**Information Operations**

**Newsletter**

**Compiled by**: **Mr. Jeff Harley**

**US Army Space and Missile Defense Command**

**Army Forces Strategic Command**

**G39, Information Operations Division**

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

[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. 02 (November 2011)

1. [The First Rule of Twitter Fight Club: Everyone Re-tweets Twitter Fight Club](#_The_First_Rule)
2. [Stuxnet Raises 'Blowback' Risk in Cyberwar](#_Stuxnet_Raises_'Blowback')
3. [Assassination Backlash](#_Assassination_Backlash)
4. [China's Cyber-Warfare Capabilities Are 'Fairly Rudimentary'](#_China's_Cyber-Warfare_Capabilities)
5. [No Other Nation Has Anything Like It](#_No_Other_Nation)
6. [Feds Cite Chinese Cyber Army Capability](#_Feds_Cite_Chinese)
7. [China scorns U.S. cyber espionage charges](#_China_scorns_U.S.)
8. [Fighting in the Fifth Dimension](#_Fighting_in_the)
9. [NATO Turns To Radio to Try and Get Its Own Message to Afghan People](#_NATO_Turns_To)
10. [DRDO Developing a Futuristic E-Bomb](#_DRDO_Developing_a)
11. [CIA following Twitter, Facebook](#_CIA_following_Twitter,)
12. [Speculation Continues Over Hezbollah’s Ability To Disable Israeli Drones](#_Speculation_Continues_Over)
13. [Beijing’s electronic Pearl Harbor](#_Beijing’s_electronic_Pearl)
14. [Cyberwar Most Likely to Take Place Among Smaller Powers, Experts Say](#_Cyberwar_Most_Likely)
15. [Canada puts up $477 million to foil cyber attacks](#_Canada_puts_up)
16. [Turkey Centralizes Efforts for National Cyber Security](#_Turkey_Centralizes_Efforts)
17. [Cyber Terror](#_Cyber_Terror)
18. [First Look: Electronic Warfare Missile](#_First_Look:_Electronic)
19. [U.S. Works to Counter Electronic Spy Risks](#_U.S._Works_to)

The First Rule of Twitter Fight Club: Everyone Re-tweets Twitter Fight Club

By Daniel W. Drezner, [Foreign Policy](http://drezner.foreignpolicy.com/posts/2011/09/15/the_first_rule_of_twitter_fight_club_everyone_re_tweets_twitter_fight_club), September 15, 2011

In honor of its 5th anniversary, let's take a look at the following Twitter exchange between spokesmen for the Taliban and ISAF, as captured by The Guardian's Haroon Siddique:

As the 20-hour assault by Taliban insurgents on Kabul's diplomatic and military enclave drew to a close on Wednesday, insurgents and coalition forces decided to prolong the battle the modern way: on Twitter.

If the continued insurgency in Afghanistan represents a failure of dialogue, the spat between the Taliban and the press office of the international security assistance force (ISAF) on Wednesday proved that they are ready to exchange words directly, even if their comments offered little hope of peace being forged anytime soon.

The argument began when @ISAFmedia, which generally provides dry updates in military speak of the security situation in Afghanistan, took exception to comments from a Taliban spokesman, tweeting: "Re: Taliban spox on #Kabul attack: the outcome is inevitable. Question is how much longer will terrorist put innocent Afghans in harm's way?"

The Taliban - who, when in power, eschewed most modern technology, including television and music players - decided to point the finger of blame back at the international forces for endangering Afghan civilians. Showing an affinity with textspeak, Taliban tweeter Abdulqahar Balk (@ABalkhi) wrote: "@ISAFmedia i dnt knw.u hve bn pttng thm n 'harm's way' fr da pst 10 yrs.Razd whole vllgs n mrkts.n stil hv da nrve to tlk bout 'harm's way'"

@ISAFmedia was moved to respond by providing statistical backing for its case. "Really, @abalkhi? Unama reported 80% of civilians causalities are caused by insurgent (your) activities http://goo.gl/FylwU"

But @ABalkhi questioned the value of the quoted statistics, pointing out in somewhat sarcastic tones that ISAF, an organisation established by the UN security council, was using figures from another UN body (the UN assistance mission in Afghanistan) to try to win the argument: "@ISAFmedia Unama is an entity of whom? mine or yours?"

Naturally, this led to many Twitter responses. Counterterrorism expert Daveed Gartenstein-Ross got off the best quip: "And then... ISAF and the Taliban unfollowed each other."

OK, seriously, what is the takeaway from this sort of exchange? Is this kind of interaction a uniquely 21st century form of statecraft, or just old wine in new, snarker bottles?

It's very tempting to roll one's eyes and say that we've seen this sort of thing before. CNAS' Andrew Exum argues that this exchange is similar to the "cross-trench trash-talking" of the Spanish Civil War. Which would be true... if the majority of the rest of the world had the option of witnessing the trash-talking in real time.

No, this is something different, something that I suspect is activating Anne-Marie Slaughter's sixth sense of detecting "modern social-liberal" trends. And as more and more international affairs heavyweights go on Twitter, it might be a harbinger of a whole new arena of the world politics sandbox.

What I'm not sure is whether this kind of Twitter exchange is terrifically meaningful. As the Guardian story observes, it came about in response to real-world events in Kabul, so in some ways the Twitter engagement between public spokespeople is simply an extension of traditional global public relations. PR has been a part of world politics since the days of E.H. Carr, so I'm not sure this is really all that new and different.

That said, I'll close with two questions for which I do not have easy answers. The first is whether this kind of engagement on Twitter is a legitimating act or not. Does ISAF, by engaging the Taliban on Twitter, elevate the latter group somehow in the global public sphere? This was an argument that the Bush administration used to make for why it would not negotiate with Iran or North Korea. The Bushies posited that the very act of sitting down to talk with these odious regimes conferred legitimacy on them that they otherwise would not have earned. That was a somewhat dubious proposition when dealing with governments of sovereign states. What about non-state actors, however? What about cranks on Twitter? I'm not sure.

The second question is.... is it even possible to win at Twitter fight club? In an exchange with Exum, former debate champion Gartenstein-Ross made an trenchant point about online debate:

[I]t's generally hard to win a name-calling contest. If I call someone an America-hating pinko, they can fire back that I'm a right-wing tool of the military industrial complex. Those two insults seem essentially to cancel each other out: why give someone an area that can end up a draw if I believe that I can prove all of my other arguments to be correct? Second, I find that if I'm civil, I can actually (sometimes) persuade people I'm arguing against that they're wrong about an issue. In contrast, if I begin a debate by insulting someone, it only further entrenches him in his initial position, thus making it more difficult to talk sense into him.

Twitter tends to bring out the snark in me, and I suspect I'm not the only one, so I wonder if, in the end, Twitter exchanges in world politics will all wind up as stalemates (unless either Dave Weigel or Keith Law take an interest in international relations). That said, the ISAF/Taliban exchange did seem pretty civil by Twitter standards -- so maybe PR professionals will live up to Gartenstein-Ross' standards.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Stuxnet Raises 'Blowback' Risk in Cyberwar

By Tom Gjelten, [NPR](http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar), November 2, 2011

The Stuxnet computer worm, arguably the first and only cybersuperweapon ever deployed, continues to rattle security experts around the world, one year after its existence was made public.

Apparently meant to damage centrifuges at a uranium enrichment facility in Iran, Stuxnet now illustrates the potential complexities and dangers of cyberwar.

Secretly launched in 2009 and uncovered in 2010, it was designed to destroy its target much as a bomb would. Based on the cyberworm's sophistication, the expert consensus is that some government created it.

"Nothing like this had occurred before," says Joseph Weiss, an expert on the industrial control systems widely used in power plants, refineries and nuclear facilities like the one in Iran. "Stuxnet was the first case where there was a nation-state activity to physically destroy infrastructure [via a cyberattack]."

Reactions to the use of Stuxnet in Iran generally fall into two categories. For those focused on the danger of Iran developing a nuclear weapon, Stuxnet was something to celebrate, because it set back Iran's nuclear program, perhaps by years.

But for people who worry about the security of critical U.S. facilities, Stuxnet represented a nightmare: a dangerous computer worm that in some modified form could be used to attack an electric or telecommunications grid, an oil refinery or a water treatment facility in the United States.

Cybersecurity analysts look at a diagram that shows their computer network, which is coming under attack, during a mock exercise at the Idaho National Laboratory in September.

"It's just a matter of time," says Michael Assante, formerly the chief security officer for the North American Electric Reliability Corporation. "Stuxnet taught the world what's possible, and honestly it's a blueprint."

Further complicating the Stuxnet story is the widely held suspicion that the U.S. government, possibly in partnership with Israel, had a hand in the creation of this lethal cyberweapon, notwithstanding the likelihood that in some form it could now pose a threat to the U.S. homeland.

**Training To Face A Catastrophe**

The prospect of a cyberattack on U.S. infrastructure assets has prompted the Department of Homeland Security to arrange a new training program for the people who are supposed to protect the electric grid, manufacturing plants, refineries, water treatment centers and other critical facilities.

The top concern is the industrial control systems (ICS) that oversee the operation of key equipment at those facilities, from the valves to the breaker switches.

By hacking into the computer networks behind the industrial control systems, an adversary could reprogram an ICS so that it commands the equipment to operate at unsafe speeds or the valves to open when they should remain closed. This is roughly the way Stuxnet was able to damage the centrifuges in Iran.

Participants in the training program, based at the Idaho National Laboratory in Idaho Falls, are taken step by step through a simulated cyber-intrusion, so they can experience firsthand how a Stuxnet-like attack on their facilities might unfold.

During an Idaho National Laboratory exercise that was staged for visiting reporters in late September, instructor Mark Fabro installs his "red" team on the second floor of the training center, with the mission of penetrating the computer network of an unsuspecting industrial company, set up on the floor below.

The trainees on the "blue" team downstairs sit in a mock control room, monitoring their computer screens for any sign of trouble.

At first, everything appears normal. The attackers have managed to take control of the computer network without the defenders even realizing it. But gradually, problems develop in the control room.

"It's running really slow," says one operator. "My network is down."

Sitting at their monitors upstairs, the attacking team is preparing to direct the computer system to issue commands to the industrial equipment.

"Take this one out," says Fabro, pointing to a configuration that identifies the power supply to the control room. "Trip it. It should be dark very soon."

Within 30 seconds, the mock control room downstairs is dark.

"This is not good," says Jeff Hahn, a cybersecurity trainer who this day is playing the role of the CEO of the industrial company under attack. The blue team is under his direction.

"Our screens are black and the lights are out. We're flying blind," Hahn says.

During the exercise, the critical industrial facility under attack is a pumping station, such as might be found in a chemical plant or water treatment center. As the operators sit helpless at their terminals, the pumps suddenly start running, commanded by some unseen hand. Before long, water is gushing into a catch basin.

Marty Edwards, director of the DHS Industrial Control Systems Cyber Emergency Response Team (shown here at the Idaho National Laboratory in September) says the U.S. government's cybersecurity lab had no role in the development of Stuxnet.

"There's nothing we can do," one of the operators tells the CEO. "We can only sit here and watch it happen."

If this mock facility were an actual chemical plant, hazardous liquids could be spilling. If it were an electric utility, the turbines could be spinning out of control.

If it were a refinery, the tanks could be bursting or pipelines could be blowing up, all because the cyberattackers have been able to take over the computer network that controls the key operations.

The cyberattack scenario is all the more worrisome, because it is not clear that such attacks can be effectively stopped.

"Some of these [systems] can't be protected," says Weiss, the industrial control systems security expert. "We're going to have to figure out how to recover from events that we simply can't protect these systems from."

**A U.S. Role In Stuxnet?**

The challenge of managing a Stuxnet-like attack is compounded by the possibility that the U.S. government itself had a role in creating the cyberweapon.

U.S. officials were certainly aware of the ICS vulnerabilities that the Stuxnet worm ultimately exploited. An Idaho National Laboratory experiment in 2007, dubbed "Project Aurora," first demonstrated how cybercommands alone could destroy industrial equipment. Idaho lab researchers, who at the time included Michael Assante, rewrote the ICS computer code for the generator, directing the generator to destroy itself.

"When we started to conduct the test, that really robust machine couldn't take it," Assante recalls. "The coupling broke ... and you saw black smoke belching out of it."

In 2008, Idaho National Laboratory researchers performed a demonstration expanding on the Aurora experiment and their further analysis of ICS vulnerabilities. The PowerPoint briefing was prepared specifically for Siemens, the company whose equipment the Stuxnet attack targeted. One year later, the worm was introduced into Siemens ICS equipment used at a uranium enrichment facility in Natanz, Iran.

Ralph Langner, a German cybersecurity researcher who was among the first to analyze the Stuxnet code, came away convinced that it was a U.S. creation.

"To us, it was pretty clear that the development of this particular malware required resources that we only see in the United States," Langner says.

Marty Edwards, director of the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, based at the Idaho lab, denies any Idaho National Laboratory role in the creation of Stuxnet, and says the ICS traits the worm exploited were relatively well-known by the time it was created.

"I think it was only a matter of time before those common weaknesses or vulnerabilities were leveraged in an event such as Stuxnet," Edwards says. He would not comment on any role that other U.S. government agencies might have played in the development of the Stuxnet weapon.

