**Information Operations**

**Newsletter**



**Compiled by**: [**Mr. Jeff Harley**](mailto:Jeff.Harley@SMDC-CS.army.mil?subject=ARSTRAT%20IO%20Newsletter)

**US Army Space and Missile Defense Command**

**Army Forces Strategic Command**

**G39, Information Operations Division**

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

[Table of Contents](#_Table_of_Contents)

[ARSTRAT IO Newsletter on OSS.net](http://www.oss.net/IO)

[ARSTRAT IO Newsletter at Joint Training Integration Group for Information Operations (JTIG-IO) - Information Operations (IO) Training Portal](https://jko.harmonieweb.org/coi/InformationOps/news/default.aspx)

**Table of Contents**

Vol. 12, no. 01 (October 2011)

1. [Electronic Warfare Is More than Jamming IEDs](#_Electronic_Warfare_Is)
2. [Crowdsourcing Democracy through Social Media](#_Crowdsourcing_Democracy_through)
3. [Coast Guard Cyberdefense Office: Small but Mighty](#_Coast_Guard_Cyberdefense)
4. [U.S. cyberweapons had been considered to disrupt Gaddafi’s air defenses](#_U.S._cyberweapons_had)
5. [US Air Force Wins U.S. National Cybersecurity Innovation Award](#_US_Air_Force)
6. [The Next Generation Jammer Will Not Be Used For Cyber Warfare](#_The_Next_Generation)
7. [US General: Communications with Pakistan on cross-border operations inconsistent but improving](#_US_General:_Communications)
8. [Chinese Military Suspected in Hacker Attacks on U.S. Satellites](#_Chinese_Military_Suspected)
9. [Twitter war with the Taliban](#_Twitter_war_with)
10. [Internet Censorship Growth Hampers News, Study Says](#_Internet_Censorship_Growth)
11. [Creech Drone Virus Infection Accidental, STRATCOM Commander Says](#_Creech_Drone_Virus)
12. [Suspected US satellite hacking attacks: Reaction](#_Suspected_US_satellite)
13. [How Electronic Warfare Is Redefining the Battlefield](#_How_Electronic_Warfare)
14. [China Denies It Is Behind Hacking Of U.S. Satellites](#_China_Denies_It)
15. [Hacks make large-scale sabotage possible](#_Hacks_make_large-scale)
16. [Army Sees Cyber Threats As Imminent](#_Army_Sees_Cyber)
17. [Geospatial Information Authority targeted in cyber attack: Maeda](#_Geospatial_Information_Authority)
18. [Third Army conducts public affairs, military information support operations seminar for LAF](#_Third_Army_conducts)

Electronic Warfare Is More than Jamming IEDs

By Joe Gould, [Defense News](http://defensenews.com/blogs/ausa/2011/10/11/electronic-warfare-is-more-than-jamming-ieds/), October 11th, 2011

When it comes to electronic warfare, the Army’s longtime focus has been roadside bombs and jamming the signals that trigger them. But now the Army is readying to go on the attack.

Col. Jim Ekvall, chief of the Army’s Electronic Warfare Division, said the service is developing its Integrated Electronic Warfare System, a family of technologies that will include the ability to attack and disrupt the enemy’s command, control and communications capabilities.

The mainstay of Army electronic warfare has been an evolving series of vehicle-mounted, counter-IED systems meant to jam the signals of repurposed household gear -– from key fobs to cordless phones — used to detonate roadside bombs.

But the Army’s still-developing technology, whose first stages received pre-acquisitions approval in August, would be geared toward full-spectrum operations.

The systems are meant to jam anything from low-end cellphones and proximity-fused munitions to multimillion radar systems and aerial drone uplinks.

“It’s a family of systems that will operate in the full spectrum of conflict against a variety of targets, which far exceeds the $3 walkie-talkie,” Ekvall told Army Times.

The goal is to provide maneuver commanders with the ability to operate freely in the electromagnetic spectrum, while denying adversaries the use of it, whether that adversary is in Iraq and Afghanistan, or Iran and China.

“We will be victorious in our war against terrorism, and then another adversary will come along and he will not look like the enemy we’re fighting today, and he may be more inclined to a high-intensity conflict,” Ekvall said. “Electronic warfare has a place in high-intensity conflict, as it has in the past, and in the COIN environment.”

As part of IEWS, the Army is developing the offensive Multifunctional Electronic Warfare; the EW Planning & Management Tools meant to help prevent jammers from knocking out friendly communications and other sorts of signal fratricide; and IED-jamming capabilities geared toward countries outside of Iraq and Afghanistan, Army officials said.

In August, Army acquisitions executive Heidi Shyu approved “analysis of alternatives” studies for Multifunctional Electronic Warfare and EW Planning & Management Tools. The electronic warfare requirements community is looking at what technologies are already available.

The studies are expected to take six to nine months for the planning tool and a year for the offensive capability.

EW acquisitions officials released two requests for information in August to solicit the defense industry’s input on the two systems, and also hosted an industry day for contractors, academia and other government organizations at Aberdeen Proving Ground, Md.

Michael Ryan, the Army’s deputy project manager for electronic warfare, said companies have been spending money on electronic warfare research, and the Army needs to help guide that spending.

Given electronic warfare’s focus on counter-IED technologies, Ekvall said defense contractors often ask him whether the Army’s electronic warfare programs will survive the conclusion of hostilities in Afghanistan and Iraq. “Absolutely,” he says.

“There is fear out there that when we cease operations in Afghanistan and we’re no longer confronted by an IED threat that we’ll completely shelve the electronic warfare development and maturity,” Ekvall said. “I don’t believe there is a danger of that. I believe the senior leadership of the Army understands electronic warfare is more than just the defeat of IEDs.”

In 2009, the Army announced plans to establish an electronic warfare career field for officer, warrant officer and enlisted career fields. The Army has a requirement for 3,283 electronic warfare soldiers for the active component, Reserve and National Guard, of which 1,570 have been authorized. According to Army data, 384 active component soldiers have completed 29-series training.

The Multifunctional Electronic Warfare System is due to be fielded in stages. Increment 1, which is expected to be fielded in 2017, is primarily meant to jam enemy command, control and communications.

“With Increment 1, we’re really looking for where we can do some rapid turn and field some things in the next three to five years,” Ryan said.

The Army plans for these systems to be mounted on unmanned aerial vehicles, wheeled vehicles and on backpacks.

The EW Planning & Management Tools are software that would help the Army’s new cadre of electronic warfare experts deconflict offensive, defensive and friendly signals.

The software would essentially mesh intelligence and terrain data to provide a common operational picture for the electromagnetic spectrum. Electronic warfare officers would use it to perform pre-mission planning, identify likely threats, advise commanders and predict which devices would be most effective.

“Today, those [electronic warfare officers] have nothing,” Ryan said. “They’re smart guys and gals that give advice, but they don’t have this ability today, and when you start to field these more complex systems, they’re going to need these types of tools.”

Army officials predicted that as these technologies proliferate, they would be almost as invisible to soldiers on the battlefield as the electromagnetic spectrum itself.

Rod Mentzer, the Army’s program manager for electronic warfare, said as it would grant more soldiers the ability to “blacken the eyes and ears” of an enemy, but that its impact would largely be strategic.

“For the infantry soldier, I don’t think the change to him will be as noticeable,” Mentzer said.

Ekvall envisioned a future in which soldiers wear systems on their backpacks that automatically hone in on and jam enemy signals, whether to neutralize enemy communication or protect soldiers from IEDs and proximity-fused munitions.

“All you’ll know is you have it on your back,” he said.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Crowdsourcing Democracy through Social Media

From [Kurzweil](http://www.kurzweilai.net/crowdsourcing-democracy-through-social-media?utm_source=KurzweilAI+Weekly+Newsletter&utm_campaign=f6d10fa973-UA-946742-1&utm_medium=email), October 12, 2011

Social media can identify and help prevent dangerous situations from occurring during elections, says Georgia Tech Associate Professor Michael Best.

