are defined as being at risk, they should protect their critical systems immediately," he explained. "Cyber-attacks on certain institutions could cause serious damage."

"For example, Israel Railways transports tens of thousands of people per day," he explained. "The monitoring process thus begins right from the control room of the Israel Railways office. Vulnerable computer systems, if damaged, could 'black out' Israel's cell towers, its electricity, and other vital resources."

Changes Needed?

S-74's work may be extensive, but not everyone is impressed with Israel's cyber-security.

Dr. Michael Orlov, head of the cyber-engineering department of Shamoon College Engineering in Be'er Sheva, explained to Arutz Sheva earlier this month that Israel needs to step up its efforts to train more hackers to keep up with the attacks, which are becoming more and more organized.

As Orlov explained, the hacking projects against Israel by Anonymous - a loosely organized group of hackers worldwide, but for #OpIsrael mostly localized to Middle-Eastern Muslim countries - is a childish attempt to "feel important," and nothing more. Currently, cyber-attacks against Israel largely focus on replacing a site's content with propaganda, and leaving a site alone after it is fixed. This, he said, "is not a serious problem."

Future attacks may be, however. Orlov emphasizes that if a major country - e.g. Iran - were to set aside the "relatively small amount" of $50 million dollars to establish a professional hacking team, Israel could be in trouble.

"We have seen Iran do this in the past to other countries, like Saudi Arabia," Orlov stated, "Hackers attacked, broke into [websites] and deleted information. If this happens, we cannot dismiss the impact of attacks."

Table of Contents

New Bill Requires Voice of America to Toe U.S. Line

By John Hudson, Foreign Policy, APRIL 29, 2014

A powerful pair of lawmakers in the House of Representatives have agreed on major legislation to overhaul Voice of America and other government-funded broadcasting outlets that could have implications for the broadcaster's editorial independence, Foreign Policy has learned.

The new legislation tweaks the language of VOA's mission to explicitly outline the organization's role in supporting U.S. "public diplomacy" and the "policies" of the United States government, a move that would settle a long-running dispute within the federal government about whether VOA should function as a neutral news organization rather than a messaging tool of Washington.

"It is time for broad reforms; now more than ever, U.S. international broadcasts must be effective," said Rep. Ed Royce (R-CA), the chairman of the House Foreign Affairs Committee, in a statement.

The bill is the result of a year's worth of negotiations between Democrats and Republicans working hand-in-glove with their counterparts in the Senate Foreign Relations Committee. It has the support of the committee's most senior Democrat, New York Congressman Eliot Engel, and will get a vote on Wednesday in the committee. Corresponding bipartisan legislation is currently in the works in the Senate.

Besides clarifying VOA's mission, the bill reorganizes the federal agency responsible for supervising U.S.-funded media outlets, the Broadcasting Board of Governors. Instead of being led by a group of part-time board members, the bill establishes a full-time, day-to-day agency head. It also consolidates Radio Free Europe, Radio Free Asia and the Middle East Broadcasting Network -- other foreign-facing broadcast outlets -- into a single non-federal organization, and aims to save costs by downsizing the number of federal contractors at the outlets in the years to come.

Within VOA, the proposed reforms to its mission may prove the most controversial. Founded in 1942 as a part of the Office of War Information, the VOA was originally tasked with countering Japanese and Nazi propaganda. In the 1950s, it moved to the State Department and the U.S. Information Agency where it focused its efforts on countering Communist propaganda. In later years, VOA concentrated on providing news to individuals living under repressive regimes. In 1976, President Gerald Ford signed its principles into law, emphasizing VOA's mission as an "accurate, objective, and comprehensive" source of news, as opposed to a propaganda outlet.

For many years since then, employees at the TV and radio broadcaster have insisted on viewing themselves as objective journalists as opposed to instruments of American foreign policy. On some rare occasions, that sense of independence has resulted in news stories that depict the United States in a less than favorable light.

"The persian News Network of Voice of America has been documented to show anti-American bias," the conservative Heritage Foundation alleged in a policy brief this month.

Such instances have led congressional overseers to wonder why they're spending hundreds of millions of dollars on a news outlet without a more explicitly pro-American editorial focus.

"This legislation makes clear that the Voice of America mission is to support U.S. public diplomacy efforts," reads a summary of the new bill. "The VOA charter states that VOA will provide a 'clear and effective presentation of the policies of the United States ... Over time, VOA has abandoned this mission."

Lynne Weil, a spokesperson for the BBG, declined to weigh in on the proposal. "The agency does not comment on pending legislation," she said.

The timing of the bill comes as the crisis in Ukraine has prompted a renewed information war between Washington and Moscow. In recent weeks, the Kremlin has put its TV network RT into overdrive to castigate Western involvement in Ukraine and denounce the Kiev government as right-wing fascists. Meanwhile, Congress passed a bill last month providing more authority to VOA and RFE/RL to expand broadcasting into Ukraine and eastern Europe. The BBG's budget request for fiscal year 2015 is $721 million.

Table of Contents

Everything Old Is New Again

By M.S., the Economist, Apr 29th 2014

ONE of the key characters in Victor Pelevin's marvellous 2008 short story, "The Hall of the Singing Caryatids", is described as a "political technologist". The story concerns a bizarre scheme he has hatched to lure back to Russia an oligarch who owes his billions to the commercial exploitation of "military neuro-linguistic programming" techniques. Like much of Mr Pelevin's work, the story takes for granted that the reality we perceive is really a flimsy ideological hallucination cobbled together by various powerful actors interested in guiding our actions for reasons of their own. His work is more sophisticated than that of many latter-day Orwell imitators in that in his world different actors are simultaneously cobbling together incompatible hallucinations, and most of them are doing a hilariously inept job of it.