That the United States has an offensive capability in the cyberwar domain is a matter of official record. Activities in that area are highly classified, but officials privately acknowledge that U.S. agencies have developed cyberweapons for offensive use.

The Stuxnet computer worm reportedly affected several laptops belonging to employees of the Bushehr nuclear power plant (shown here in a photo from August 2010 and released by the International Iran Photo Agency) in Iran, as well as centrifuges at Natanz, the country's most important uranium enrichment facility.

It has also been reported that the United States has engaged previously in the sabotage of Iranian nuclear facilities. The use of Stuxnet would fit squarely within such a category.

Joel Brenner, the former inspector general at the National Security Agency, writes in his new book, *America the Vulnerable*, that the use of Stuxnet "would ... have been consistent with U.S. policy but not with previous U.S. methods, which avoided computer operations likely to damage others besides its intended targets."

Some observers have argued that the risk of a weapon like Stuxnet being turned against U.S. assets was so great that no U.S. government agency could logically have supported its development. But others aren't so sure.

Among them is Assante, who was among the first cybersecurity experts to warn that Stuxnet could provide a blueprint for attacks on U.S. infrastructure.

Now the president of the National Board of Information Security Examiners, Assante argues that concerns about Iran developing a nuclear weapon could have justified Stuxnet's creation.

"That is probably one of the largest national security challenges I can envision," Assante said in a recent meeting with reporters at the Idaho lab. "In that context, you can make a pretty strong argument that the benefit of using a cyberweapon to slow down or delay [a nuclear weapon program] or to achieve a specific objective might absolutely outweigh the risk."

**Questions Of Information-Sharing**

Given the secrecy around the U.S. offensive cyberwar capability, however, that cost-benefit analysis could only be carried out at the highest levels of the U.S. government. Moreover, it is unclear whether agencies responsible for defending the U.S. infrastructure would even be part of the deliberation.

"[The development of a cyberweapon] would probably be so highly classified that the people at DHS wouldn't even know about it," says one former intelligence official.

Such a strict compartmentalization of policymaking would raise the question of whether there is sufficient communication between the offensive and defensive teams in the cyberwar domain.

If Stuxnet was developed by U.S. cyberweapon specialists, the DHS personnel who spent a year analyzing the computer code were presumably engaged in a major duplication of effort.

But Greg Schaffer, assistant secretary of homeland security for cybersecurity and communications, says DHS officials have no complaint over coordination with U.S. agencies responsible for offensive cyber-activities.

"DHS is focused on network defense," Schaffer says. "We do get assistance from the organizations that work on the offensive mission. Whether they bring their work [to us] is something they have to decide. That is not something that we worry about."

A growing awareness of the cyberthreat to critical U.S. infrastructure assets, however, may well deepen concerns about the "blowback" risk to the U.S. homeland from the development of a potent cyberweapon designed to be used elsewhere.

The appropriate level of information-sharing between the offensive and defensive teams within the U.S. cybercommunity is likely to be the focus of intense interagency discussion.

"My sense is that there are lots of people talking about it," says Herbert Lin, chief scientist at the National Academy of Sciences and a co-editor of [a book on policy, law and ethics in cyberwar](http://www.nap.edu/openbook.php?record_id=12651&page=1). "But almost all of the discussion is going on behind closed doors."

Eventually, this could change. Whether and when the United States should use nuclear weapons or chemical weapons or land mines has been vigorously debated in public for years, and it may be only a matter of time until the use of cyberweapons gets similar attention.

--- **What Is Stuxnet?**

"Stuxnet" is a computer worm designed to attack large-scale industrial facilities like power plants, dams, refineries or water treatment centers. It targets the computer systems used to monitor and control specific operations in those facilities, and most famously was used to destroy centrifuges in a uranium enrichment facility in Natanz, Iran.

In that case, the Stuxnet worm rewrote the code in a component that controlled the rotor speeds of the centrifuges. The code alteration resulted in slight variations in the rotor speeds, subtle enough not to cause attention but significant enough to cause physical damage to the centrifuges. The name "Stuxnet" comes from a combination of key file names hidden in the code.

Several features of the Stuxnet worm distinguished it as highly advanced. No previous computer virus had been used to physically sabotage industrial machinery. It is also unique in its ability to remain undetected for a long period of time, largely by sending fake messages that suggest processes are running normally. It has the ability to search for particular components, leaving others undisturbed. At least two U.S. computer systems in the United States were found to be "infected" by Stuxnet, but they were not "affected," according to Department of Homeland Security officials, because they did not match the Stuxnet requirements.

The sophistication and complexity of the Stuxnet worm has led researchers to believe that only a well-resourced nation-state could have developed it.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Assassination Backlash

By Andrew Cockburn, [Los Angeles Times](http://www.latimes.com/news/opinion/commentary/la-oe-cockburn-assassination-20111103%2C0%2C6016732.story), November 3, 2011 (op-ed)

There is no denying that 2011 has been a banner year for taxpayer-funded assassinations — Osama bin Laden, Anwar Awlaki, five senior Pakistani Taliban commanders in October and many more. Given the crucial U.S. backup role in Libya, and the ringing exhortation for the Libyan leader's death issued by Secretary of State Hillary Rodham Clinton just before the event itself, we can probably take a lot of credit for Moammar Kadafi's messy end too.

Once upon a time, U.S. officials used to claim that we were merely targeting "command and control centers," rather than specific individuals, as in the hunt for Saddam Hussein during the 1991 Persian Gulf War or the raid on Kadafi in 1986. Nowadays no one bothers to pretend. Successful assassination missions, whether by elite special forces or remote-controlled drones, are openly celebrated.

Clearly, the sentiment prevalent among our leaders is that eliminating particular enemy leaders is bound to have a beneficial effect. Thus in our recent wars, the U.S. has made the pursuit of "high-value targets," the principal objective of so-called human network attacks, a priority. "The platoon's mission is to kill or capture HVTs," recalled Matt Cook, a sergeant in the 101st Airborne based in northern Iraq in 2005. "That is all we do."

By 2008, according to a U.S. Strategic Command study, our military was simultaneously engaged in no fewer than 285 human network attack programs.

So, now that assassination is an official tool of U.S. foreign policy, along with trade embargoes and overseas aid, it is surely time for an open debate on whether it is indeed effective. Surprisingly for some, evidence based on hard numbers demonstrates unequivocally that the answer is no.

The numbers are derived from a study conducted in Iraq during the "surge" campaign of 2007-08 that enabled the U.S. to declare victory and wind down the war. Key to the surge was an intensive and ruthless hunt for key individuals in the "IED networks" that were organizing homemade bomb attacks against U.S. troops. Cause and effect — more dead network leaders leading to fewer bombs — seemed so self-evidently obvious that nobody bothered to check.

Early in 2008, however, Rex Rivolo, an analyst at the Counter-IED Operations/Intelligence Center attached to U.S. headquarters in Baghdad, briefed his superiors on some hard realities of the campaign. With access to any and all information relating to U.S. military operations in Iraq, he had identified about 200 successful missions in which key IED network individuals had been eliminated. Then he looked at the reports of subsequent bomb attacks in the late insurgent leader's area of operation. The results were clear: IED attacks went up, immediately and sharply. One week after the hit, on average, incidents within about three miles of the dead leader's home base had risen 20%.

Why, with the commander dead, did the enemy fight with such reinforced vigor? Eliminated enemy commanders, intelligence revealed, were almost always replaced at once, usually within 24 hours. "The new guy is going to work harder," Rivolo told me. "He has to prove himself, assert his authority. Maybe the old guy had been getting lazy, not working so hard to plant those IEDs. Fresh blood makes a difference."

Once posited, this consequence may appear obvious, but Rivolo's study, so far as I am aware, was the only time that anyone with access to relevant data had looked at the consequences of our principal national security strategy in a systematic way. However, even as he submitted his conclusions, the same strategy was being exported to Afghanistan on a major scale. Ever-increasing special forces "night raids" have indeed subsequently succeeded in killing large numbers of insurgent commanders (along with many civilians), but the consequences have been depressingly predictable.

"I used to be able to go talk to local Taliban commanders," a journalist long resident in Afghanistan told me, "but they are all dead. The ones who replaced them are much more dangerous. They don't want to talk to anyone at all."

Nongovernmental groups similarly report that the new breed of Taliban leadership is unwilling to allow the free passage of aid workers permitted by their assassinated predecessors. Neither in Afghanistan nor Pakistan, where high-value targets are the responsibility of the CIA's burgeoning killer-drone bureaucracy, is there any indication that the enemy's military capability has been diminished.

As Matthew Hoh, the foreign service officer who quit in protest at the futility of the Afghan war, told me recently, "War is a breeding ground for unintended consequences."

President Obama should think about that.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

China's Cyber-Warfare Capabilities Are 'Fairly Rudimentary'

By Duncan Geere, [Wired](http://www.wired.co.uk/news/archive/2011-11/02/china-cyberwar), 02 November 11.

Amidst growing concern over electronic warfare, an Australian academic has dismissed China's cyber-warfare capabilities as "fairly rudimentary".

Desmond Ball, a professor in the Strategic and Defence Studies Centre in Australia's National University argues that the country's offensive capabilities are actually pretty limited, and that its internal security has a bunch of vulnerabilities.

Ball says that China has carried out a selection of high-profile hacks recently, as well as website defacements and DDoS attacks, but that those attacks have demonstrated little in the way of sophistication. "The viruses and trojan horses they have used have been fairly easy to detect and remove before any damage has been done or data stolen. There is no evidence that China's cyber-warriors can penetrate highly secure networks or covertly steal or falsify critical data," says the [paper](http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf) (PDF).

"They would be unable to systematically cripple selected command and control, air defence and intelligence networks and databases of advanced adversaries, or to conduct deception operations by secretly manipulating the data in these networks."

Ball rated other countries' capabilities significantly higher than China, despite it having had an information warfare plan since 1995 and having conducted exercises since 1997.

He predicts that "China is condemned to inferiority in [information warfare] capabilities for probably several decades".

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

No Other Nation Has Anything Like It

[Strategy Page](http://www.strategypage.com/htmw/htiw/articles/20111102.aspx), November 2, 2011

China continues to expand its already enormous Internet Army. The latest effort is ordering companies to organize their Internet savvy employees into a cyber-militia, and inspire these geeks to find ways to protect the firm's networks. In practice, many companies just tell all males under 30 that they have volunteered. Less publicized is the training given to some of these company militias on how to carry out Internet based espionage. The understanding is that there much less risk if this capability is only used against foreign firms.

All this is the result of 13 years of effort. It was in the late 1990s that the Chinese Defense Ministry established the "NET Force." This was initially a research organization, which was to measure China's vulnerability to attacks via the Internet. Soon this led to examining the vulnerability of other countries, especially the United States, Japan and South Korea (all nations that were heavy Internet users). NET Force has continued to grow.

In 1999, NET Force organized an irregular civilian militia; the "Red Hackers Union" (RHU). These are several hundred thousand patriotic Chinese programmers and Internet engineers who wished to assist the motherland, and put the hurt, via the Internet, on those who threaten or insult China. The RHU began spontaneously (in response to American bombs accidentally hitting the Chinese embassy in Serbia), but the government gradually assumed some control, without turning the voluntary organization into another bureaucracy. Various ministries have liaison officers who basically keep in touch with what the RHU is up to (mostly the usual geek chatter), and intervene only to "suggest" that certain key RHU members back off from certain subjects or activities. Such "suggestions" carry great weight in China, where people who misbehave on the web are very publicly prosecuted and sent to jail. For those RHU opinion-leaders and ace hackers that cooperate, there are all manner of benefits for their careers, not to mention some leniency if they get into some trouble with the authorities. Many government officials fear the RHU, believing that it could easily turn into a "counter-revolutionary force." So far, the Defense Ministry and NET Force officials have assured the senior politicians that they have the RHU under control.

NET Force was never meant to be just volunteers. Starting in the late 1990s, China assembled the first of what eventually grew to 40,000 Ministry of Public Security employees manning the Golden Shield Project (nicknamed as The Great Firewall of China). This was an effort to monitor and censor Internet use throughout the country, and punish those who got out of line. In the last decade, over a billion dollars has been spent on this effort. While the Great Firewall cannot stop someone expert at how the Internet works, it does greatly restrict the other 99 percent of Internet users. And it provides lots of information about what is going on inside all that Internet traffic. Foreign intelligence agencies are beginning to find the Great Firewall of China is going from nuisance to obstacle. This has put government intelligence organizations in a difficult position. In the U.S., the feds feel compelled to seek assistance from, and work with, hackers who are developing new ways to tunnel through the Golden Shield. There are several non-governmental outfits that are involved with this effort, and most are hostile to intelligence agencies. Nevertheless, some relationships have been formed, to deal with mutual problems.

It's not only the intel agencies who are keen to learn their way around, and through, the Great Firewall. Cyber War organizations see the Great Firewall as a major defensive weapon as well. The Chinese have a much better idea of what is coming into their country via the Internet, and that makes it easier to identify hostile traffic, and deal with it. Some American Cyber War officials are broaching the idea of building something like Golden Shield, just for military purposes. But that would be difficult in most Western countries, because of privacy issues. But with Golden Shield, China could unleash worms and viruses on the Internet, and use their Great Firewall to prevent Chinese systems from becoming as badly infected. China needs every advantage it can get, because it has the worst protected, and most infected, PCs in the world. This is largely the result of so many computers using pirated software, and poorly trained operators. Meanwhile, the thousands of people running the Golden Shield are gaining valuable experience, and becoming some of the most skillful Internet engineers on the planet.