When nearly 40 million Nigerians took to the polls last April to elect a new president, Best provided technical support for a Nigerian group that wanted to use social media for tracking the election process and identifying any problems that cropped up.

Best and his team of researchers designed a social media aggregator tool that could pull content from about 20 different sources (including Twitter, Facebook, SMS messaging, blogs, and social-media websites) and analyze the data in real time using keywords.

At the peak of activity, the aggregator tracked about 50 reports per second and analyzed them based on keywords and location data. The Nigerian Social Media Tracking Centre (SMTC), formed just before the election by the organization Best was supporting, forwarded confirmable reports of election irregularities — and ultimately, reports of violence — to Nigerian authorities.

The aggregator collected about 750,000 reports containing pre-identified keywords. Following the election, the SMTC issued a summary report that listed recommendations for using social media and instant messaging to improve future election experiences, such as:

* Training civilian groups and voters to tweet election results
* Organizing SMS group accounts for both national and local election officials
* Establishing a central database to collate election results, and having local precincts send results via SMS
* Advising international monitoring organizations to partner with domestic groups that will monitor social media
* Using social media in real time to help improve the electoral process itself, acknowledging that civilian reports can provide critical information. If violence erupts, the hours or even minutes saved by having identified the situation through social media posts could make a significant difference in response.

Best and team want to produce open-source software to monitor major events to complement traditional monitoring techniques. For example, the National Democratic Institute and the European Union both sent observers to Nigeria for its April elections, and today Liberia will likewise see international teams on the ground, monitoring and reporting on the country’s electoral processes.

As reports begin to filter in, the aggregator will use posts clustering around certain keywords as evidence in a real-time catalog of “curated incidents.” If the team identifies a situation it decides should be reported to Liberian authorities, Best has partnered with iLab Liberia, an information technology support organization, which will staff a “response room” in the country.

In 2012, Best hopes to employ the aggregator in monitoring elections in Kenya, Senegal, and the new nation of South Sudan.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Coast Guard Cyberdefense Office: Small but Mighty

By Eric Beidel, [National Defense Magazine](http://www.nationaldefensemagazine.org/archive/2011/November/Pages/CoastGuardCyberdefenseOfficeSmallbutMighty.aspx), November 2011

Like the Army, Navy, Air Force and Marine Corps, the Coast Guard suffers thousands of attacks on its networks each month.

The Army has some 21,000 personnel devoted to network defense.

The Coast Guard: just 18.

Coast Guard Cyber Command, which is still in its infancy and awaiting a final stamp of approval, has aspirations to carry out a variety of missions. As a force that straddles the law enforcement and military realms, it is in a unique position, its leaders say.

“We’re smack dab in the middle of this,” says Coast Guard Lt. H. “Lars” McCarter, who is now assigned to a tactics branch at U.S. Cyber Command.

Officials say the threat to the Coast Guard is real. In late 2009, the service suffered the largest ever intrusion of its unclassified network. Dozens of systems were affected, some in geographically remote locations. There is a high probability that the attackers were able to exfiltrate sensitive information to foreign locations, though the initial source of the hack remains unknown, officials say.

But there are currently more Coast Guard personnel being funded by the Defense Department and assigned to U.S. Cyber Command in Fort Meade, Md., than there are back at the service’s own operation in Washington, D.C. McCarter is one of 20 from the small service currently focused on carrying out the Pentagon’s cyberspace mission. They will return to the Coast Guard when they finish their assignments, but there may or may not be space for them in network security roles.

The 18 personnel that currently make up Coast Guard Cyber Command come from a variety of information technology, operational and intelligence backgrounds and have a tall order ahead of them. In addition to defending their networks and protecting more than 45,000 workstations and users, they plan to use the Internet to keep tabs on drug runners and other criminals and keep critical infrastructure at the nation’s ports running safely. The service would like to beef up the command to carry out these missions, but potential budget cuts could put a damper on some of these efforts.

The Coast Guard already takes advantage of network security and intelligence training offered by other services and had to cut spending on other programs just to carve out the 18-person detachment. The chronically underfunded service is likely to have to trim some more in the current fiscal environment.

“I think what we find with cyber is that it’s more expensive to ignore it than to deal with it,” McCarter says. But as money dwindles, clear priorities must be established. “What is more important? The southern border or protecting domestic cyberspace? That is a very challenging question.”

The Coast Guard has begun looking internally for redundancies within its network security and across the board. The service recently found that it had 130 processes related to information assurance spread throughout its operations. Officials streamlined those and assigned them to appropriate entities. But as budgets get tighter, they will have to lean even more on agencies with abundant resources. Eventually, the service would like to imbed personnel with related outfits at the Department of Homeland Security and throughout the government.

On the high seas, Navy ships often carry Coast Guard detachments because the larger service can’t board vessels for law enforcement purposes. Officials are pondering what the equivalent of such actions would be in cyberspace. The smallest service’s title authorities place it at the crossroads of defense, homeland security and law enforcement missions. That versatility could prove crucial to a government that is still trying to figure out exactly how it should handle the spectrum of operations in cyberspace, officials say.

After all, there may be situations when U.S. Cyber Command just can’t pull the trigger on a law enforcement measure, but the Coast Guard can.

“That’s still being worked out right now,” says Commander Cliff Neve, chief of operations at Coast Guard Cyber Command. “We’ve not gone down that path, but I believe we will be going there.”

Coast Guard Cyber Command has its hands full with the missions it has already established. The most difficult and complex of them will require a level of cooperation between the federal government and private sector rarely achieved.

In addition to protecting its own networks, the Coast Guard is tasked with ensuring the safe travel of goods upon the nation’s waterways. This means working with commercial partners to assess and respond to threats to key infrastructure at ports around the country. These ports are becoming increasingly automated, providing new avenues for adversaries to break into them. All of the padlocks in the world can’t keep a hacker from gaining access to a computer system that controls a drawbridge, for instance.

“They could drop a bridge on a ship at the wrong time,” Neve says. “Anything that has a sensor — like an oil rig that has remote sensors — there’s a connection there and that connection could potentially be abused.”

A cyber-attack on a U.S. port could be devastating to the local operation and to the global economy. The Coast Guard must keep an eye on supervisory control and data acquisition (SCADA) systems, or the means by which industrial infrastructure and port facilities are connected to a network so they can be remotely operated. Hacking into these controls is a sure-fire way to wreak havoc, officials say.

“If you want to bring a port down, shut the electricity off or turn off the terminal operating system,” says John Holmes, a retired Coast Guard captain and executive deputy director of operations at the Port of Los Angeles. “If you shut down the terminal operating system, which tells them where every container is going, they are dead.”

It’s not “if” but “when” this type of attack will occur, he says during a recent maritime security conference.

“Something’s going to happen in a major port, and every port should know how to get their infrastructure running again.” This resiliency will require better communication between government and businesses, Holmes says.

“You don’t want a port to shut down because somebody closed a bridge and won’t let it open because it was connected to the Internet somehow,” McCarter says.

The Coast Guard already has ties to the commercial port industry and now must translate those relationships to the cyberspace domain to assess network vulnerabilities at U.S. ports.. The .mil and .gov networks are under constant attack, McCarter says, but it is harder to get a handle on the same kind of activity within commercial systems at the ports.

Companies often are reluctant to share information about intrusions for fear their reputations would be damaged. The Coast Guard is working on a way to increase reporting by allowing parties to announce intrusions while remaining anonymous.

“We know the threats are there,” McCarter says. “Whether or not threat actors have actually acted on it is a challenge, because somebody would have to tell us that it happened.”