I thought of Mr Pelevin's "military neuro-linguistic programming" while reading Keith Darden's New York Times op-ed yesterday, "The War on Truth in Ukraine." Like many independent Russian commentators, Mr Darden focuses on the surreal quality of the information environment in Ukraine, including Russia's use of mysterious insignia-less "green men", its incitement of separatist uprisings (that look like a directed reality-TV version of Kiev's EuroMaidan), the (probably fake) threats against Jews, and other untraceable incidents of "provokatsiya". Mr Darden is careful to note that both pro-Russian and pro-Ukrainian actors are engaging in these information-manipulation efforts (though the Russians are obviously much better at it), forming at least two incompatible visions of reality in separate, polarised camps. "Doubt's shadow has not left Ukraine," he writes. "Instead, the failure to agree on facts—to share a basic reality—has become the norm."

> "The elusiveness of truth is a symptom and an accelerant of Ukraine's descent into uncertainty. Legitimate authority—governmental, factual, legal, moral—is unrelentingly being effaced...Thomas Hobbes wrote eloquently about life in the absence of political authority, but he couldn't foresee the modern fracturing of facts and narratives that accompanies its collapse. Today, as authority in all its forms is degraded, life becomes not only "nasty, brutish and short"; it becomes so riddled with disinformation and lies that there is no clear path to settlement. And the void in trust invites armed action."

At about the point where Mr Darden begins to speak of the "failure to agree on facts" and the degradation of "legitimate authority", one begins to wonder just how separate what is happening in Ukraine is from political trends in the rest of the world. To put things another way: to me, the techniques of propaganda and ideological manipulation Vladimir Putin's government is employing in Ukraine feel new, adept, and cutting-edge; they seem to tell us something about where the world is heading. But how different is the fragmentation of reality in Ukraine from the much-commented polarisation of reality in America? For that matter, is this really anything new, or is it just the latest version of the types of propaganda that political actors have always used to split or unify target populations?

On the first question, it's interesting to compare a recent study by the Pew Foundation's internet research project that mapped American Twitter conversation networks around different kinds of topics. The researchers observed six distinct patterns of networking that developed around different issues. For example, when breaking news stories are politically neutral, they may develop into "fractured communities" of people conversing with each other, each around their own favourite information source; or they may turn into a hub-and-spoke model, with many communities all disseminating retweets from a central major-media source. For political topics, however, the result is often what the researchers called a "polarised crowd" model.

> “If a topic is political, it is common to see two separate, polarized crowds take shape. They form two distinct discussion groups that mostly do not interact with each other. Frequently these are recognizably liberal or conservative groups. The participants within each separate group commonly mention very different collections of website URLs and use distinct hashtags and words. The split is clearly evident in many highly controversial discussions: people in clusters that we identified as liberal used URLs for mainstream news websites, while groups we identified as conservative used links to conservative news websites and commentary sources. At the center of each group are discussion leaders, prominent people who are widely replied to or mentioned in the discussion. In polarized discussions, each group links to a different set of influential people or organizations that can be found at the center of each conversation cluster.”

As examples of this model, the study uses a hashtag, #My2k, launched by the White House as part of the budget dispute with Republican leaders in the winter of 2012-13, as well as discussions around the sequestration that took effect when no budget-cut agreement was reached. Essentially, two entirely different groups of people discussed these events on Twitter, one liberal, one conservative. No inter-group discussion took place, and each group formed its own separate vision of reality. If liberals and conservatives are unable even to agree on the broad outlines of what has happened in America over the past six years, this is one of the reasons.

Political actors are well aware of these dynamics. When a political actor does something that generates political controversy along group lines (like pick a fight over the budget, or call for a secession referendum in Crimea), they are tripping a reaction they know will distil the population into two opposing clans. Either they expect to split the country and end up with the larger half (as Patrick Buchanan hoped the GOP would in 1972 if Democrats could be lured into nominating a black man for vice president), or they hope to rally enthusiasm among their core supporters. Some of the techniques the Putin regime has deployed in Ukraine are startling, including the use of unmarked troops, the deployment of seamlessly up-to-date government-controlled sensationalist mass media, shameless lying, and the seeding of what amounts to an AstroTurf colour revolution in the Donbass. But the Russians are essentially aiming at the same annihilation of reality through political polarisation that has been more or less achieved in America via the party system. Though it bears noting that in America the political debate is free, robust and uncensored, while in Russia the airwaves are controlled by a blood-stained despot.

The other question, though, is just how new any of this is. Two elements certainly feel relatively new: the colonisation of the mass media by partisan ideological players with their own TV networks (Fox News, RT), and the political deployment of the internet and social media. There was a time when people hoped that the latter would frustrate partisan efforts at polarisation, by forging peer-to-peer connections resistant to political manipulation. Those hopes have proved naive. Social media amplify polarisation, and effective politicians, including Mr Putin as well as American political actors on both sides of the aisle, have learned how to take advantage of this. But it is not entirely clear that what is happening here is any more than a technical update on the kinds of propaganda efforts that adventurous, polarising politicians have been employing since the early 20th century.

Which brings me back to Mr Pelevin's "military neuro-linguistic programming". I love that phrase in part because it's a typically savage Russian spoof of the craze for "neuro-linguistic programming" that swept through management circles in the late 1990s. I had a friend at the time who quit a job at a major bank in order to try to get gigs as a consultant plugging the stuff. I frankly have no idea what "neuro-linguistic programming" is, but I always had a feeling that it was more or less what we used to call "human social interaction". And, at some level, you could translate the phrase "military neuro-linguistic programming" as simply "the nation-state". The "war on truth" in Ukraine, and the similar war on truth in American politics, feel scarily, shinily new. But it may be the same old ideological warfare we've been waging since the birth of the modern state, kitted out with new gear.

Table of Contents