The military also has a growing number of formal Cyber War units, as well as military sponsored college level Cyber War courses. These Cyber War units, plus the four larger organizations, apparently work closely with each other, have provided China with a formidable Cyber War capability. NET Force, with only a few thousand personnel, appears to be the controlling organization for all this. With the help of RHU and Golden Shield, they can mobilize formidable attacks, as well as great defensive potential. No other nation has anything like it.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Feds Cite Chinese Cyber Army Capability

By Mathew J. Schwartz, [InformationWeek](http://www.informationweek.com/news/security/attacks/231902276), November 03, 2011

The U.S. government continues to point the cyber-attack finger at China and Russia, but at least one academic is questioning the actual capabilities of China's cyber army.

The most recent U.S. government accusations came on Thursday, with the release of a report to Congress from the top U.S. counterintelligence agency. The report's title, "[Foreign Spies Stealing U.S. Economic Secrets in Cyberspace](http://www.ncix.gov/publications/reports/fecie_all/index.html)," left little doubt as to its findings. All that was left was to identify the foreign governments in question.

"Chinese actors are the world's most active and persistent perpetrators of economic espionage," according to the report, released by the Office of the National Counterintelligence Executive. And, "Russia's intelligence services are conducting a range of activities to collect economic information and technology from U.S. targets."

"Trade secrets developed over thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors," said national counterintelligence executive Robert "Bear" Bryant, at a press briefing that detailed the report's findings, reported The Washington Post.

While the annual counterintelligence report has been released since 1995, this is the first year that a report has emphasized "foreign collectors" exploits. According to news reports, administration officials said that was because of the severity of the problem.

Part of the issue, of course, is that nearly all business-critical information today gets stored digitally, which makes for a larger online attack target than ever before. Unlike the old days of espionage, online attackers also face few personal risks when they try to procure digital data. "Cyberspace makes it possible for foreign collectors to gather enormous quantities of information quickly and with little risk, whether via remote exploitation of victims' computer networks, downloads of data to external media devices, or email messages transmitting sensitive information," according to the report.

But China and Russia aren't the only countries being blamed. In fact, U.S. allies are also gunning for sensitive data, sometimes using [social engineering attacks](http://www.informationweek.com/news/security/vulnerabilities/231601868) to get it. "Some U.S. allies and partners use their broad access to U.S. institutions to acquire sensitive U.S. economic and technology information, primarily through aggressive elicitation and other human intelligence tactics. Some of these states have advanced cyber capabilities," said the report.

But how bad is the actual threat? In the wake of reports such as this one, observers sometimes accuse the government of inflating cyber threats, in part due to agencies positioning themselves to be the future guardians of the nation's cyber defenses, in light of the potential for massive, related appropriations from Congress.

If China has unleashed a massive intelligence-gathering campaign against the United States and its close allies, however, what can be done about it? For starters, leading government and private sector CIOs have called on the government to improve its threat intelligence information-sharing efforts with the private sector, to help businesses more easily spot advanced persistent threats that can target just a handful of computers at a small number of companies, yet succeed.

Information aside, some of the blame for China's success at spying may go to U.S. businesses simply not being serious enough about information security. Indeed, one study of China's cyber warfare and online exploitation capabilities finds that the country's attacks are hardly state of the art.

"China is condemned to inferiority in [information warfare] capabilities for probably several decades," according to "[China's Cyber Warfare Capabilities](http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html)," published in the most recent issue of Security Challenges.

The report's author, Desmond Ball, is a professor in the Strategic and Defense Studies Center at the Australian National University, and has long studied China's cyber warfare and espionage capabilities. He's found that without exception, Chinese attackers rely on rudimentary viruses and Trojan applications that would pale in comparison to the best botnet toolkits available on the black market.

"They have evinced little proficiency with more sophisticated hacking techniques," said Ball in this report, referring to China. "The viruses and Trojan Horses they have used have been fairly easy to detect and remove before any damage has been done or data stolen.

"There is no evidence that China's cyber-warriors can penetrate highly secure networks or covertly steal or falsify critical data," he said. "They would be unable to systematically cripple selected command and control, air defense and intelligence networks and databases of advanced adversaries, or to conduct deception operations by secretly manipulating the data in these networks."

 [China’s Cyber Warfare Capabilities]

 

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

China scorns U.S. cyber espionage charges

[Reuters](http://in.reuters.com/article/2011/11/04/idINIndia-60319820111104), 4 Nov 2011

BEIJING (Reuters) - China on Friday dismissed a U.S. report on online spying as "irresponsible", rejecting the charge that China uses cyber espionage to steal lucrative U.S. trade and technology secrets.

The U.S. intelligence report said on Thursday China and Russia are using cyber espionage to steal U.S. trade and technology secrets to bolster their own economic development, which poses a threat to U.S. prosperity and security.

So much sensitive information sits on computer networks that foreign intruders can net massive amounts of valuable data with scant risk of detection, said the report to Congress.

Foreign intelligence services, corporations and individuals stepped up their efforts to steal information about U.S. technology that cost many millions of dollars to develop, according to the report by the Office of the National Counterintelligence Executive, a U.S. government agency.

But the Chinese Foreign Ministry spokesman Hong Lei rejected the report, and repeated Beijing's long-standing position that it wants to help.

"Online attacks are notable for spanning national borders and being anonymous. Identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers is both unprofessional and irresponsible," Hong told a daily news briefing in answer to a question about the report.

"I hope the international community can abandon prejudice and work hard with China to maintain online security," he added.

The U.S. report acknowledged the difficulty of determining who exactly is behind a cyber attack. U.S. companies have reported intrusions into their computer networks that originated in China, but U.S. intelligence agencies cannot confirm who specifically is behind them.

Intelligence officials say it is part of the national policy of China and Russia to try to acquire sensitive technology for their own economic development, while the United States does not do economic espionage as part of its national policy.

The State Department in June said it had asked Beijing to investigate Google's allegation of a major hacking attack that the Internet giant said originated in China.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Fighting in the Fifth Dimension

[Al Jazeera](http://english.aljazeera.net/programmes/aljazeeraworld/2011/10/2011101916939402528.html?utm_content=automateplus&utm_campaign=Trial6&utm_source=SocialFlow&utm_medium=MasterAccount&utm_term=tweets), 2 Nov 2011

It has been called the 'fifth dimension of warfare'. Along with land, sea, air and space - the cyberworld is increasingly becoming a new frontline.

Innovations in technology are changing the tactics of modern-day conflict. There are new tools in today's arsenal of weapons. Helped by advances in electro-magnetics and modern information and communications technology, a new form of electronic warfare has been created. It is called cyberwar and is increasingly recognised by governments and the military as posing a potentially grave threat.

"If you have a few smart people and a good computer, then you can do a lot. You don't need an aircraft, you don't need tanks, you don't need an army. You can penetrate another country, create huge damage without even leaving your armchair."

Alon Ben David, military analyst for Israel's Channel 10

And it is not just cyberwar that is a growing phenomenon. The internet has empowered cyberactivism, allowing people to share information and mobilise support to take direct action - both online and on the streets.

Social networking sites such as Facebook, Twitter and YouTube have been at the forefront of this new wave of cyberactivism, helping to galvanise the protests that have recently spread across the Arab world.

The so-called Arab Spring has been described as an electronic revolution. Protesters were turned into citizen journalists - taking frontline images on their mobile phones and uploading them via their computers for the world to see. The regimes may have jammed the signals of satellite news channels and banned international reporters from entering their country, but they were unable to prevent citizens from becoming reporters in their own right.

**From cyberactivism to cyberwar**

Using the internet as a platform for political action is one thing. But infiltrating and disrupting computer networks and databases takes cyberwar to another level. American security experts have warned that a cyber-attack could cripple key governmental and financial systems and it is a threat the US is taking seriously.

"Cyberspace is real. And so are the risks that come with it. From now on, our digital infrastructure, the networks and computers we depend on every day, will be treated as they should be, as a strategic national asset."

Barack Obama, the US president

In recent years a cyberwar has been brewing between China and the US, with both countries accusing each other of running an 'army of hackers'.

A key battlefield in this war has been the case of Google.

The US internet company partially withdrew from China in 2010 after a tussle with the government over censorship and government-backed hacking.

China accuses the US of using Google to spy on the country, while Google accuses China of hacking into the email accounts of some of its members.

"We must differentiate between independent hackers and those of the state. We must understand that in some countries the authorities hire hackers with excellent technical knowledge to serve their interests. Everything is possible and states shouldn't accuse each other since all options are open in this war."

Han, a Chinese internet hacker

The US also appears to be engaged in a cyberwar with another erstwhile enemy: Iran.

It appeared to begin in 2009 following Iranian anti-government protests - sparked by the disputed presidential elections which saw Mahmoud Ahmadinejad win another term in office.

Seeking to deprive the opposition of its main means of mobilising the masses, the Iranian authorities sought to choke off internet access.

But the protestors continued to use sites such as YouTube and Twitter and when Twitter planned some routine maintenance that would have taken it offline for a few hours, Hillary Clinton, the US secretary of state, asked the site to stay up and running while the protests continued.

**Electronic eyes and ears**

In the Middle East, Israel has set up a cyber command to secure the country against hacking attacks on its key networks.

Israel's immediate neighbourhood is the place where it puts into use much of its technical know-how. Along its northern border with Lebanon, Israel deploys a large network of electronic eyes and ears.

And in the ongoing intelligence war between Israel and Lebanon's Hezbollah, increasingly sophisticated electronic equipment is being used.

In February 2010, Lebanon arrested a man who reportedly confessed to being a Mossad agent. It was claimed that he had used sophisticated surveillance equipment that sent signals to his Israeli handlers via a mobile phone and computer located in a hidden compartment inside his car.

It may all sound like science fiction, but a global spying network does exist that can eavesdrop on every single phone call and email on the planet.

Eavesdropping on phone calls and text messages has become increasing easy for those with the right equipment, especially with the development of GSM networks - the technology used on the vast majority of mobile phone networks around the world.

"Give me your mobile phone for 30 seconds, give me 30 seconds alone with your mobile phone and I can install software that would make your mobile phone a travelling microphone. From that moment on, even if it is shut down, your mobile phone will broadcast everything that goes on around you, through a number that I determine."

Alon Ben David, military analyst for Israel's Channel 10

**A brave new world?**

Many analysts are amazed at how internet users voluntarily hand over vast amounts of personal data to social media sites.

And planting software into a person's phone or computer to steal data has become a new tactic of warfare in the fifth dimension.

"Our entire life is now on the internet: personal information, emails, credit cards. We give all this information on the internet to sites like Facebook, Google and Amazon. Governments impose pressure on these sites as they know how much information they have. These governments have asked for personal information from these sites, and they gave them what they needed."

Marwan Taher, IT specialist

We live in a brave new world of information and communication technology. The possibilities seem infinite, endless ... and uncertain.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Ex-U.S. General Urges Frank Talk On Cyber Weapons

By Andrea Shalal-Esa, [WHTC](http://whtc.com/news/articles/2011/nov/06/ex-us-general-urges-frank-talk-on-cyber-weapons/), November 06, 2011

WASHINGTON (Reuters) - The United States should be more open about its development of offensive cyber weapons and spell out when it will use them as it grapples with an increasing barrage of attacks by foreign hackers, the former No. 2 uniformed officer in the U.S. military said.

"We've got to step up the game; we've got to talk about our offensive capabilities and train to them; to make them credible so that people know there's a penalty to this," said James Cartwright, the four-star Marine Corps general who retired in August as the vice chairman of the Joint Chiefs of Staff.

Cartwright, who raised the profile of cyber security issues while still in uniform, told Reuters in an interview that the increasing intensity and frequency of network attacks by hackers underscored the need for an effective deterrent.

"You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you," Cartwright, now a fellow at the Washington-based Center for Strategic and International Studies, said in one of his first interviews after leaving office.

Current and former U.S. officials are tight-lipped about any specific weapons. But it is widely acknowledged the United States has both offensive and defensive ways to respond to escalating and increasingly destructive attacks from overseas.

Underscoring the threat, this week an arm of the U.S. intelligence community released a report identifying China and Russia as the most active and persistent nations that are using cyber espionage to steal U.S. trade and technology secrets.

Cartwright said it was important to send a strong signal to potential adversaries that the United States viewed responding to cyber attacks as its "right to self-defense," even if hackers were using a server in a third country.

"We've got to get that done, because otherwise everything is a free shot at us and there's no penalty for it," he said.

His comments come as the Obama administration debates the rules of engagement for cyberspace, now seen as a fifth domain for military operations, joining air, land, sea and space.

Earlier this year, the White House released a new cyber strategy that said that, when warranted, the United States would respond to hostile acts in cyberspace "as it would to any other threat to our country."

Now the military must work out exactly how to implement that. Key questions include how forthright Washington will be about work on offensive computer network attack weapons; what would constitute an act of war; and operational plans for training, testing and using of its electronic arsenal.

PENTAGON PRIORITY

Recent attacks on U.S. corporations such as Google Inc, the Nasdaq stock exchange, Lockheed Martin Corp, and RSA, the security division of EMC Corp, have given government officials and lawmakers a renewed sense of urgency about addressing threats to U.S. computer networks.