Earlier this year, National Defense University, which is located near Coast Guard headquarters, issued a solicitation for an expert that could help the service’s Cyber Command establish a baseline for its maritime mission. The one-year position would involve studying a specific port for the purposes of identifying problems and ways to solve them. The contractor sought by NDU also was to help the Coast Guard understand all of its authorities and how they can be applied to cyberspace.

It appears that the service will have its hands full just defending its own network.

During a typical month, emails carry about 25,000 viruses into the Coast Guard network. And attacks on computer systems have been increasing wholesale. In November 2009, a little more than 150 Coast Guard workstations showed infections, according to data from the service. By February 2010, viruses had been planted on more than 1,000 computers. That same month saw an additional 20,000 or so attacks that the service’s response system handled automatically.

“One of the problems with cyber-attacks is that they happen in machine time. Once you’ve found out about it, it’s already occurred,” Neve says. “As a result, part of the defense system for intrusion prevention is to automate that process.”

But attacks are becoming automated too. Hackers will rent out botnets, or groups of compromised computers, by the hour for others to conduct denial of service attacks under a cloak of anonymity.

“It used to be that hackers were very specialized. There were very few people who could carry out a computer attack,” Neve says. “Now you can go find computer [software] online and leverage it with a couple clicks of the mouse.”

Even seemingly harmless hackers can cause disarray across the Coast Guard network. If the service has to take down a server to fix it, operations in the field could be affected.

“You have to make a pretty quick call on whether or not you’re going to pull the plug on it to stop the infection from spreading or keep it up and maintain operations,” Neve says. “You have a security person saying, ‘Take it down.’ Then you have an operator saying, ‘You can’t take it down. We’re running a search-and-rescue mission’ or ‘we’re running a counter-drug mission.’”

It is a delicate balance. The service used to rush to kick an intruder off the network, take the server down to fix it and then put it back up. Now, though, Coast Guard security professionals see the value in being more patient, Neve says. They may want to let someone troll around a bit to see if they can gather more information on the offender. They may even allow the hacker to get away with some data to see where it is being taken.

Sometimes, the Coast Guard will have to ask for help from the Defense Department, other times from the FBI or DHS. And the service will focus on strengthening those relationships while the whole of government waits for the laws of cyberspace to be defined.

“The Coast Guard is so small it’s imperative that we team very closely with other organizations,” Neve says. And with just 18 people in its Cyber Command, the service must find a way to borrow personnel and resources from larger organizations.

“Having those 20 people up at U.S. Cyber Command is a big deal, because those folks will come back to the Coast Guard with a tremendous knowledge base,” Neve says.

But not all of them will come back to Coast Guard Cyber Command. McCarter, whose assignment with the Defense Department ends in the summer, knows he probably won’t. He most likely will find himself back in a communications engineering role.

“There is just not going to be an available job at Coast Guard Cyber Command for me next summer,” he says. “That doesn’t mean I won’t go back there in a couple of years, but I don’t know.”

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

U.S. cyberweapons had been considered to disrupt Gaddafi’s air defenses

By Ellen Nakashima, [Washington Post](http://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html), October 17, 2011

Top Pentagon officials considered using their secretive arsenal of cyberweapons to disrupt Libya’s air defenses before deciding that bombs would be the better option for preparing the way for U.S.-led coalition airstrikes.

The debate, which officials said did not reach the White House, was aborted when it became clear that there was not enough time for a cyberattack to work. Libyan government forces, led by Moammar Gaddafi, were at the time close to overrunning Benghazi, a rebel stronghold where U.S. officials feared massacre might occur without fast intervention, said current and former officials who spoke on the condition of anonymity to describe sensitive policy discussions.

“We just ran out of time,” a former military official said. “It was overcome by events.”

That the cyberattack option was raised at all underscores the U.S. military’s growing capabilities in cyberwarfare and the appeal of such weapons as alternatives to conventional military options. But the debate also showed some of the practical limits on using computer code as a weapon.

U.S. officials have never publicly disclosed the cyberweapons at their disposal, though the military last year established the U.S. Cyber Command, based at Fort Meade, to coordinate the military use of cyberspace, including potential offensive operations.A cyberattack against Libya, said several current and former U.S. officials, could have disrupted Libya’s air defenses but not destroyed them. For that job, conventional weapons were faster, and more potent.

Had the debate gone forward, there also would have been the question of collateral damage. Damaging air defense systems might have, for example, required interrupting power sources, raising the prospect of the cyberweapon accidently infecting other systems reliant on electricity, such as those in hospitals.

There was also the possibility of any damage inflicted by a cyberweapon being temporary, allowing the Libyan government to potentially restore its air defenses quickly.

The debate over whether to mount a U.S. cyberattack on Libya was first reported by the New York Times on its Web site Monday.

“Cyber is just going to destroy or disable a component,” a former U.S. official said. “It’s not going to blow something up on the rails.”

A U.S.-led coalition, operating under United Nations authority, began strikes against Libyan air defenses and troop formations on March 19. The campaign, called Operation Odyssey Dawn, was carried out by the U.S. Africa Command and directed by a U.S. admiral aboard the USS Mount Whitney in the Mediterranean.

U.S. elements included sea-launched cruise missiles, B-2 stealth bombers, Harrier fighter planes and Growler jamming aircraft. France, Britain, Denmark and some other countries also participated. NATO took over command of the operation on March 31.

Had the debate proceeded and a cyberattack option been chosen, the task could have fallen to the U.S. Cyber Command or another military command.

The Obama administration avoided a confrontation with Congress over whether the airstrikes triggered the War Powers Act by ending its role in attacking Libyan ground forces in early April. The administration contended that ongoing U.S. strikes against Libyan air defenses did not constitute “hostilities” under the terms of the law.

The question of whether a cyberattack on Libya’s air defenses would trigger the War Powers Act was never discussed because the debate never advanced, the former official said.

In general, the U.S. government has been cautious in its deliberations over the use of cyberweapons, recognizing that using them can reveal capabilities and set precedents that might encourage other nations.

In this case, officials said, the main concern was time. In 2003, the George W. Bush administration considered dismantling Iraq’s financial system in a cyberattack before the U.S. invasion. The plan was blocked over concerns about collateral damage that might affect systems beyond the target, a former official said.

At the time, there was also an unwritten international taboo on targeting a banking system, which was seen as dangerous to global financial systems.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

US Air Force Wins U.S. National Cybersecurity Innovation Award

From [Defence Professionals](http://www.defpro.com/news/details/29118/?SID=d28f5451104d03a95a982196ed64574f), 24 October 2011

08:25 GMT, October 24, 2011 WASHINGTON | The SANS Institute announced today that the U.S. Air Force's 39th Information Operations Squadron (IOS) was selected as 2011 U.S. National Cybersecurity Innovation Award winner for its innovative use of a realistic cyber range woven into in the training of military personnel in cybersecurity.

Finding and developing cybersecurity talent is among the highest cyber priorities, as recognized by a long list of government officials and senior corporate executives, including Department of Homeland Security Secretary Janet Napolitano and U.S. Cyber Command Chief Gen. Keith Alexander. Sadly, most government agencies cannot find people with the right skills and experience. Too often, they are forced to bring in people who are able to theorize about security but who lack the practical, hands-on skills needed to protect critical systems.

The U.S. military is investing heavily to build cybersecurity training programs that can prepare the next generation of hands-on cyber defenders and cyber operators. The Air Force made a breakthrough when it moved its program away from the common overreliance on classroom training and instead deployed a cyber range where students can "fight in cyberspace" every day, testing and honing their new skills and improving their impact.

The 39th IOS cyber "Flight Simulator" and "Training Range" allow each student to conduct defensive cyber operations against real-time network attacks in controlled training scenarios. In the simulations, students use a graduated set of hands-on skills to find hidden flags, analyze security flaws, remotely access other computers within the network, analyze evidence to determine attacker activities, and defend their networks as they move to the next level of exercise.

This program adheres to a key tenet of effective development of Airmen: "fight like you train and train like you fight."

The US Air Force 39th Information Operations Squadron is awarded the 2011 National Cybersecurity Innovation Award in Developing World-Class Cyber Talent for setting a high standard that is already being noticed and copied by other organizations that need cybersecurity people with hands-on skills.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

The Next Generation Jammer Will Not Be Used For Cyber Warfare

15:46 GMT, October 26, 2011 The U.S. Navy is developing a much-needed airborne jamming system to replace its Vietnam-era jammers. It's called the Next Generation Jammer, and if all goes as planned then U.S. aviators will soon have an electronic warfare tool with greater power, precision and agility than any previous jammer. That's a good thing, because hostile emitters are proliferating like bunnies in the springtime.

However, one thing aviators will not be getting is a new tool for conducting cyber warfare against enemy information networks. Contrary to what trade-press stories keep reporting about the new jammer, it will not have the capability to insert viruses into enemy networks. There is no formal requirement for such a capability -- which is just as well, since it will be hard enough to meet the requirements that actually have been specified for more radiated power, greater spectral precision, and the like.

It's not that the Next Generation Jammer couldn't be used as a cyber weapon or shouldn't be used, but simply that it won't be. No requirement, hence no capability. Maybe someday the cyber warfare features will be added, but right now they would just complicate the task of developing a new jamming system. So forget all those gee-whiz stories about using the Next Generation Jammer to penetrate enemy nerve centers. It isn't going to happen anytime soon.

----

Loren B. Thompson, Ph.D.

Early Warning Blog, Lexington Institute

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

US General: Communications with Pakistan on cross-border operations inconsistent but improving

By Associated Press, Published: October 27

WASHINGTON — Cross-border radio communications with Pakistan’s military collapsed after the raid that killed Osama bin Laden in May and are still not consistent or up to what the U.S. would like to see, a top U.S. general said Thursday.

U.S. Army Lt. Gen. Curtis Scaparrotti, who directs day-to-day military operations in Afghanistan, said officials are trying to re-establish military communications along the border, particularly between Afghan and Pakistani units that are facing each other.

Offering a more detailed accounting of some of the cross-border problems with Islamabad that plagued U.S. and Afghan operations over the spring and summer, Scaparrotti said that Pakistan’s Frontier Corps forces at times looked the other way when nearby insurgents fired into Afghanistan.

Pakistani leaders were incensed when U.S. special operations forces crossed the border for the bin Laden raid, seeing it as a violation of their country’s sovereignty. Pakistan has also rebuffed increasing pressure from the U.S. to go after insurgents — particularly the Haqqani network — who operate in safe havens along the border and launch attacks into Afghanistan.

Describing the border friction, Scaparrotti said that there appeared to be either collaboration between the Frontier Corp troops and the insurgents, or at the very least they deliberately did nothing when insurgents fired rockets or mortars from locations in sight of their combat posts.

But he said there are now signs that things may be starting to improve.

“Since we began our discussions here lately, the Pakistanis have in fact returned fire on several of those points of origin that we’ve taken fire from now,” Scaparrotti said. “That’s a positive indicator here in the last month.”

Scaparrotti said when he was in Afghanistan a year ago he would routinely run coordinated operations, with the Afghans on one side of the border and the Pakistanis on the other.

“When I came in July, the communication was not, was not open, and there was a good deal of difficulty,” he told Pentagon reporters Thursday. “After the bin Laden raid, those routine communications just were not available in most cases. We had a difficult time arranging border flag meetings. We had a difficult time arranging communications back and forth.”

Citing a recent meeting with Pakistani officials, he said they are writing up new procedures that would lay out the daily communications expected of each side.

“Right now we’re having conversations, and I hope to see that that’ll move into action here in the near term,” he said.

Asked about the insurgents safe havens in Pakistan, Scaparrotti said they are one of the biggest threats to the U.S. campaign in Afghanistan. But, he said that even if the safe havens remain, he believes the U.S. can meet its objectives to pull combat troops out of Afghanistan by 2014 as long as the Afghans can build a strong, layered defense along the Pakistan border.

He said that would include bolstering the border posts with mobile units that can cover the gaps, and using the conventional police and Army forces to supplement them.

Asked about efforts to withdraw 10,000 U.S. troops by the end of the year and another 23,000 next September, Scaparrotti said about a third of those coming out this year will be combat troops, while the remainder will come from support forces at bases and headquarters units.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Chinese Military Suspected in Hacker Attacks on U.S. Satellites

By Tony Capaccio and Jeff Bliss, [Bloomberg Business Week](http://www.businessweek.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html), 27 Oct 2011

Oct. 27 (Bloomberg) -- Computer hackers, possibly from the Chinese military, interfered with two U.S. government satellites four times in 2007 and 2008 through a ground station in Norway, according to a congressional commission.

The intrusions on the satellites, used for earth climate and terrain observation, underscore the potential danger posed by hackers, according to excerpts from the final draft of the annual report by the U.S.-China Economic and Security Review Commission. The report is scheduled to be released next month.

“Such interference poses numerous potential threats, particularly if achieved against satellites with more sensitive functions,” according to the draft. “Access to a satellite‘s controls could allow an attacker to damage or destroy the satellite. An attacker could also deny or degrade as well as forge or otherwise manipulate the satellite’s transmission.”

A Landsat-7 earth observation satellite system experienced 12 or more minutes of interference in October 2007 and July 2008, according to the report.

Hackers interfered with a Terra AM-1 earth observation satellite twice, for two minutes in June 2008 and nine minutes in October that year, the draft says, citing a closed-door U.S. Air Force briefing.

The draft report doesn’t elaborate on the nature of the hackers’ interference with the satellites.

Chinese Military Writings

U.S. military and intelligence agencies use satellites to communicate, collect intelligence and conduct reconnaissance. The draft doesn’t accuse the Chinese government of conducting or sponsoring the four attacks. It says the breaches are consistent with Chinese military writings that advocate disabling an enemy’s space systems, and particularly “ground-based infrastructure, such as satellite control facilities.”

U.S. authorities for years have accused the Chinese government of orchestrating cyber attacks against adversaries and hacking into foreign computer networks to steal military and commercial secrets. Assigning definitive blame is difficult, the draft says, because the perpetrators obscure their involvement.

The commission’s 2009 report said that “individuals participating in ongoing penetrations of U.S. networks have Chinese language skills and have well established ties with the Chinese underground hacker community,” although it acknowledges that “these relationships do not prove any government affiliation.”

Chinese Denials

China this year “conducted and supported a range of malicious cyber activities,” this year’s draft reports. It says that evidence emerging this year tied the Chinese military to a decade-old cyber attack on a U.S.-based website of the Falun Gong spiritual group.

Chinese officials long have denied any role in computer attacks.

The commission has “been collecting unproved stories to serve its purpose of vilifying China’s international image over the years,” said Wang Baodong, a spokesman for the Chinese Embassy in Washington, in a statement. China “never does anything that endangers other countries’ security interests.”

The Chinese government is working with other countries to clamp down on cyber crime, Wang said.

Defense Department reports of malicious cyber activity, including incidents in which the Chinese weren’t the main suspect, rose to a high of 71,661 in 2009 from 3,651 in 2001, according to the draft. This year, attacks are expected to reach 55,110, compared with 55,812 in 2010.

Relying on the Internet

In the October 2008 incident with the Terra AM-1, which is managed by the National Aeronautics and Space Administration, “the responsible party achieved all steps required to command the satellite,” although the hackers never exercised that control, according to the draft.

The U.S. discovered the 2007 cyber attack on the Landsat-7, which is jointly managed by NASA and the U.S. Geological Survey, only after tracking the 2008 breach.