Cartwright's concerns are widely shared by U.S. military and law enforcement officials, who are alarmed by the lack of adequate network security they see in corporate America.

General Martin Dempsey, chairman of the Joint Chiefs of Staff, told lawmakers at a classified briefing on Tuesday that improving cyber security was an increasingly important priority.

"He prominently mentioned cyber security as a growing threat ... something that needs to be much higher up on our national security priority lists than it has been in the past," Representative Adam Smith, the top Democrat on the House Armed Services Committee, told reporters after the briefing.

U.S. Army General Keith Alexander, director of the National Security Agency and U.S. Cyber Command, last month said U.S. military officials would finalize new rules of engagement and operational planes for cyber space in coming months.

QUESTIONS ABOUT DETERRENCE

Experts say any deterrent posture must be carefully crafted, but that is particularly true in cyberspace.

David Smith, a fellow at the Potomac Institute for Policy Studies and former U.S. diplomat engaged in talks with the former Soviet Union, said a deterrence policy had to be crafted very carefully to establish a credible threat of possible action without being too specific.

"You deter by keeping a level of uncertainty," Smith told Reuters. "To craft a good deterrent posture, you sort of tell people the kinds of things you have, and roughly, what the response would be if the interest of the United States were threatened, basically, that nothing is off the table."

Unlike the nuclear arena, where it was fairly easy to determine who had launched a ballistic missile attack, attribution remains an enormous challenge in cyberspace, where hackers can mask their identities.

Eric Sterner, a former Pentagon official and fellow at the conservative Marshall Institute think tank, said being too clear about what would provoke a response would invite hackers to test the limits up to that point.

"As soon as you declare a red line, you're essentially telling people that everything up to that line is OK," Sterner said.

Cartwright said it would probably take hackers two to five years before they could disable a large percentage of the banking industry or the U.S. electrical grid. But even a smaller attack could undermine confidence in financial markets, he said.

Establishing a deterrent posture now would help stem the endless tide of attacks coming from overseas, he said.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

NATO Turns To Radio to Try and Get Its Own Message to Afghan People

By Glenn Zorpette, [IEEE Spectrum](http://www.pri.org/stories/politics-society/nato-turns-to-radio-to-try-and-get-its-own-message-to-afghan-people-6832.html), 7 Nov 2011

There's a radio station in Afghanistan that sounds like any other popular Pashtun radio broadcast. But this one is different.

The station’s funding comes from NATO. Its general manager used to work at CNN. And its studios are at Kandahar Airfield, one of the largest NATO bases here.

Ted Iliff, who manages the station, said it was created to provide an alternative to listeners in southern Afghanistan who speak Pashtun. Iliff is an American who works for Strategic Social – a contractor to the U.S. Army, which is running the operation for NATO.

“It’s intended to be a news, information, and cultural station, finding a niche in the market for primarily local and regional news, and local and regional cultural affairs to try to give a local flavor to the listeners that they don’t seem to be getting from the other broadcasters,” he said.

Here in Afghanistan, the golden age of radio is now, because the average Afghan can’t read, can’t afford a television, and has only sporadic access to electricity. So radio fills an enormous void, one NATO is making sure it fills, especially when it comes to news programming.

“News is a huge area of interest for the population here,” said Major Thomas Wood, the chief of broadcast media for the U.S. Army’s Tenth Mountain Division, stationed at Kandahar.

He said in many Afghan villages, news is still delivered by word of mouth.

“Due to the terrain and the lack of mass transportation, the populations generally have been not able to gather news from different areas ... as they’re being exposed to radio broadcasting in particular, there’s a hunger for more information about what’s going on throughout the world,” he said.

Wood says the military has set up roughly a hundred transmitting stations throughout Afghanistan. Many are what are known as a “radio in a box."

Each box consists of a simple transmitter, an antenna, a laptop computer, and a small diesel generator. The whole setup would fit in a walk-in closet. The broadcast signal is sent to the boxes via the Internet – typically from a regional station, such as the one here at Kandahar, where news and music programs are produced by a staff of Afghan professionals.

Wartime radio has come a long way from World War II and the days of Tokyo Rose – the name for a group of Japanese women who played American popular music and broadcast messages of foreboding to Allied soldiers in the Pacific.

Like Tokyo Rose, NATO’S radio operations in Afghanistan are a form of psychological operations. But NATO’s broadcasts are more subtle than the dire warnings that soldiers heard in the Pacific 70 years ago.

Iliff said NATO’s sponsorship hasn't really affected how he covers the news.

“It doesn’t a lot, very much at all. There are certain things that they want to emphasize or think are important,” he said. For example, “governance, security, education, agriculture in terms of poppy eradication. Reintegration in terms of opposition to insurgents joining the government and putting down their weapons ... we know what the sponsor is interested in, but at the same time, we do news and they know that we’ve built as much of a firewall as we can between news and other information so we can maintain our credibility as best as any news organization can.”

So, in the interest of presenting all viewpoints in a story, would he put a representative of the Taliban on the air? For that, Iliff said, he’d have to check with his military sponsors in NATO.

“It’d have to be a really special case, and it’d have to be something the sponsor would authorize. In fairness to the sponsor, they’ve been very open to all kinds of ideas. I don’t know how they’d react in that situation, but they have left us alone ... It’s been very refreshing, how they have their opportunities to say what they want to say, and they leave us alone with news and information to do what we think is necessary,” Ted Iliff said.

Make no mistake: NATO isn’t footing the multimillion-dollar bill to run RIAB stations in Afghanistan simply because it wants Afghans to have better news choices. This network is a crucial part of NATO’s information war here. Taliban and insurgent forces are present in many of the country’s scattered rural villages, and in those villages especially, NATO needs to counter the Taliban media’s version of events.

“We tell the people that in Afghanistan, it’s not only fighting going on,” said Mohammed Sarwar, an announcer at the station at the Governor’s palace in Kandahar.

“If you see outside, there is improvement in education. In the time of Taliban, there was not any schools, but you see now there are hundreds of schools out there ... Our target is to tell the people, that Afghanistan, day by day, they’re improving. We want to tell them, there is not only fighting, but also construction work going on. The people, they’re happy, and they need peace. Now, do you know some time, do you know the Taliban says something against government, so we have to tell them the reality. This is not the reality. This is the reality.”

When a pastor in Florida burned a Koran last March, three days of rioting across Afghanistan followed. In Kandahar alone, 14 people were killed and more than a hundred injured. Major Wood says NATO's network took on the Taliban directly.

“You had Taliban media putting out things along the lines of, there’s multiple instances of it; it wasn’t just an isolated case, and it was something that was being perpetrated not only by people back in the states, but being done by forces here in Afghanistan. You have Kandahar media center and the local journalists who redress those accusations, and by providing honest and open reporting, are able to counter that,” Wood said.

To make sure Afghans get the message, NATO has handed out thousands of green AM-FM radios that can be powered by either the sun or a hand crank.

Someday, after NATO leaves, the Afghan government will be left with transmitters scattered across the country. Military officials here suggest that those stations could form the basis of a new public radio network in Afghanistan.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

DRDO Developing a Futuristic E-Bomb

By Vijay Mohan, [Tribune](http://www.tribuneindia.com/2011/20111108/main4.htm) (India), 7 Nov 2011

Chandigarh, November 7

With electronic warfare and network-centric operations playing an increasingly significant role in today’s battlefield, the Defence Research and Development Organisation (DRDO) is developing a weapon that renders electronic gadgets useless and effectively neutralises the adversary’s command, control and communication capability.

Commonly referred to as “e-bomb”, the weapon produces a strong electromagnetic field generating powerful electricity surges that can play havoc with electronic circuits within a specified area.

“We have developed and validated the technology and the weapon in its usable form is expected to be complete within the 12th Plan,” Terminal Ballistics Research Laboratory (TBRL) director Dr Manjit Singh said.

“Though this is the biggest weapon of mass destruction next to a nuclear bomb, it has a limited collateral damage as it does not target humans and is designed to hit computer systems and networks,” he said.

The e-bomb, based on Explosive Driven High Energy Pulse Power Technology, can be deployed against non-military establishments like banking and civic utility networks, communication and power generation networks.

It not only disables gadgets and networks but also destroys or damages them, which can seriously affect day-to-day functioning of the society over an extended period of time. The bomb can also be used against mobile enemy command and control centres or advancing formations to render them “blind” by disrupting communication.

The basic principle of the weapon, according to APS Sodhi, a senior scientist working on the programme, is converting the explosive’s chemical power into electrical power. “Detonation of 1 kg of the designed explosive mixture can produce about 4.5 megaJoule of electricity energy,” he said. The explosive is a mixture of RDX and TNT.

Initially, DRDO’s e-bomb is being designed for delivery by combat aircraft and later, as technology is matured and the warhead made more compact, it would be integrated with missiles.

How does it work

The e-bomb produces a strong electromagnetic field generating powerful electricity surges that can play havoc with electronic circuits in a specified area

It not only disables and damages gadgets and networks, but also destroys them

The bomb can be used against mobile enemy command and control centres to render them “blind” by disrupting communication

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

CIA following Twitter, Facebook

By Kimberly Dozier, [Associated Press](http://www.washingtontimes.com/news/2011/nov/4/cia-following-twitter-facebook/print/), November 4, 2011

McLEAN, Virginia (AP) — In an anonymous industrial park in Virginia, in an unassuming brick building, the CIA is following tweets — up to 5 million a day.

At the agency's Open Source Center, a team known affectionately as the "vengeful librarians" also pores over Facebook, newspapers, TV news channels, local radio stations, Internet chat rooms — anything overseas that anyone can access and contribute to openly.

From Arabic to Mandarin Chinese, from an angry tweet to a thoughtful blog, the analysts gather the information, often in native tongue. They cross-reference it with the local newspaper or a clandestinely intercepted phone conversation. From there, they build a picture sought by the highest levels at the White House, giving a real-time peek, for example, at the mood of a region after the Navy SEAL raid that killed Osama bin Laden or perhaps a prediction of which Mideast nation seems ripe for revolt.

Yes, they saw the uprising in Egypt coming; they just didn't know exactly when revolution might hit, said the center's director, Doug Naquin.

The center already had "predicted that social media in places like Egypt could be a game-changer and a threat to the regime," he said in a recent interview with The Associated Press at the center. CIA officials said it was the first such visit by a reporter the agency has ever granted.

The CIA facility was set up in response to a recommendation by the 9/11 Commission, with its first priority to focus on counterterrorism and counterproliferation. But its several hundred analysts — the actual number is classified — track a broad range, from Chinese Internet access to the mood on the street in Pakistan.

While most are based in Virginia, the analysts also are scattered throughout U.S. embassies worldwide to get a step closer to the pulse of their subjects.

The most successful analysts, Naquin said, are something like the heroine of the crime novel "The Girl With the Dragon Tattoo," a quirky, irreverent computer hacker who "knows how to find stuff other people don't know exists."

Those with a masters' degree in library science and multiple languages, especially those who grew up speaking another language, "make a powerful open source officer," Naquin said.

The center had started focusing on social media after watching the Twitter-sphere rock the Iranian regime during the Green Revolution of 2009, when thousands protested the results of the elections that put Iranian President Mahmoud Ahmadinejad back in power. "Farsi was the third largest presence in social media blogs at the time on the Web," Naquin said.

The center's analysis ends up in President Barack Obama's daily intelligence briefing in one form or another, almost every day.

After bin Laden was killed in Pakistan in May, the CIA followed Twitter to give the White House a snapshot of world public opinion.

Since tweets can't necessarily be pegged to a geographic location, the analysts broke down reaction by languages. The result: The majority of Urdu tweets, the language of Pakistan, and Chinese tweets, were negative. China is a close ally of Pakistan's. Pakistani officials protested the raid as an affront to their nation's sovereignty, a sore point that continues to complicate U.S.-Pakistani relations.

When the president gave his speech addressing Mideast issues a few weeks after the raid, the tweet response over the next 24 hours came in negative from Turkey, Egypt, Yemen, Algeria, the Persian Gulf and Israel, too, with speakers of Arabic and Turkic tweets charging that Obama favored Israel, and Hebrew tweets denouncing the speech as pro-Arab.

In the next few days, major news media came to the same conclusion, as did analysis by the covert side of U.S. intelligence based on intercepts and human intelligence gathered in the region.

The center is also in the process of comparing its social media results with the track record of polling organizations, trying to see which produces more accurate results, Naquin said.

"We do what we can to caveat that we may be getting an overrepresentation of the urban elite," said Naquin, acknowledging that only a small slice of the population in many areas they are monitoring has access to computers and Internet. But he points out that access to social media sites via cellphones is growing in areas like Africa, meaning a "wider portion of the population than you might expect is sounding off and holding forth than it might appear if you count the Internet hookups in a given country."

Sites like Facebook and Twitter also have become a key resource for following a fast-moving crisis such as the riots that raged across Bangkok in April and May of last year, the center's deputy director said. The Associated Press agreed not to identify him because he sometimes still works undercover in foreign countries.

As director, Naquin is identified publicly by the agency although the location of the center is kept secret to deter attacks, whether physical or electronic.

The deputy director was one of a skeleton crew of 20 U.S. government employees who kept the U.S. Embassy in Bangkok running throughout the rioting as protesters surged through the streets, swarming the embassy neighborhood and trapping U.S. diplomats and Thais alike in their homes.

The army moved in, and traditional media reporting slowed to a trickle as local reporters were either trapped or cowed by government forces.