The Landsat-7 and Terra AM-1 satellites utilize the commercially operated Svalbard Satellite Station in Spitsbergen, Norway that “routinely relies on the Internet for data access and file transfers,” says the commission, quoting a NASA report.

The hackers may have used that Internet connection to get into the ground station’s information systems, according to the draft.

While the perpetrators of the satellite breaches aren’t known for sure, other evidence uncovered this year showed the Chinese government’s involvement in another cyber attack, according to the draft.

TV Report

A brief July segment on China Central Television 7, the government’s military and agricultural channel, indicated that China’s People’s Liberation Army engineered an attack on the Falun Gong website, the draft said.

The website, which was hosted on a University of Alabama at Birmingham computer network, was attacked in 2001 or earlier, the draft says.

The CCTV-7 segment said the People’s Liberation Army’s Electrical Engineering University wrote the software to carry out the attack against the Falun Gong website, according to the draft. The Falun Gong movement is banned by the Chinese government, which considers it a cult.

After initially posting the segment on its website, CCTV-7 removed the footage after media from other countries began to report the story, the congressional draft says.

Military Disruption

The Chinese military also has been focused on its U.S. counterpart, which it considers too reliant on computers. In a conflict, the Chinese would try to “compromise, disrupt, deny, degrade, deceive or destroy” U.S. space and computer systems, the draft says.

“This could critically disrupt the U.S. military’s ability to deploy and operate during a military contingency,” according to the draft.

Other cyber intrusions with possible Chinese involvement included the so-called Night Dragon attacks on energy and petrochemical companies and an effort to compromise the Gmail accounts of U.S. government officials, journalists and Chinese political activists, according to the draft.

Often the attacks are found to have come from Chinese Internet-protocol, or IP, addresses.

Businesses based in other countries and operating in China think that computer network intrusions are among the “most serious threats to their intellectual property,” the draft says.

The threat extends to companies not located in China. On March 22, U.S. Internet traffic was “improperly” redirected through a network controlled by Beijing-based China Telecom Corp. Ltd., the state-owned largest provider of broadband Internet connections in the country, the draft said.

In its draft of last year’s report, the commission highlighted China’s ability to direct Internet traffic and exploit “hijacked” data.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Twitter war with the Taliban

By Sr. National Security Producer Charley Keyes, [CNN](http://security.blogs.cnn.com/2011/10/26/4835/?hpt=wo_bn4), 26 Oct 2011

Bits of information - not just bullets and bombs - are in the thick of the fighting in Afghanistan.

U.S. forces feared they were losing the information war to the Taliban and now are fighting back with Twitter - using those brisk 140-character messages to get out the other side of the story.

"The Taliban were just constantly putting out false information and propaganda," said Lieutenant Colonel Jimmie Cummings. "Some of it was so wrong we finally had to start engaging, and backing up our information with the facts"

This new reliance on all social media is quick and cheap.

"It allows us to keep our followers dynamically informed while also keeping the enemy's statements in check," Cummings said in an e-mail exchange with CNN.

It is easy to see this play out on any day. A Twitter account that frequently puts out news reports favoring the Taliban, , trumpets information of a major battlefield success. "Mujahedeen bring down US helicopter in Kunar," says the tweet.

But over at International Security Assistance Force headquarters, the social media experts are on the case on the ISAF Twitter account. "We have no reports of any missing helos. Take any Taliban reports with a block of salt," their tweet answers. And later, "Reports of a shoot-down are false."

Cummings jokes that the Taliban keep up a steady stream of wildly inflated reports. "The usual is every day we lose 20 tanks and 30 people, if you follow the Taliban. We pick and choose what we come back with."

And the turning point came just last month, with the attack on the U.S. Embassy and NATO headquarters in Kabul.

"Our guys were telling us about what the Taliban was posting," Cummings recalls. In addition to false claims about U.S. fatalities, the Taliban-leaning sites called the Americans cowards and invaders. "It was so false. It dawned on us, we have to engage, to get the facts out."

Cummings says he and the other members of the public affairs team work in a big room together at the headquarters of the International Assistance Force. When one of the tweets comes in from the other side there is a group discussion on how to react and then the two military personnel who are totally dedicated to social media type a response and hit the send key.

"Being able to reach out and inform a younger generation is a key," Cummings said. "The younger generation here is one of the cornerstones to the future success of Afghanistan."

But some experts take a more skeptical view of the keypad duel between U.S. forces and their enemies.

Georgetown University's Martin Irvine says these "micro-community communications" can be hard to evaluate. "There is so much noise on Twitter, it is difficult to know if any of that information is going to get through," Irvine said from his Washington office. He is associate professor in Communications, Culture and Technology and wonders how many people in Afghanistan have cell phones or internet-enabled computers.

ISAF claims more than 14,000 followers on its Twitter account, including, of course, the Taliban, local journalists as well as regular people. And this hourly, if not minute by minute competition between U.S. forces and their enemies is just warming up, providing lessons now that can be brought to the next conflict.

"We believe so far we have been successful with our increased social media activities," Cummings said. "ISAF (NATO's International Security Assistance Force) will continue to grow and improve in this part of our communication realm."

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Internet Censorship Growth Hampers News, Study Says

By John Markoff, [New York Times](http://www.nytimes.com/2011/10/11/business/media/battling-internet-censorship-must-evolve-study-says.html?_r=2), October 11, 2011

A detailed study of Internet censorship in China and Iran shows that blocking techniques are changing rapidly and are becoming significant new obstacles for news organizations, governments and businesses.

The study, being published on Tuesday, focuses on Internet blocking faced by Iranian and Chinese visitors to BBC Web sites during periods of political unrest in the two countries over the last two years.

“This problem of Internet control is becoming an issue for more than human rights concerns,” said an author of the report, Ronald Deibert, the director of the Canada Center for Global Security Studies and the Citizen Lab, a University of Toronto organization that focuses on Internet security. “The fact is that you have dozens of countries not just filtering for porn, but political filtering and key events as well.”

The study, by the BBC and Dr. Deibert’s center, acknowledges that the Internet accounts for only about 13 percent of the broadcaster’s global audience, which totaled 225 million people in 2010-11. But it is increasingly important in authoritarian countries; for example, there are now 500 million Chinese Internet users, many times the number that listen to shortwave broadcasts.

The study documents the activities of firewall censorship during a variety of political events, including anniversaries of events like the Tiananmen Square protests.

The activities of censoring authorities are not easily predictable and can change rapidly, the authors say, adding that broadcasters must be ready to engage in a “cat and mouse” game with censors by constantly monitoring government firewall systems and by clever use of alternatives like Twitter and other social media.

Government censorship of broadcasters goes back at least to World War II, the report says. The Nazis enacted strict laws to prevent Germans from listening to foreign broadcasts, and radios were designed so they could not receive the broadcasts. During the cold war, the Soviets began an intensive radio-jamming campaign, and the United States responded with a “ring plan” — vast deployments of strategically placed shortwave transmitters meant to overwhelm the jammers.

The report, “Casting a Wider Net: Lessons Learned in Delivering BBC Content on the Censored Internet,” says the news media will need to form alliances to combat censorship efforts.

“Vietnam has been learning its blocking technology from China,” said the lead author, Karl Kathuria, the BBC’s senior operations manager. “One of our recommendations is that broadcasters get together as well.”

To help make its service available through firewalls, BBC has collaborated with Psiphon, a software firm that is a spinoff of the University of Toronto computer security researchers. The firm supplies circumvention software to BBC and the Voice of America as well as other organizations.

There are several ways to avoid firewall blocking systems. One of them, known as a Web proxy, routes requests for Web pages through an intermediate Internet address.