"But within an hour, it was all surging out on Twitter and Facebook," the deputy director said. The CIA homed in on 12 to 15 users who tweeted situation reports and cellphone photos of demonstrations. The CIA staff cross-referenced the tweeters with the limited news reports to figure out who among them was providing reliable information. Tweeters also policed themselves, pointing out when someone else had filed an inaccurate account.

"That helped us narrow down to those dozen we could count on," he said.

Ultimately, some two-thirds of the reports coming out of the embassy being sent back to all branches of government in Washington came from the CIA's open source analysis throughout the crisis.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Speculation Continues Over Hezbollah’s Ability To Disable Israeli Drones

By Nicholas Blanford, The [Daily Star](http://www.dailystar.com.lb/News/Politics/2011/Nov-09/153450-speculation-continues-over-hezbollahs-ability-to-disable-israeli-drones.ashx#ixzz1dJUIUyXc) , 9 Nov 2011

BEIRUT: The recent mysterious disappearance of a suspected Israeli pilotless reconnaissance plane from the radar screen of the French UNIFIL battalion in south Lebanon has raised speculation that Hezbollah has found a way of electronically jamming and disabling drones.

Information has been circulating for over a year that Hezbollah has been exploring – and may have discovered – a means of jamming the data link between a drone and its ground control base or interfering with the guidance system of drones on pre-programed flight missions in order to crash them.

There is no confirmation yet that Hezbollah has acquired the ability to jam and destroy Israeli reconnaissance drones, but there is no question that its highly secret electronic warfare and communications capabilities have advanced tremendously over the past decade and will play a critical role in any future war with Israel.

The French UNIFIL battalion detected an aerial object on the afternoon of Oct. 29 as it passed over the Bint Jbeil area. The object’s radar signature indicated that it was a reconnaissance drone, one of dozens that fly over Lebanese airspace on a weekly basis. The French tracked the drone until it reached the area above Wadi Hujeir, a deep forested valley system east of the villages of Ghandourieh and Froun, when it suddenly vanished from the screen.

UNIFIL alerted the Lebanese Army and a search was conducted in the Wadi Hujeir area but nothing was found. There is unconfirmed information that a searchlight was seen in the valley, presumably used by someone other than UNIFIL and the army.

There is also unconfirmed information that another Israeli drone was deployed to Wadi Hujeir shortly afterward, possibly to look for the missing aircraft. There has been no mention in the Israeli media of a drone having been lost over Lebanon.

It is possible that the drone simply malfunctioned and crashed into Wadi Hujeir, although that would not explain the absence of wreckage. There are no known previous incidents of drones malfunctioning and crashing over Lebanon, although some have been shot down in the past. Also it is unclear how thoroughly UNIFIL and the Lebanese Army conducted their search. As far as UNIFIL is concerned, once the incident has been reported, it is the responsibility of the Lebanese Army to take the lead on any investigation and further ground searches.

Drones comprise about 70 percent of all Israeli overflights in Lebanese airspace and unlike jets, they are difficult to spot because of their size and the high altitude at which they usually operate. But UNIFIL and the Lebanese Army have no difficulty in tracking the drones on radar and sometimes identifying the model.

Israel has been using drones for reconnaissance in the Lebanon theater since the 1982 invasion. In the July 2006 war Israel deployed missile-firing drones for the first time, some of which were responsible for targeting civilian vehicles fleeing south Lebanon and attacking two parked ambulances in Qana during a transfer of injured individuals.

Although drones cannot carry the same amount of firepower as Israel’s fleet of Apache and Cobra helicopter gunships, they are stealthier, have the ability to deliver pin-point strikes and, for casualty-conscious Israel, there are no aircrews to lose.

In August 2010, Sayyed Hassan Nasrallah, Hezbollah’s secretary-general, revealed that in the mid-1990s the party had found a way to intercept and download the video feed from Israeli drones. The video footage was unencrypted at the time which allowed Hezbollah’s technicians to watch on television screens whatever the drones had been filming. According to Nasrallah, it was this intelligence-gathering technique that allowed Hezbollah to mount an ambush against a team of Israeli naval commandos beside the village of Ansariyah in September 1997, killing 12 of them. Israel began encrypting its drone video data following the Ansariyah debacle after suspecting that Hezbollah may have found a way to intercept it.

In the mid-1990s, Hezbollah’s electronic warfare capabilities were limited, mainly to scanners to record garrulous Israeli soldiers chatting on their cellphones in their frontline outposts.

Hezbollah’s electronic warfare and communications revolution took off from 2000 when it began building a military infrastructure of bunkers, tunnels and rocket-firing platforms in south Lebanon and connecting together its various facilities with a newly installed fiber-optic communications network.

Not only does Hezbollah have access to commercially available technology, it also benefits from Iran’s military-grade electronic warfare capabilities.

Although much attention is paid to Hezbollah’s acquisition of new weapons systems such as rockets and anti-aircraft assets, it is the advances in its electronic warfare capabilities – what one Hezbollah fighter termed the “war of brains” with Israel – that really illustrates the qualitative military leap Hezbollah has made in the past 15 years.

Given the importance to Israel of reconnaissance drones and given Hezbollah’s ability more than a decade and a half ago to intercept video feeds, it is only natural that Hezbollah’s technicians would be seeking ways of electronically disabling drones or cracking the encrypted video data.

Furthermore, Hezbollah is not alone in exploring drone interception. In December 2009, it was revealed that Kata’eb Hezbollah, an Iran-supported group in Iraq to which Lebanese Hezbollah has ties, had hacked into live video feeds of U.S. Predator drones operating in Iraqi airspace. U.S. soldiers had discovered “highly technical, highly sophisticated” equipment and recordings of downloaded video data from drones in the hands of captured Kata’eb Hezbollah personnel.

Since the Oct. 29 incident, UNIFIL has been buzzing with speculation about the possibility that Hezbollah may have brought down the drone electronically. It would not be the first time that UNIFIL has stumbled upon curious radar tracks. For a period in early 2010, UNIFIL radar stations picked up mysterious rocket launchings from the border district. The radar located the launch site, tracked the rocket’s trajectory and marked the impact location inside Israel. Yet, there was no further evidence rocket launches apart from the radar. At first, UNIFIL wondered whether Hezbollah had found a way of tricking radars by transmitting false signals to disguise real rocket launches.

Then UNIFIL thought Israeli electronic interference might be responsible but the peacekeepers were unable to come to any firm conclusion.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Beijing’s electronic Pearl Harbor

By Brett M. Decker and William C. Triplett II, [Washington Times](http://www.washingtontimes.com/news/2011/nov/11/beijings-electronic-pearl-harbor/), November 11, 2011

In November 1997, Deputy Defense Secretary John Hamre testified before the Senate Subcommittee on Terrorism that “we’re facing the possibility of an electronic Pearl Harbor. … There is going to be an electronic attack on this country some time in the future.” Two years later, he told a secret session of the House Armed Services Committee, “We are at war - right now. We are in cyberwar.” Fast-forward more than a decade, to 2011. President Obama’s choice for secretary of defense, Leon Panetta, tells the Senate Armed Services Committee at his confirmation hearing that the United States faces a possible “electronic Pearl Harbor.” Mr. Panetta had been the CIA director for the previous two years - so he would have known.

Two extreme, nearly identical warnings 12 years apart should have brought home the magnitude of the electronic threat facing the country. Yet nothing was done. When former Director of National IntelligenceAdm. Mike McConnell was asked directly by Congress about our ability to withstand such an onslaught, he replied, “The United States is not prepared for such an attack.”

The Obama administration has shown a shocking disinterest in this threat, earning it a blunt rebuke from former White House national security official Richard Clarke. While “our government is engaged in defending only its own networks … it is failing in its responsibility to protect the rest of America from Chinese cyber-attack,” Mr. Clarke wrote in the Wall Street Journal. In other words, the federal government has taken action to protect itself, but not the rest of us. Mr. Clarke further declared that “senior U.S. officials know well that the government of China is systematically attacking the computer networks of the U.S. government and American corporations,” and yet, “In private, U.S. officials admit that the government has no strategy to stop the Chinese cyber-assault.”

This searing denunciation of the Obama administration’s passivity toward China is made all the more powerful by the fact that Mr. Clarke is no Republican partisan. To the contrary, he had a bitter falling out with the Bush administration during his service, after which he became a generous contributor to liberal groups such as Moveon.org and to Democratic candidates including Barack Obama himself.

Illustration: Bowing to BeijingThe Obama administration at least claims to recognize the problem. Deputy Defense Secretary William Lynn told a European audience in June 2011, “The third and most dangerous cyberthreat is destruction, where cybertools are used to cause physical damage. … It is possible to imagine attacks on military networks or on critical infrastructure - like the transportation system and energy sector - that cause economic damage, physical destruction, or even loss of life.” However, the administration’s grand solution is, as Mr. Lynn took great pride in announcing, merely to institute “a pilot program with a handful of defense companies to provide more robust protection for their networks.” The commanders of the Chinese Army must be quaking in their desk chairs.

Most Americans don’t realize the Chinese have already successfully attacked many U.S. government and civilian computer systems. The Wall Street Journal noted that in one major Chinese intrusion, the attackers were “able to copy and siphon off several terabytes of data related to design and electronics systems … potentially making it easier to defend against [American F-35 fighter-jets].” Consequently, “Chinese spies enjoyed months of access to the personal Google emails of U.S. officials and human rights activists,” reported London’s Telegraph in 2011.

In 2006, network intrusions caused authorities to shut down the entire computer system at the U.S. Naval War College. Air Force Gen. Richard Goetze, a professor at the military school who previously was the commander in charge of developing America’s strategic nuclear war plan, told his students the Chinese “took down” the war college’s network. Even the school’s website and email systems went down. For weeks afterward, military officers - both students and professors - at the school were forced to use private email accounts such as yahoo and gmail instead of their official addresses, exposing government business to untold security risks. This embarrassing attack exposed a serious Pentagon vulnerability as the Naval War College was where the Defense Department created a cyberwarfare center specifically to counter the threat from hackers. Two days after the incident, U.S. Strategic Command raised the security alert level of America’s entire military computer network. Alan Paller, a security expert at the SAND Institute, observed, “The depth of the penetration is more than anybody is admitting.”

America isn’t the only target; financial institutions and international organizations are also vulnerable to Beijing’s cyber-offensive. Chinese hackers blew through the defenses of the Indian company Satyam that held the computer services contract for the World Bank in 2008. Internal World Bank emails called this an “unprecedented crisis,” as World Bank officials held angry closed door meetings with China’s executive director with the bank. Similarly, the International Monetary Fund won’t say who penetrated its information systems in the spring of 2011, but most experts point to China. In 2009, a Canadian think tank identified China as the source of a cybernetwork that “tapped into classified documents from government and private organizations of 103 countries.”

CNN’s computer expert Adam Segal notes that Chinese hackers stole proprietary information from “DuPont, Johnson & Johnson, General Electric, RSA, Epsilon, NASDAQ and at least a dozen other firms.” Moreover, a 2011 Chinese cyber-assault on major Western oil companies, nicknamed “Night Dragon,” was discovered by cybersecurity firm McAffee, Inc., which also found that a “one-state actor” had successfully penetrated scores of industrial companies in what McAffee dubbed “Operation Shady Rat.” The firm didn’t specify which nation was behind Shady Rat, but a major clue is found in the operation’s targeting of the International Olympic Committee, the World Anti-Doping Agency, and various national Olympic committees, all this occurring just before and just after the 2008 Beijing Olympics. Finally, Oak Ridge National Laboratory, where the first atomic bomb was produced, was victimized by Chinese hackers in the fall of 2007 as a follow-on to a larger penetration of U.S. national security just months before.

The Chinese hackers appear to be a vast army of chair-borne warriors associated with or downright part of the People’s Liberation Army. According to a secret U.S. State Department cable revealed by WikiLeaks, American specialists have tracked some of the most serious attacks back to sites known to belong to electronic espionage units of the Chinese military. In 2007, angry U.S. defense officers leaked an internal review reporting that the Chinese military had attacked Pentagon computer networks, including the one serving Defense Secretary Robert Gates.

We now know that the attack on the Pentagon network was more serious than initially reported, to the point that one expert, James Lewis, director of the technology and public policy program at the Washington think-tank Center for Strategic and International Studies, called it an “espionage Pearl Harbor.” In 2010, Mr. Lewis told “60 Minutes” that “terabytes of information” had been downloaded from “all of the high-tech agencies, all of the military agencies” - the State Department, the Department of Energy (which runs our nuclear weapons labs), and the Department of Defense. Asked how big a “terabyte” is, Mr. Lewis replied, “The Library of Congress, which has millions of volumes, is about 12 terabytes. So, we probably lost the equivalent of a Library of Congress worth of government information in 2007.” If the American intelligence community conducted a damage assessment afterward, it has not publicized the details.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Cyberwar Most Likely to Take Place Among Smaller Powers, Experts Say

By Jesse Emspak, [SecurityNewsDaily](http://www.securitynewsdaily.com/cyberwar-small-powers-1329/), Nov 14, 2011

Most Americans who worry about cyberwarfare are concerned that it will be directed against the United States. But the truth is that cyber conflict is far more likely to involve smaller players — and the dangers associated with that possibility are just as real.

That's because war is more common in small, unstable areas: it's where the most conflicts are. The U.S. and other big powers — Russia and China, for instance — have pretty well-established diplomatic channels. Such hotlines are less common, for example, in Central Asia, where many nations trace their modern independence to the early 1990s, or in the Middle East, where a tit-for-tat skirmish between pro-Israeli and pro-Palestinian hackers broke out just last weekend.

Jeffrey Hunker, a Pittsburgh-based cybersecurity consultant who worked for the National Security Council under President Bill Clinton as senior director for critical infrastructure, said the problem is compounded by the fact that the appropriate response to a cyberattack hasn't yet been worked out.

Fighting in the fog

"Nobody can quite figure out rules for use of engagement and response," Hunker said. "When is it an act of war? What is the mechanism for deterrence? What is the doctrine for deterrence?"

The ambiguities could create big problems if a small "patriotic" group — such as the Russian-speaking hackers who attacked Estonian websites in 2007 — were to mount a hacking attack that caused real damage, all without the explicit support of a nation-state. Thus far, such attacks haven't provoked a military response.

But they might provoke such a response in the future. Hunker noted that the Pentagon's recently unclassified cyberwar strategy treats cyberattacks, no matter who launches them, as acts of war, and other countries may see them in the same light.

Then there's the problem of governance. Pakistan, for example, has state institutions that are comparatively weak. That leaves room for rogue actors within the system to attack other countries — perhaps India. The Pakistani government might deny involvement, but that doesn't mean India would believe it.

"The scope for someone to do something irrational is expanded," Hunker said.

Jeffrey Carr, chief executive officer of Taia Global, a security consulting firm based in McLean, Va., and an expert who blogs about cyberconflict, expects attacks by non-state actors in the near future.

"I think you'll see more of that in the next few years," Carr said. "You'll see an increase in religious or other fanatical groups that just want to destroy things."

Supplementing physical attacks

Carr said he sees cyberconflict as part of larger wars and struggles. He thinks there isn't any ultimate cyberweapon that would bring down an entire nation's infrastructure. But, he said, there are other kinds of attacks that can work in tandem with "real" military force and shade into espionage.

For example, the Israeli external intelligence agency Mossad reportedly used a Trojan to infect a computer belonging to Mahmoud Al-Mabhouh, a Hamas military commander. Mossad agents allegedly read his email, figured out his travel schedule and assassinated him in a Dubai hotel room in January 2010.

During the brief war between Russia and Georgia in August 2008, "patriotic" Russian hackers disrupted communications in Georgia, but that was part of a larger pattern of attacks involving real military hardware.

Both Hunker and Carr noted that cyberweapons of any kind are much cheaper than the usual military hardware and level the playing field somewhat. Destructive malware can be downloaded from the Internet, and it is often just a matter of devoting some time and resources to developing it further.

This is something different from the days when small conflicts might be sponsored by larger powers. When the U.S. or China sells crates full of guns, they know that those guns will still be guns — even if they are turned on them by terrorists.

A cyberattack, via malware or other code, might come from anywhere and be modified in a number of ways. And small conflicts are good laboratories for such modifications.

The fact that many countries have access to at least low-level cybercriminal technology means that police actions by powerful nations, such as the NATO intervention in Libya, might provoke a digital response by smaller states.

"Ten years from now ... there's an increased chance that the U.S. or NATO would get hit by something," Hunker said.

It isn't just attacks on infrastructure or a website that can make a group powerful.

"Al-Qaida is as powerful as they are because of cyber," Hunker said, noting that prior to the Internet, a group like al-Qaida might have stayed a small, local terrorist organization.

YouTube has also given al-Qaida and other militant Islamist groups an avenue for propaganda at little cost. That was not lost on the pro-Israel hackers who in 2008 attacked Hamas websites, or the mysterious American hacker known as The Jester, who has been attacking al-Qaida-affiliated recruitment sites.

Carr said that in order to reduce the danger that small, faraway conflicts could precipitate an attack against the U.S., there would have to be a rethinking of national cyberdefense that would scrap the "fortress" mentality in favor of a more focused set of solutions.

For example, the Department of Defense is experimenting with "microgrids" to power military bases — essentially localized power supplies. That would eliminate the possibility that a power grid attack could accomplish much.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Canada puts up $477 million to foil cyber attacks

By Matthew Fisher, [Postmedia News](http://www.canada.com/news/canada-in-afghanistan/Canada%2Bputs%2Bmillion%2Bfoil%2Bcyber%2Battacks/5704819/story.html#ixzz1dmZIb68X) November 14, 2011

"This is part of Canada’s effort to protect crucial information that we and commercial interests possess that have an effect on the economy," said Peter MacKay, Canadian Minister of National Defence.Photograph by: Mark Wilson, Getty ImagesKABUL — Canada is poised to spend nearly half a billion dollars to gain access to a constellation of U.S. air force satellites designed to foil foreign cyber attacks.

Global Mercury, as Canada’s $477 million share of the Wideband Global Satcom (WGS) network, is to be known, will be immediately activated when a memorandum of understanding between the Department of National Defence and the U.S. air force is signed within the next few weeks.

"Our global security interests are not all protected by planes, ships and tanks. Some of the greatest threats are invisible, but real," Defence Minister Peter MacKay said after a visit to the Afghan capital to meet senior Afghan and NATO officials and some of the nearly 1,000 Canadian soldiers that began training Afghan security forces earlier this year as Ottawa’s 64-month combat mission in Kandahar ended.

Attempts by foreign governments to penetrate military and other government computer systems and those run by Canadian businesses were occurring "on an almost daily basis," according to a senior DND source.

MacKay did not name which countries Canada suspected of cyber attacks. However, it is widely believed that Russia and China are the leaders in this rapidly growing form of military and commercial espionage against the West.

"This is part of Canada’s effort to protect crucial information that we and commercial interests possess that have an effect on the economy," the minister said. "Because of where it is coming from, that’s why we are investing. We are spending a great deal of time studying how to protect our country against cyber attacks."

WGS was launched by the U.S. in 2007. When completed in 2018, the joint American-Australian initiative will have nine communications satellites each capable of handling massive amounts of bandwidth transmitting and exchanging secure data.

Cyber warfare was raised six weeks ago at the first meeting between MacKay and Leon Panetta, the new American secretary of defence. Panetta has, according to Reuters, said that "cyber is the battlefield of the future."

MacKay and the former director of the CIA are to meet again later this week at the Halifax International Security Forum.

Cyber security had not yet caught the attention of many Canadians "because it does not figure prominently in people’s lives," MacKay said. "It is very futuristic to speak of the cyber threat."

Another reason Canadians were generally unaware of the high number of cyber attacks against their country was that "you don’t give opponents your playbook," he said. "Speaking publicly about it does not necessarily improve our situation. Doing something about it does."

Among the other challenges that Canada faced was how to communicate much better in the Arctic, MacKay said. Radarsat 2 network has existed for several years but was in need of further upgrades, he said, including links between satellites and underwater sonar detection systems in the North and along Canada’s coastlines. The Department of Defence announced two years ago that it was to spend $25 million on such upgrades in a program known as Polar Epsilon.

Given the vastness of the High Arctic, drones, which are another emerging technology, "will figure prominently in our surveillance," MacKay said. "But we still have to determine the right platform."

Small unarmed surveillance drones known as ScanEagles had been tested for the first time three months ago in the Far North by the Royal Canadian Air Force. Canada’s first experience with flying larger unarmed drones in Afghanistan "had been instructive," although the flying conditions in the extreme heat of South Asia were much different than those found in northern Canada, MacKay said.

"The capability of drones goes up exponentially when you arm them like a fighter jet," he said. However, he noted that Canada was "investing in the F-35 (fighter jet) to cover that capability."

There has been much debate recently in the U.S. about the legality of using attack drones against suspected insurgents. Until now Canada has never acquired armed drones. However, Public Works Canada has alerted prospective manufacturers that if a project know as JUSTAS (Joint Uninhabited Surveillance and Target Acquisition System) is approved, Ottawa could spend more than $1 billion to purchase drones including attack drones.

"We are not yet at the discussion point about whether to proceed or not," with JUSTAS, MacKay said.

The media and political opposition have hounded MacKay and Canada’s top general, Walter Natynczyk lately about the justification for some flights they have taken on military aircraft.

Brushing these sometimes personal attacks aside, MacKay said: "It doesn’t compare to the work our soldiers do each day and the stress their families are under. These are part of the trials and tribulations of public life. It pales beside the suffering of Master Corporal (Byron) Greff’s family. "

Greff was the 158th Canadian soldier to die in Afghanistan. He was killed along with 15 Afghans, Americans and Britons when a suicide bomber struck the armoured bus that was transporting them between Afghan army and police training bases in Kabul last month

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Turkey Centralizes Efforts for National Cyber Security

By Ümit Enginsoy, ANKARA - [Hürriyet Daily News](http://www.hurriyetdailynews.com/n.php?n=turkey-centralizes-efforts-for-national-cyber-security-2011-11-21), November 21, 2011

Turkey is set to coordinate its various government departments’ individual efforts in order to build a national cyber security umbrella as part of its anti-terror warfare, including efforts to set up a national office.

In October Turkey’s top defense company, Aselsan, sponsored a critical workshop with the participation of government experts and academics. A series of policy recommendations was released.

“The workshop helped devise a draft road map,” said a senior security official familiar with the effort. “There is an understanding that a national coordination body will be set up.”

An independent cyber security expert said the national efforts to build a new architecture would be spearheaded by Havelsan, with contributions from Aselsan and other local companies.

A major recommendation is to launch a coordination office that will take concerted action to bring individual efforts under a national security umbrella. Another policy recommendation is to build a team of cyber security experts, similar to the U.S. efforts for the same goal, according to the document.

“It is imperative that especially government agencies with strategic importance increase their current level of security against cyber attacks,” the document said. “Local solutions at the moment do not provide government agencies with sufficient protection. Therefore, local companies must be supported to invest in better software solutions.”

Presently, Turkey’s various government departments employ individual solutions against cyber attacks. The government’s scientific research institute, TÜBİTAK, offers crypto solutions while strategic departments like the General Staff and the national intelligence agency, MİT, rely on local cyber security solutions developed by the defense software company Havelsan.

“What Turkey needs to do is to boost security at government agencies with critical strategic importance, nationalize some of the firewalls used in others and provide national solutions in general,” the expert said.

At the moment most government departments other than the General Staff and MİT rely on foreign solutions while these two have built their systems on domestic solutions. “When these efforts evolve, what we might see on a nationwide security basis could be a hybrid picture, featuring both foreign and local solutions, varying from one department to another,” the security official said.

One policy recommendation is that selected Turkish universities launch postgraduate courses to produce the necessary human resources for future efforts. “No doubt, universities will be at the core of the idea to build a solid, reliable architecture,” the cyber security expert said.

Although Turkey in 2010 included cyber terrorism and other cyber threats in a formal list of threats its national security is facing, it so far has failed to create a planned unified command to coordinate actions against this danger. Some defense officials said Turkey was intending to set up a probably two- or three-star Cyber Command at the office of the General Staff, partly resembling the Pentagon’s Cyber Command, but such a command would now probably be included in the broader plan for a national office.

In March, the government took the first steps by training eight computer specialists who would make the first core unit of any future coordination office. The team works under the command of the General Staff.

Cyber warfare generally refers to politically motivated hacking to conduct sabotage and espionage, and is a form of information warfare. Some experts qualify cyber warfare as actions by a nation state or a non-state actor to penetrate another nation’s computers or networks for the purpose of causing damage or disruption.

In the United States, the Cyber Command was set up to protect only the military, whereas the government and corporate infrastructures are primarily the responsibility respectively of the Department of Homeland Security and private companies.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

Cyber Terror

By William L. Tafoya, Ph.D., [FBI law Enforcement Bulletin](http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror), November 2011

Anyone ever misquoted recognizes the importance of context. Wrong assumptions about concepts, words, and phrases easily lead to misunderstanding. In the law enforcement community, officers who use a weapon in the line of duty to defend themselves or innocent bystanders may kill but not murder. Context often serves as the crucial variable justifying the use of deadly force. Murder is always killing, but killing is not always murder. Similarly, accurate knowledge of the context and targets of cyber attacks enhances clarity and helps to avoid obscuring intent.

“Cyber terrorism is a component of information warfare, but information warfare is not...cyber terrorism. For this reason, it is necessary to define these topics as separate entities.”1 Said another way, undefined and misunderstood terms easily could lead a conversation to proceed along parallel lines rather than an intersecting track. Thus, differentiating concepts and terms is important, as in the case of understanding what cyber terror is and what it is not.

Information Warfare

Dorothy Denning, one often-cited expert, describes but does not define information warfare (IW): “Information warfare consists of offensive and defensive operations against information resources of a ‘win-lose’ nature.” Further, “Information warfare is about operations that target or exploit information resources.”2 Nevertheless, several secondary and tertiary sources term her description “Denning’s Definition.”3 Other researchers assert that “Information warfare is combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information.”4

IW has several variants. Electronic warfare (EW), primarily a military term, is older than IW and dates back to World War II. Information operations (IO) is the more contemporary military nomenclature. EW and IO both are synonymous with IW. None of the three, however, are synonymous with cyber terror. IW, EW, and IO encompass the use of cryptography (cryptology and cryptanalysis), radar jamming, high-altitude aerial reconnaissance, electronic surveillance, electronically acquired intelligence, and steganography. Cyber terrorists may use these same tools. The distinction, however, is not the technological tools employed but the context and target.