\*\*[Note: readers of the IO newsletter can download free copy of the report at <http://uoft.me/casting>.] \*\*

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Creech Drone Virus Infection Accidental, STRATCOM Commander Says

By Chris Carroll, [Stars and Stripes](http://www.stripes.com/blogs/stripes-central/stripes-central-1.8040/creech-drone-virus-infection-accidental-stratcom-commander-says-1.158091), October 18, 2011

WASHINGTON – A virus found to be infecting computers used to control U.S. drones flying in the Middle East “entered from the wild” and was not specifically targeted at the system, Gen. Robert Kehler, head of U.S. Strategic Command said Tuesday.

The virus hit computers at Creech Air Force Base in Nevada, as first reported Oct. 7 by Wired’s Danger Room blog. The Air Force initially refused to comment on the report based on unnamed sources, saying, “We generally do not discuss specific vulnerabilities, threats, or responses to our computer networks since that helps people looking to exploit or attack our systems to refine their approach.”

But heavy media coverage of the reported infection of computers that control drones– an iconic symbol of the war on terror – apparently caused Air Force officials to reconsider. On Oct. 13, they acknowledged a “credential stealer” virus had cropped up in the system.

Kehler said the virus had caused no operational problems, and only affected ground control computers, not those that control the drones in flight.

Kehler said investigators are still trying to determine how the system was infected.

The military must do better defending its computers so necessary capabilities aren’t lost, he said. “Perfect defense is probably not something we can achieve, but the idea of mission assurance is something we must achieve,” Kehler said.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Suspected US satellite hacking attacks: Reaction

From [BBC News](http://www.bbc.co.uk/news/business-15490687), 28 October 2011

Hackers interfered with two US satellites four times between 2007 and 2008, according to reports.

The claim is made in a draft paper prepared for the US-China Economic and Security Review Commission, according to the Bloomberg news agency.

It said the incidents involved the Landsat-7 and Terra AM-1 earth observation systems which were targeted through a ground station in Norway. The satellites are used to observe the earth's climate and terrain.

The report highlights the risks that would have been posed had the breaches involved satellites with "more sensitive functions".

The draft document notes that previous penetrations have involved individuals linked to the Chinese underground community. The Chinese government has repeatedly denied its role in computer attacks.

The BBC asked three security experts for their views:

Dr Markus Kuhn, University of Cambridge computer laboratory

If there really has been a serious security problem with these two satellites, I would argue that to be entirely due to negligence by its designers or operators.

It has long been basic computer-science textbook knowledge how to implement "cryptographic end-to-end message authentication", a very effective technique to prevent unauthorized parties executing commands on remote devices.

This story appears to be little more than someone gaining temporary access to some remote computer that steers a satellite dish.

These link stations merely forward messages to and from satellites, like a postal delivery service.

The security of the satellite does not have to rely on the security of any particular remote dish antenna.

A serious security risk to a satellite would be someone disrupting all communication with it by jamming its uplink frequencies.

But that is hardly practical for these polar orbiting satellites, which fly very low and are therefore visible from any point on Earth only for a few minutes at a time.

If such a satellite cannot talk to one link station, it must be prepared to use the next one on its path.

In a well-designed satellite system, it should not make much difference if one ground antenna is unavailable for a while, be it due to some teenage hacker or just heavy snowfall.

Prof John Walker, computing and informatics, Nottingham Trent University

The thing to remember about satellites is that they do not just support military operations, but they also provide the backbone infrastructure for commercial operations.

Sky TV and the global automotive industry are just two examples.

As with any infrastructure components, these systems are reliant on ground based computers to provide elements of command-and-control.

They send data and equipment where they need to be, and can tell them what to do.

This opens up an opportunity to circumvent security - depending on how it is being applied.

Recent news stories have reported that US unmanned drone military aircraft were infected with a virus that gathered information.

If a malicious code is able to infect such a sensitive project, it is highly possible there could be other attacks targeting the information on military satellites satellites via system-to-system conversations.

Amichai Shulman, chief technology officer at Imperva

I think that for years the basic information security assumption by military and government agencies was that they should keep their data on isolated networks that were not connected in any way to commercial and public communication infrastructure.

With this assumption and staff screening, they believed that the systems were safe.

However, in today's reality most military and government systems are interconnected and have substantial data links - some online and some offline - to public and commercial systems and networks.

Hence, once the "total isolation" assumption proved to be false, the traditional military security model collapsed in a magnificent way.

The latest, alleged, Landsat incident is a clear example of that. While the system is operated mainly from military facilities and systems, it can be accessed from a commercial station in Norway which in turn is connected to the internet.

The report hints that the attack on the control system was indeed related to this commercial control system.

This is yet another wake up call for these organisations to gradually abandon their older model and start deploying in-depth layered security into their information systems, much like the commercial organizations do.

We should remember though that making this change - both mentally and logistically - is a long process given the huge scope of these systems.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

How Electronic Warfare Is Redefining the Battlefield

By Ryan Dube, [TSW](http://www.topsecretwriters.com/2011/10/electronic-warfare-redefining-battlefield/), 31 Oct 2011

Today, more than ever before in the history of the world, electronics are fast playing a central role in military warefare.

In 2010, the Air Force constructed a $300 million research facility at Eglin Air Force Base, Florida called the United States Reprogramming Laboratory.

The ominous sounding laboratory is actually a facility intended to fine-tune the electronic warfare capabilities of the F-35 Joint Strike Fighter.

This is one example how one heavily just one branch of the military is investing in the field of electronic warfare. The Air Force defines the field as “the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.”

Applications of Electronic Warfare

That is a very broad description that actually encompasses a dizzying range of potential applications in military as well as intelligence.

While in years past the extent of electronic warfare encompassed little more than systems that would help a jet fighter evade incoming signals or jam targetting systems of ground forces, newer weapons are being built that are more of the offensive end of the spectrum.

The Army’s FM 3-36 Manual titled “Electronic Warfare in Operations” describes the need for control of the electromagnetic spectrum on the battlefield and explain how commanders need to accomplish that task:

“They do this by locating, targeting, exploiting, disrupting, degrading, deceiving, denying, or destroying the enemy’s electronic systems that support military operations or deny the spectrum’s use by friendly forces”

Examples provided in the manual of electronic warfare include:

–> Using directed EM or directed energy, or antiradiation weapons to proactively attack enemy locations to take out the enemy’s ability to utilize the electromagnetic spectrum at all.

–> Outfitting military communication equipment with defensive gear that can block a similar EM attack from the enemy.

–> EM Jamming, antiradiation missile, flares and decoys, and even an element of weaponry referred to as only “electromagnetic deception”.

Electromagnetic deception – an interesting term – is defined in the Army manual as manipulating electromagnetic energy in some way that will mislead the enemy or their EM weapons.

Some examples of this include providing misleading signals to the enemy, simulating “friendlies” or fake hostile forces, or transmitting EM signals that mimic the enemies own signals.

Other Uses of Electromagnetic Weapons

An impressive use of electromagnetic weaponry on the battlefield was described in a February 2011 report in Popular Science, where a new device developed by Felix Vega and Nicolas Mora – two doctoral students from Switzerland – was used to set off an IED from 65 feet away.

The device accomplished the task by rapidly sending electromagnetic pulses toward the device, and once hitting the same frequency as the remote device that the enemy uses to set off the bomb, the device explodes. This is a form of electronic warfare that can actually save the lives of countless soldiers.

On the flip side, you’ve got slightly more offensive weaponry that can completely disable enemy communications. One example is the U.S. Navy’s EA-18 Growler, which was used over Libya throughout the early part of 2011 to bombard Moammar Kadafi’s ground radar facilities with electromagnetic noise, making those weapons completely useless to the enemy.

Satellite Hacking by the Chinese

While the U.S. military takes great pride in its electronic warfare capabilities, there is the other side of the coin where nations like China seek to dismantal that electronic advantage through hacking and other countermeasures.

One example came on October 27th, when Business Week reported that Chinese computer hackers were suspected of interfering with U.S. government satellites from 2007 through 2008.

Oddly enough, the satellites in question were only observation satellites used for climate and terrain, however the fact that the Chinese established the ability to accomplish the task was very disturbing to most observers. If you can interfere with a satellite’s signals, then you could potentially disable that satellite as well.

Of course, China denies the charges and claims that the activities are simply a symptom of rampant cyber crime taking place throughout china, and the Chinese authorities promise U.S. officials that they will work harder to “clamp down on cyber crime.”

However, the entire episode is just one example of how high the stakes are these days when it comes to electronics, communications and the entire electromagnetic spectrum over the entire planet.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

China Denies It Is Behind Hacking Of U.S. Satellites

[Reuters](http://www.reuters.com/article/2011/10/31/us-china-us-hacking-idUSTRE79U1YI20111031), 31 Oct 2011

BEIJING (Reuters) - Beijing on Monday denied a U.S. commission's claim that China may have been responsible for hacking incidents on U.S. environment-monitoring satellites, saying that the committee had "ulterior motives" in writing such a draft report.

At least two U.S. environment-monitoring satellites were interfered with four or more times in 2007 and 2008 via a ground station in Norway, and China's military is a prime suspect, according to the draft report to Congress.

The U.S.-China Economic and Security Review Commission, which reported the interference, said the events had not actually been traced to China. It said it was citing them "because the techniques appear consistent with authoritative Chinese military writings" that have advocated disabling satellite control facilities in any conflict.

The committee "has always been viewing China with colored lenses," Foreign Ministry spokesman Hong Lei said at a regular news briefing on Monday. "This report is untrue and has ulterior motives. It's not worth a comment."

Hong reiterated China's stance that it "is also a victim of hacking attacks and will oppose any form of cyber crime, including hacking."

The cyberattacks add to the long list of tensions between the United States and China that span trade issues, human rights, the value of the yuan currency and Taiwan.

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Hacks make large-scale sabotage possible

By Jordan Robertson, [USA Today](http://www.usatoday.com/tech/news/story/2011-10-30/hacker-sabotage/50980234/1), 30 Oct 2011

SAN JOSE, Calif. – When a computer attack hobbled Iran's unfinished nuclear power plant last year, it was assumed to be a military-grade strike, the handiwork of elite hacking professionals with nation-state backing.

Yet for all its science fiction sophistication, key elements have now been replicated in laboratory settings by security experts with little time, money or specialized skill. It is an alarming development that shows how technical advances are eroding the barrier that has long prevented computer assaults from leaping from the digital to the physical world.

The techniques demonstrated in recent months highlight the danger to operators of power plants, water systems and other critical infrastructure around the world.

"Things that sounded extremely unlikely a few years ago are now coming along," said Scott Borg, director of the U.S. Cyber Consequences Unit, a nonprofit group that helps the U.S. government prepare for future attacks.

While the experiments have been performed in laboratory settings, and the findings presented at security conferences or in technical papers, the danger of another real-world attack such as the one on Iran is profound.

The team behind the so-called Stuxnet worm that was used to attack the Iranian nuclear facility may still be active. New malicious software with some of Stuxnet's original code and behavior has surfaced, suggesting ongoing reconnaissance against industrial control systems.

And attacks on critical infrastructure are increasing. The Idaho National Laboratory, home to secretive defense labs intended to protect the nation's power grids, water systems and other critical infrastructure, has responded to triple the number of computer attacks from clients this year over last, the U.S. Department of Homeland Security has revealed.

For years, ill-intentioned hackers have dreamed of plaguing the world's infrastructure with a brand of sabotage reserved for Hollywood. They've mused about wreaking havoc in industrial settings by burning out power plants, bursting oil and gas pipelines, or stalling manufacturing plants.

But a key roadblock has prevented them from causing widespread destruction: they've lacked a way to take remote control of the electronic "controller" boxes that serve as the nerve centers for heavy machinery.

The attack on Iran changed all that. Now, security experts — and presumably, malicious hackers — are racing to find weaknesses. They've found a slew of vulnerabilities.

Think of the new findings as the hacking equivalent of Moore's Law, the famous rule about computing power that it roughly doubles every couple of years. Just as better computer chips have accelerated the spread of PCs and consumer electronics over the past 40 years, new hacking techniques are making all kinds of critical infrastructure — even prisons — more vulnerable to attacks.

One thing all of the findings have in common is that mitigating the threat requires organizations to bridge a cultural divide that exists in many facilities. Among other things, separate teams responsible for computer and physical security need to start talking to each other and coordinate efforts.

Many of the threats at these facilities involve electronic equipment known as controllers. These devices take computer commands and send instructions to physical machinery, such as regulating how fast a conveyor belt moves.

They function as bridges between the computer and physical worlds. Computer hackers can exploit them to take over physical infrastructure. Stuxnet, for example, was designed to damage centrifuges in the nuclear plant being built in Iran by affecting how fast the controllers instructed the centrifuges to spin. Iran has blamed the U.S. and Israel for trying to sabotage what it says is a peaceful program.

Security researcher Dillon Beresford said it took him just two months and $20,000 in equipment to find more than a dozen vulnerabilities in the same type of electronic controllers used in Iran. The vulnerabilities, which included weak password protections, allowed him to take remote control of the devices and reprogram them.

"What all this is saying is you don't have to be a nation-state to do this stuff. That's very scary," said Joe Weiss, an industrial control system expert. "There's a perception barrier, and I think Dillon crashed that barrier."

One of the biggest makers of industrial controllers is Siemens AG, which made the controllers in question. The company said it has alerted customers, fixed some of the problems and is working closely with CERT, the cybersecurity arm of the U.S. Department of Homeland Security.

Siemens said the issue largely affects older models of controllers. Even with those, the company said, a hacker would have to bypass passwords and other security measures that operators should have in place. Siemens said it knows of no actual break-ins using the techniques identified by Beresford, who works in Austin, Texas, for NSS Labs Inc.

Yet because the devices are designed to last for decades, replacing or updating them isn't always easy. And the more research that comes out, the more likely attacks become.

One of the foremost Stuxnet experts, Ralph Langner, a security consultant in Hamburg, Germany, has come up with what he calls a "time bomb" of just four lines of programming code. He called it the most basic copycat attack that a Stuxnet-inspired prankster, criminal or terrorist could come up with.

"As low-level as these results may be, they will spread through the hacker community and will attract others who continue digging," Langer said in an e-mail.

The threat isn't limited to power plants. Even prisons and jails are vulnerable.

Another research team, based in Virginia, was allowed to inspect a correctional facility — it won't say which one — and found vulnerabilities that would allow it to open and close the facility's doors, suppress alarms and tamper with video surveillance feeds.

During a tour of the facility, the researchers noticed controllers like the ones in Iran. They used knowledge of the facility's network and that controller to demonstrate weaknesses.

They said it was crucial to isolate critical control systems from the Internet to prevent such attacks.

"People need to deem what's critical infrastructure in their facilities and who might come in contact with those," Teague Newman, one of the three behind the research.

Another example involves a Southern California power company that wanted to test the controllers used throughout its substations. It hired Mocana Corp., a San Francisco-based security firm, to do the evaluation.

Kurt Stammberger, a vice president at Mocana, told The Associated Press that his firm found multiple vulnerabilities that would allow a hacker to control any piece of equipment connected to the controllers.

"We've never looked at a device like this before, and we were able to find this in the first day," Stammberger said. "These were big, major problems, and problems frankly that have been known about for at least a year and a half, but the utility had no clue."

He wouldn't name the utility or the device maker. But he said it wasn't a Siemens device, which points to an industry-wide problem, not one limited to a single manufacturer.

Mocana is working with the device maker on a fix, Stammberger said. His firm presented its findings at the ICS Cyber Security Conference in September.