Dr. Tafoya, a retired FBI special agent, is the coordinator of and a professor in the Information Protection and Security Program at the University of New Haven in Connecticut.

In 1991 during Operation Desert Storm, coalition forces used IW, EW, and IO through the clandestine introduction of viruses and logic bombs into Iraqi Republican Guard (IRG) command-and-control-center computers and peripherals, causing the disruption and alteration of the targeting and launching of Scud missiles.5 Military combatants engaging one another on the battlefield constitutes IW, EO, and IO. Attacking the largely civilian critical infrastructure is not warfare, but terrorism—cyber terror. But, how does cyber terror differ from IW, EW, and IO?

Cyber Terror

The term was coined in the 1980s by Barry Collin who discussed this dynamic of terrorism as transcendence from the physical to the virtual realm and “the intersection, the convergence of these two worlds....”6 The Center for Strategic and International Studies (CSIS) has defined it as “the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population.”7 The author defines cyber terror as “the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information.”

As an illustration in size, this article does not compare to the holdings of the Library of Congress. The loss of the former would be traumatic to the author, but would impact few other people. Loss of the latter, likely irreplaceable, would prove devastating if a cyber attack deleted those files. Of course, neither could compare to the loss of one human life. But, if data or information from any of the nation’s critical infrastructure databases were attacked and destroyed, that certainly would impact quality of life.

One expert asserted that if people wanted to know how much to spend on information security, they should calculate the cost of replacing their hard drives and databases in the event they became intentionally wiped out—then, double that estimate.8 Recently, a graduate student observed that “Cyber terrorism is a critical threat to national security and public policy. The intelligence community (IC) is at a turning point because it is difficult to catch a criminal who establishes an identity in cyberspace. Further, [we are at] a critical point in [time] for public policy because the government will have to devise regulations of electronic data transfer for public, as well as private, information that can be identified and accessed via the Internet.”9

Although some experts assert that no credible evidence exists that terrorists have initiated cyber attacks, groups, such as Hamas and Hezbollah, allegedly undertook such attacks more than a decade ago.10 “Lone wolves” have perpetrated more recent ones. The highest levels of government have emphasized the need to focus on this specter.11

What are the most vulnerable targets of cyber terrorists? What constitutes the significance of the targets and the magnitude of the threat? Does it matter what the threat is called? Does cyber terror constitute an element of computer crime?

Computer Crime

More than a half century later, not even the most prominent authorities have reached a consensus about what constitutes computer crime. According to one of the pioneers of this genre, the earliest occurrence of such abuse occurred in 1958.12 The first prosecution under federal law, the Computer Fraud and Abuse Act, Title 18, Section 1030, U.S. Code, was of Robert Tappan Morris, Jr., then a graduate student of computer science, who unleashed the so-called Internet Worm in 1988.13

Along the time continuum, this is where the line begins to blur between “conventional” computer crime and what the author refers to as cyber terror. This genus includes the Melissa Virus (1999), ILOVEYOU Virus (2001), Code Red Worm (2002), Blaster Virus (2004), and Conficker Worm (2008). These attacks differ from extortion, fraud, identify theft, and various scams, all of which certainly are malicious. However, acts of cyber terror as here defined impact society—even the nation—not just an individual, elements of the business sector, or government agencies.

Space limitations do not allow for an incident-by-incident accounting of cyber terror episodes. One example is the case of U.S. v. Mitra. In 2003, Rajib K. Mitra undertook an ongoing attack on a police emergency radio system. Initially, authorities investigated Mitra’s cyber assaults as a violation of Wisconsin state law, but, ultimately, deemed them attacks on the critical infrastructure. The case was prosecuted under federal law (Computer Fraud and Abuse Act). Mitra, a lone wolf, was tried and convicted on March 12, 2004, and later sentenced to 96 months imprisonment. Subsequently, his appeal failed. U.S. Seventh Circuit Court of Appeals judges ruled unanimously, noting that “it is impossible to fathom why any sane person would think that the penalty for crippling an emergency-communication system on which lives may depend should [not] be higher than the penalty for hacking into a Web site to leave a rude message.”14

Clearly, law enforcement agencies need to stay well informed about what the experts think. Most contemporary professionals remain cautious. However, if people wait until they have absolute proof positive, it may be too late. The cyber trends seem clear. Over the course of approximately 13 years, both the number and frequency of instances of digital disorder have intensified, and the sophistication and diversity of types of cyber attacks have increased.

One high-profile specialist contended that “stories of terrorists controlling the power grid, or opening dams, or taking over the air traffic control network and colliding airplanes, are unrealistic scare stories.” He went on to invoke a cost-benefit ratio perspective: “We need to understand the actual risks. Here’s the critical question we need to answer: Just how likely is a terrorist attack, and how damaging is it likely to be?”15 Another authority notes that “threats to the critical infrastructure are becoming increasingly frequent” and goes on to say, “Cyber attacks are one of the greatest threats to international peace and security in the 21st Century.”16 Where there is smoke, is fire not obviously far behind? And, what about the future? What technological innovations will impact the ability to serve and protect in the near-term future?

Tomorrow’s Challenges

Concerning the use of the term cyber terror, do experts resemble the proverbial blind men who feel different parts of the same elephant? On the near-term horizon, technological wonders will arise of which the unscrupulous will avail themselves, just as others before them have done.17 But, where do vulnerabilities lie, and what technological tools will terrorists use?

SCADA Systems

Not the only concern, but certainly a major worry, are supervisory control and data acquisition (SCADA) systems. Closely related are digital control systems (DCS) and programmable logic controllers (PLC). SCADA systems are more ubiquitous than personal computers and laptops combined. Without onsite human intervention, they automatically and remotely collect data from sensors in devices used for industrial processing. They store information in databases for subsequent central-site management and processing.SCADA systems have existed since the 1960s. In the early days, they were stand-alone, and few were networked. Today, virtually all are accessed via the Internet. This may be great as a cost-cutting measure, but not from an information security perspective. Quietly and without fanfare, SCADA systems have proliferated rapidly—for starters, in the electric, oil, and gas; water treatment; waste management; and maritime, air, railroad, and automobile traffic control industries. SCADA systems also are embedded in “telephone and cell phone networks, including 911 emergency services.”18

These obscure little drone-like computer systems have virtually no security, firewalls, routers, or antivirus software to protect them. They are spread far and wide across the nation, even in some of the most remote places imaginable.19 One anonymous hacker interviewed for a television program said, “SCADA is a standard approach toward control systems that pervades everything from water supply to fuel lines.” He goes on to describe that the systems run operating systems that make them vulnerable.20

Ominous Threats

Electromagnetic pulse (EMP) bombs and high-energy radio frequency (HERF) weapons differ from the malicious codes, computer viruses, and worms of yesteryear. While the latter remain worrisome, EMP and HERF are serious menacing perils of the near-term technological age. EMP devices are compact, and perpetrators can use them to overload computer circuitry. These devices can destroy a computer’s motherboard and permanently, irretrievably erase data in memory storage devices.21 Like EMPs, HERF devices use electromagnetic radiation.22 They, too, deliver heat, mechanical, or electrical energy to a target. The difference is that individuals can focus HERF devices on a specific target using a parabolic reflector.23 HERF, as asserted, does not cause permanent damage—EMP does.24 An array of demonstrations of the power of such homemade devices is depicted at several Web sources, such as YouTube.

Bots

Two decades ago, an expert warned about Internet agents, including bots (robots), Web crawlers, Web spiders, and Web scutters, software apps that traverse the Internet while undertaking repetitive tasks, such as retrieving linked pages, specified words or phrases, or e-mail addresses.25 Although bots have served benign functions—for example, harvesting e-mail addresses—for many years, they now loom large as a near-term future IC and policing issue. More recent research supports this contention. Given these forecasts, the question is not what might happen tomorrow, but, rather, how well-prepared law enforcement will be to protect and serve.

Implications for Law Enforcement

Federal agencies responsible for investigating terrorism, including cyber terror, must remain vigilant. This includes ensuring adequate funding for staffing, equipment, and training. But, beyond that, local law enforcement officers must encourage citizens to be alert and to report suspicious behavior. Many local law enforcement agencies have had useful resources, such as citizens’ police academies, for decades. These programs can educate taxpayers about activity in the physical realm that should be reported. However, what about transcendence to the virtual realm? Since 1996, the FBI’s InfraGard Program, an information sharing and analysis effort, has focused on marshaling the talents of members of America’s information security (INFOSEC) community.26 However, what of “main street USA”?

See Something, Say Something is a terrific crime prevention slogan promoted in New York City.27 It seems to have resonated recently in Times Square when an observant man, a street vendor and Vietnam veteran, alerted the New York Police Department to the SUV used in what turned out to be, fortunately, a failed Taliban-sponsored car-bombing attempt.28 Any such program should be augmented to provide to its participants examples of behavior in the business community, including those in a work environment, that could alert authorities to precursors of potential cyber misdeeds. Just as someone does not need specialized education to recognize threats in real life, anyone can recognize these digital threats. One authority notes that “an example of suspicious behavior might be a bit of malicious program attempting to install itself from opening an office document.” To reduce the threat, employees could add a “‘behavior’ layer to [antivirus products].”29 Of course, this suggestion could unnerve many civil liberty-oriented watchdog organizations; there is no reason not to include such agencies in the discussion, planning, and implementation of the augmentation here proposed. What, then, is the bottom line?

Necessary Preparations

Earthquakes, hurricanes, tsunamis, tornadoes, volcanoes, toxic spills, forest fires, and shark attacks do not occur with great frequency. Precautions, nevertheless, are in place to protect people from the physical threats posed when these natural but seldom-occurring violent events occur. Although they cannot be forecast with great accuracy, we are prepared for them. Similarly, law enforcement agencies should be prepared to deal with the aftermath of hard-to-forecast, but not regularly reoccurring, cyber attacks on the nation’s critical infrastructure.

Criminals are menacing our cyber shores, preparing to launch a large-scale attack. What is clear is that it will happen. What is not obvious is by whom or when. Respected INFOSEC authorities have made a compelling case for the “swarm”—attacks via different paths by dispersed cells. Al Qaeda already has demonstrated an understanding of the technique.30 Other countries, such as India, Saudi Arabia, China, France, Brazil, and Spain, already have experienced such attacks.31 Additionally, well-known U.S. companies have reported major breaches targeting source code.32

Cyber terrorists are pinging ports and probing our digital fortifications as they endeavor to identify vulnerabilities. Daily crackers and terrorists are skulking, battering firewalls, and learning more each time they do so. Clearly, preparations to thwart such attacks are necessary.

Conclusion

The skills, tools, and techniques are the same, but information warfare is conducted between military combatants; cyber terrorism targets civilians. Cyber terrorists indiscriminately will attack the nation’s critical infrastructure and civilians—the innocent. Thus, the context and targets, not the technological tools or frequency of attacks, are the more appropriate delimiters that distinguish cyber terror from information warfare.

Some of these criminals are being caught and prosecuted, but more remain undetected. To best serve its motto, “to protect and serve,” law enforcement must proactively guard this country’s national security on every front.

Endnotes

1 Robert Taylor, Eric Fritsch, Tory Caeti, Kall Loper, and John Liederbach, Digital Crime and Digital Terrorism (Upper Saddle River, NJ: Pearson Prentice Hall, 2011), 19.

2 Dorothy Denning, Information Warfare and Security (Reading, MA: Addison-Wesley Longman, 1999), 21.

3 Maura Conway, “Cyberterrorism: Hype and Reality,” in Information Warfare: Separating Hype from Reality, ed. E. Leigh Armistead (Washington, DC: Potomac Books, 2007), 73–93.

4 Wang Baocun and Li Fei, “Information Warfare,” Academy of Military Science, Beijing, China, http://www.fas.org/irp/world/china/docs/iw\_wang.htm (accessed October 28, 2010).

5 Denning; and Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston, MA: Little, Brown, 1993).

6 Barry Collin, ”The Future of Cyberterrorism,” Crime & Justice International Journal (March 1997): 15.

7 James Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,” Center for Strategic and International Studies, http://csis.org/files/media/csis/pubs/021101\_risks\_of\_cyberterror.pdf (accessed October 28, 2010).

8 Dr. Grace Hopper, “Future of Computing” (lectures, FBI Academy, Quantico, VA, 1985-1991). See also http://www.sdsc.edu/ScienceWomen/hopper.html (accessed October 29, 2010); http://www.youtube.com/watch?v=7sUT7gFQEsY (accessed October 29, 2010); and http://www.youtube.com/watch?v=CVMhPVInxoE&feature=related (accessed October 29, 2010).

9 Mehwish Salim, “Cyber Terror: Unequivocal Threat or Hyperbole?” (award-winning paper presentation, 34th Annual Meeting of the Northeastern Association

of Criminal Justice Sciences, Bristol, RI, June 9-12, 2010).

10 David Pettinari, “Cyber Terrorism-Information Warfare in Every Hamlet,” Police Futurist 5, no. 3 (1997): 7-8.

11 National Security Council, “The Comprehensive National Cybersecurity Initiative,” http://www.globalsecurity.org/security/library/policy/national/cnci\_2010.htm (accessed October 29, 2010); and CBS, “Sabotaging the System,” 60 Minutes, http://video.techrepublic.com.com/2422-13792\_11-364499.html (accessed October 29 2010).