Even if a manufacturer fixes the problem in new devices, there's no easy way to fix it in older units, short of installing new equipment. Industrial facilities are loath to do that because of the costs of even temporarily shutting its operations.

"The situation is not at all as bad as it was five to six years ago, but there's much that remains to be done," said Ulf Lindqvist, an expert on industrial control systems with SRI International. "We need to be as innovative and organized on the good-guy side as the bad guys can be."[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Army Sees Cyber Threats As Imminent

By Rob McIlvaine, [Army News Service](http://www.army.mil/article/68283/Army_sees_cyber_threats_as_imminent/), October 28, 2011

WASHINGTON (Army News Service, Oct. 28, 2011) -- "I think the threat [of cyber-attacks] is very real and could potentially be very near-term," said Brig. Gen. John Davis, U.S. Cyber Command at Fort Meade, Md.

The nation, he said, will demand the military be engaged in cyber defense of the nation, because the military has the greatest capacity and capabilities to do so.

Davis said that today, it's not in the "authority lane" of the military to play that role. Instead, he said, the responsibility lies with the Department of Justice and the FBI, though he said the military is responsible for its own military networks.

"But 90 percent of the military networks reside and ride on commercial infrastructure, so we're concerned about what [an adversary's] cyber activity could do to that commercial infrastructure, because it can have an adverse impact on the military's ability to do its job," he said.

Davis and other think tank specialists came together at Unified Quest 2012, Oct. 25-28, for a series of annual seminars where members of academia, and U.S. and foreign militaries examine critical issues to current and future force development.

"This is the beginning of our campaign of learning for fiscal year 2012," Lt. Gen. Keith C. Walker, deputy commanding general, futures, and director of Army capabilities integration. "We're going to use what we learn in this session on alternative futures to set the conditions for further seminar war games and experiments."

Key takeaways from Unified Quest 2012 include:

-- As the world population grows, increased global competition for affordable finite resources, notably energy and rare earth materials, could fuel regional conflict

-- Water is the new oil, and its scarcity will confront regions at an accelerated pace in this decade

-- Super-empowered individuals will have the capacity for wide-spread influence and the ability to change local and state events

-- Tight monetary policy, infrastructure enhancements, and advanced technology investments will set conditions for economic recovery in 2020 to 2028

-- U.S. retrenchment, if it occurs, will be a transient state

-- The United States will retain relative supremacy, but by a smaller margin, requiring selective strategic choices

-- Land power is required for sustainable solutions, to pursue national interests, and to demonstrate resolve

-- Technological advancements through 2028 are expected to increase, and will impact all facets of life

-- Dynamic changes in the Islamic world will continue

"The purpose of this symposium is about plausible strategic landscapes," said Col. Kevin Felix, director of the Army's Future Warfare Division. "The four working groups were given wide latitude to work towards 2028, and it was about bringing in the right folks."

Following the intense work group sessions, one idea came out stronger than the others.

"We may be facing more asymmetric threats, in the cyber environment in particular," Felix said.

Those threats were of particular concern to not only Davis, but also to Richard Russell at Army Materiel Command.

"[In] the battlefield of the future, cyber will be the dominant factor," Russell said. "The ability to have the instrument in place to affect the cyber [capabilities] of the enemy at the critical moment, to affect how their systems operate and how they are able to affect the battle, will be the thing that changes the outcome of the battle."

"From both the total cyber challenge that the nation faces and in the protection of the data, the weapon systems designs and technologies that we and our partners are developing for future warfare, it is that cyber security element that will mean whether we will have success or failure, tactical or strategic surprise in the future," Russell said.

Before information technology became known as cyber, Davis said, the Army looked at that function as essentially an equipping function for the forces. The Army provided the Soldiers with the capability to communicate, but it was a supporting function.

"The Defense Department has recently transformed the way we look at this and has declared cyber an operational domain in its own right, a domain that every other traditional war fighting domain relies on ," Davis said, adding this puts war fighting domains at risk if it is undermined.

"What I'm trying to do is scare you even more than working group one did," Davis said. "I'm not looking at 2028. I'm looking at the next 18 months."

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Geospatial Information Authority targeted in cyber attack: Maeda

The [Mainichi Daily Times](http://mdn.mainichi.jp/mdnnews/news/20111028p2a00m0na015000c.html), 28 Oct 2011

The first meeting of a public-private committee on defending against cyber attacks convenes at the Ministry of Economy, Trade and Industry on Oct. 25. (Mainichi)The Geospatial Information Authority of Japan (GSI) has been targeted in a cyber attack, Minister of Land, Infrastructure, Transport and Tourism Takeshi Maeda told a news conference on Oct. 28 -- the latest in a series of attacks on Japanese computer systems.

Speaking in a news conference after a Cabinet meeting on Oct. 28, Maeda said, "I've heard that a server of the Geospatial Information Authority of Japan has also been attacked." Organization officials said that a server holding measurement data was attacked, and computer IDs and passwords were analyzed, enabling a party to gain access to the server.

Recent cyber attacks have targeted defense-related companies, the Foreign Ministry, and diplomatic establishments abroad, with hackers attempting to steal information by sending virus-laden emails. Viruses have been detected on the work computers of House of Representatives members and a lower house server.

GSI officials said the server that was illegally accessed was one used for very long baseline interferometry, in which radio waves from stars are picked up through several antennas, and the difference in arrival time is used to measure distances.

The attack was uncovered when a research organization and private company in Japan notified the GSI after being attacked through this server. Organization officials said the server did not contain personal information.

"The server that was illicitly accessed did not contain personal or confidential information, and so far there have been no leaks," a GSI representative said.

Maeda said measures were being taken to address the problem, stating: "We have to secure the safety of computer systems. The Ministry of Land, Infrastructure, Transport and Tourism in particular has a wide jurisdiction, with information falling under the category of important state secrets."

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)

Third Army conducts public affairs, military information support operations seminar for LAF

By Staff Sgt. Regina Machine, [13th Public Affairs Detachment](http://www.dvidshub.net/news/79248/third-army-conducts-public-affairs-military-information-support-operations-seminar-laf), 29 Oct 2011

BEIRUT, Lebanon – Third Army and the Lebanese armed forces Orientation Directorate conducted a five day seminar on public affairs and military information support operations here Oct. 24–28.

The seminar focused on public affairs and strategic communications techniques, psychological operations organization and doctrine, and media production. Through a combination of presentations, open discussions, and practical exercises, the U.S. Army Central team of subject matter experts ensured that all participants would be able to develop their own organizational models to be more effective with these principles in their military operations.

Many attendees were concerned about sending the right message and what happens if the intended end state was not accomplished. Lt. Col. Marcel Schneider, Third Army/ U.S. Army Central, military information support operations officer, recommended if that should happen they should look at adjusting their objectives. “The information environment changes more frequently than the enemy,” Schneider added.

Schneider also stated the tactic used should be one that can be easily reinforced through products, actions and messages.

Attendee Col. Imad Al-Hajj Chehade, a wing commander in the Lebanese air force, relished the opportunity to learn psychological operations techniques. “I didn’t know it was like this and now I want to know more,” Al-Hajj Chehade added. He also stated that the classes were eye opening.

Through seminars like this one the Third Army/U.S. Army Central and the LAF continues to build relationships while exchanging ideas in the different areas of public affairs, psychological operations, and media production.

With the high acceptance of the Lebanese military throughout the country, Maj. Rami El Ayoubi, Lebanese army officer, reiterated that the military has special considerations here and the people have freedom of speech. “All of the Lebanese media supports us and we know the people support us. We are the backbone of our country and no one comes near the army.”

[[Table of Contents](#_Table_of_Contents)](file:///D:\My%20Documents\Newsletter%2009-08\0908Information%20Operations.doc#_Table_of_Contents)