12 Donn Parker, Crime by Computer (New York, NY: Charles Scribner’s Sons, 1976).

13 Ronald Standler, “Computer Crime,” http://www.rbs2.com/ccrime.htm (accessed October 29, 2010).

14 U.S. v. Mitra 04-2328.

15 Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World (New York, NY: Copernicus Books, 2003).

16 Jeffrey Carr, Inside Cyber Warfare (Sebastopol, CA: O’Reilly, 2010).

17 For more information, visit http://www.battelle.org.

18 Gregory Coates, “Collaborative, Trust-Based Security Mechanisms for a National Utility Intranet” (master’s thesis, Air Force Institute of Technology, 2007).

19 William Graham, Chairman, Critical National Infrastructures, “Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,” EMP Commission, http://empcommission.org/docs/A2473-EMP\_Commission-7MB.pdf (accessed October 29, 2010); Seth Fogie, “SCADA and Security,” http://www.informit.com/guides/content.aspx?g=security&seqNum=322 (accessed October 29, 2010); and Seth Fogie, “SCADA In-Security,” http://www.informit.com/guides/content.aspx?g=security&seqNum=323 (accessed October 29, 2010).

20 Tom Longstaff, “Cyberwar: Vulnerability of Scada Systems?” http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/scada.html (accessed October 29, 2010).

21 Graham.

22 For additional information, see http://www.lbl.gov/MicroWorlds/ALSTool/EMSpec/ (accessed October 29, 2010).

23 For additional information, see http://www.wordiq.com/definition/Parabolic\_reflector (accessed October 29, 2010).

24 John Geis, “Directed Energy Weapons of the Battlefield: A New Vision for 2025” (paper, Center for Strategy and Technology, Air War University, Maxwell Air Force Base, Alabama, 2003).

25 Kevin Manson, “Robots, Wanderers, Spiders and Avatars: The Virtual Investigator and Community Policing Behind the Thin Digital Blue Line” (presentation, annual meeting of the Academy of Criminal Justice Sciences, Louisville, KY, March 15, 1997).

26 For more information, visit http://www.infragard.net.

27 For more information, visit http://www.mta.info/mta/security/index.html.

28 “President Calls to Thank Times Square Vendor,” Associated Press, May 2, 2010; and Anne Komblut,“Pakistani Taliban Behind Attempted Times Square Car Bombing, Attorney General Says,” Washington Post, May 9, 2010.

29 Frances Alonzo, “Security Expert Urges Shift in Tactics Against Cyber Attacks,” http://it.moldova.org/news/

security-expert-urges-shift-in-tactics-against-cyber-attacks-206747-eng.html (accessed October 29, 2010).

30 John Arquilla and David Ronfeldt, Swarming and the Future of Conflict (Santa Monica, CA: RAND, 2000); and John Arquilla and David Ronfeldt, “Fighting the Network War,” Wired 9, no. 12 (2001).

31 Kim Zetter, “Google Hackers Targeted Source Code of More Than 30 Companies,” http://www.wired.com/threatlevel/2010/01/google-hack-attack/ (accessed October 29, 2010).

32 Kim Zetter, “Report: Critical Infrastructures Under Constant Cyberattack Globally” http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/ (accessed October 29, 2010).

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

First Look: Electronic Warfare Missile

By David Fulghum, [Aviation Week](http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/awst/2011/11/21/AW_11_21_2011_p29-395318.xml&headline=First%20Look:%20Electronic%20Warfare%20Missile), 22 Nov 2011

The U.S. has built, flown, pointed and triggered a missile designed specifically to carry a directed-energy weapon. That payload, expected to be operational soon, will be able to disrupt, shut down, spoof or damage electrical systems, but little has been revealed about the project.

However, various clues have provided substantive details about the design and concept of operations (conops) for the new missile and its exotic payload. They come from Boeing officials, industry specialists and U.S. Air Force Research Laboratory sponsors who are working on the Counter-electronics High-power Microwave Advanced Missile Project (Champ).

An illustration created by Boeing shows the missile being dropped by a B-52, which means at least some versions of the design are air-launched. However, the directed-energy, high-power microwave (HPM) payload also is designed for integration into land, sea or other air-based platforms for operational flexibility.

As to the warhead’s anti-electronics capabilities, “the whole radio frequency spectrum is viable as a target,” says Keith Coleman, Boeing’s program manager for Champ since 2009. The systems will be tailored to the target defined by the customer. The effects will depend on the frequency and effective radiated power (ERP). There are many options.

Two short video clips produced by the Air Force—without sound or annotation—indicate the conops and effects. An animation shows a cruise missile flying at low altitude firing beams of HPM from side- and downward-pointed apertures at high-rise office buildings in a city. The lights go off as the buildings are attacked. An actual video shows a room with about a half-dozen desktop computers functioning with data on the screens. Suddenly all the computers go black, with one momentarily turning back on and then off again.

That still leaves two unanswered questions—is Champ stealthy and reusable?

The notional airframe shown in Boeing’s drawings is relatively small with compressed carriage wings that extend after launch. While Boeing’s artist concepts are not exact representations of the missile, they do resemble the company’s cruise missile designs that are similarly air-launched and have low-radar-signature designs to penetrate enemy air defenses.

“Any of these systems can be made to be recoverable or otherwise,” Coleman says. “There are many proven methods of recovering vehicles from the lightweights to the heavier designs.”

Champ was first flown on May 17 at the Utah Test and Training Range at Hill AFB. The missile was successfully pointed at a series of targets to confirm that it could be controlled and timed to fire a focused beam that would minimize—and perhaps eliminate—collateral damage to nearby electronic devices. The software used in the test was identical to that required to trigger the HPM weapon warhead.

Cruise missiles are valued for their intrinsic low radar cross-section that comes with small size, and they can be shaped and treated with radar-absorbing or reflecting materials. That is why they are the primary tools for breaking down enemy air defenses on the first day of any conflict. A Champ-like design would be sure to have the same operational requirements and need for stealth. Nonetheless, HPM payloads are not restricted to Champ.

“Any unmanned aircraft would be a candidate for these types of systems,” Coleman says. However, “Boeing built the Champ system to be easily transitioned to [alternative platforms]. From the start we designed it with as many features as possible so that we would need minimum adjustments.”

Program officials will not address the question of whether Champ is associated with the Air Force’s Long-Range Strike (LRS) program. Air Force and aerospace industry officials have said that directed-energy weapons support and electronic attack will be supplied to LRS by adjunct, unmanned aircraft.

“Champ is a template for future HPM programs,” Coleman says. “There has never been this type of system with this kind of power out on any vehicle of any sort before.”

Coleman contends there would be little difficulty putting the HPM weapons technology on a smaller or larger airframe.

“The HPM system itself is a very flexible integration,” he says. If smaller, you get less ERP and if bigger you get more. But if you are smaller, you can probably get closer [to the target without being detected]. I absolutely think there is a desire to go to a bigger airframe. ERP is dependent on the size of the aperture. The bigger the aperture, the more power you can produce and the more standoff you get.”

The initial version of Champ is designed for a relatively small, unmanned aircraft, Coleman says, so “that was part of the difficulty of getting everything to fit.”

Boeing’s Phantom Works built the missile airframe and the weapon pointing system, drawing on its experience with advanced weapons, cruise missiles and unmanned strike aircraft in conjunction with the Air Force Research Laboratory.

Coleman worked on the Calcm and Jassm cruise missiles, the F-15E and F/A-18E/F strike fighters and X-45A/C unmanned combat aircraft projects that prepared him for leading a very specialized team that integrated the sophisticated directed-energy weapon payload into the unmanned platform. There are about 25 core members from the various companies involved in the program providing missile and aircraft program experience.

Raytheon’s newly acquired New Mexico-based Ktech division built the HPM warhead. The combination of airframe and warhead are to be demonstrated during a series of flight tests planned to cluster around the end of the current program in July 2012.

Raytheon recently acquired Ktech because it is making plans to build a series of HPM warheads for virtually all the missile models on its various production lines. A few years ago Raytheon planners said they were “betting the farm” on HPM pushing aside lasers as the most tactically useful and least demanding directed-energy weapon for next-generation combat operations. Boeing, in a complementary mode, has been designing its unmanned combat aircraft designs to carry reusable, multi-shot HPM weapons.

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)

U.S. Works to Counter Electronic Spy Risks

By Siobhan Gorman, [Wall Street Journal](http://online.wsj.com/article/SB10001424052970203733504577022010229695028.html), November 11, 2011

The Obama administration is quietly working to counter potential risks posed by foreign telecommunications companies' expansion in the U.S. market, which federal officials say they fear could make the nation vulnerable to spying.

The initiative, previously unreported, doesn't target a particular company or country, but China remains a focus of U.S. government concerns about electronic spying. And a key impetus for the new initiative is the U.S. expansion of Chinese telecommunications company Huawei Technologies Co., according to people familiar with the White House deliberations.

The effort looks "broadly at the opportunities, risks and implications of reliance on global, commercial markets," said Caitlin Hayden, a White House spokeswoman. The bulk of the U.S. telecommunications backbone is foreign-made—Canadian, French and Chinese—said one industry specialist.

Huawei says it welcomes Washington's focus on telecommunications security. U.S. officials haven't provided evidence of any wrongdoing on the part of Huawei.

The U.S. government accused the Chinese of being the world's "most active and persistent" perpetrators of economic espionage. Siobhan Gorman has details on The News Hub.

Huawei is a rapidly growing, closely held Chinese firm that has sold telecommunications equipment—including landline, wireless and radio networks—to more than a dozen small U.S. carriers in rural areas as well as metro areas like Chicago, said Huawei's U.S. external-affairs chief, William Plummer. Its sales revenue from North America was $772 million in 2010. Huawei is now the second-largest telecommunications-equipment provider in the world by sales after Sweden's Telefon AB L.M. Ericsson.

As American telecommunications companies integrate Huawei equipment into their systems, U.S. officials worry the Chinese government could access that equipment and track phone calls or emails, or disrupt or destroy a communications system. That access could also provide an avenue for eavesdropping on phone calls or intercepting emails in combination with other technologies, said James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies, a Washington think tank.

Huawei was singled out in a Pentagon report earlier this year for maintaining "close ties" with China's People's Liberation Army. The report didn't provide additional details. The company was founded by former People's Liberation Army officer Ren Zhengfei. An unclassified U.S. intelligence report dated Oct. 5 said the chairwoman of Huawei previously worked at the Ministry of State Security and used her connections there to help Huawei through financial problems.

Huawei isn't a vehicle for Chinese spying, and allegations of connections to the Chinese military are unfounded, Mr. Plummer said. Huawei has an "impeccable network security record," he added. He also denied that Huawei's chairwoman worked for the Ministry of State Security.

Chinese embassy spokesman Wang Baodong said, "It's normal and understandable for the various countries to bolster telecom supply chain security." He added that China and the U.S. have shared interests in upgrading infrastructure, cautioning that "mutual trust is good for our bilateral collaboration, while distrust and [an] illegitimate, suspicious mindset are harmful."

As part of the White House initiative, a task force is assessing security risks and ways to reduce them. The task force is also examining the dependence of U.S. government and economic operations on networks that rely on equipment from foreign companies, according to a letter written by White House cybersecurity chief Howard Schmidt.

The task force has mounted an intense information-collection effort, compelling roughly 900 U.S. telecommunications companies to respond to more than 50 pages of detailed questions about the security of their networks, according to another industry specialist. That information is still being analyzed, officials said.

The information requirement, issued by the Commerce Department, invoked a 60-year-old law that compelled company officials to respond or face jail time. "It was the right tool to collect the data we need," a senior Pentagon official said, because it ensured the government would get the information quickly.

That forceful approach, however, didn't sit well with the companies. "The information they're asking for, just the collection of it creates a security problem if that information is stolen or is Wikileaked," said an industry specialist.

In addition, a committee under the office of the U.S. Trade Representative is looking at ways to manage issues of fair competition from foreign telecommunications concerns. One consideration is whether the U.S. can block acquisitions or sales of foreign telecommunications equipment to protect U.S. networks, according to a person familiar with the initiative.

The initiative underscores U.S. government concerns that greater access by foreign government-affiliated companies to U.S. systems offers the foreign governments enhanced monitoring capabilities within the U.S., cybersecurity specialists said.

"We now find ourselves completely dependent on foreign suppliers for some crucial telecommunications technology, and that creates a huge new vulnerability," said James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies, a Washington think tank. "The company driving the concerns in this round is Huawei."

At least three major Huawei projects have been scuttled by potential partners after U.S. officials raised general national-security concerns, which the officials decline to detail publicly. In addition, the Commerce Department in September barred Huawei from helping build a national wireless network for emergency responders. The department cited national security concerns but didn't provide details.

Lawmakers, spurred by repeated intelligence agency warnings about Huawei, have been pressuring the Obama administration to implement stronger telecom-security measures.

"All aspects of our economy and government operations rely on the security of our nation's telecommunications network," said Michigan Rep. Mike Rogers, Republican chairman of the House intelligence committee. "Until we get more clarity on whether Huawei has ulterior motives, I urge companies doing business with Huawei to think twice in light of the national security risk."

[[Table of Contents](#_Table_of_Contents)](file:///D%3A%5CMy%20Documents%5CNewsletter%2009-08%5C0908Information%20Operations.doc#_Table_of_Contents)