GlobalResearch
Center for Research on Globalization

Finding the 'Cure' for the 'Cyber Epidemic'

By Tom Burghardt
Global Research, October 31, 2010
Antifascist Calling... 31 October 2010

Region: USA
Theme: Police State & Civil Rights

As the "War on Terror" morphs into a multiyear, multitrillion dollar blood-soaked adventure to secure advantage over imperialism's geopolitical rivals (and steal other people's resources in the process), hitting the corporate "sweet spot," now as during the golden days of the Cold War, is as American as a preemptive war and the "pack of lies" that launch them.

Always inventive when it comes to ginning-up a profitable panic, U.S. defense and security grifters have rolled-out a product line guaranteed to scare the bejesus out of everyone: a "cyber epidemic"!

This one has it all: hordes of crazed "communist" Chinese hackers poised to bring down the power grid; swarthy armies of al-Qaeda fanatics who "hate us for our freedom;" "trusted insiders" who do us harm by leaking "sensitive information," i.e. bringing evidence of war crimes and corporate malfeasance to light by spilling the beans to secrecy-shredding web sites like **WikiLeaks**, **Public Intelligence** and **Cryptome**.

And to combat this latest threat to public order, the Pentagon's geek squad, the Defense Advanced Research Projects Agency (**DARPA**) have launched several new initiatives.

Armed with catchy acronyms like **SMITE**, for "Suspected Malicious Insider Threat Elimination," and a related program, **CINDER**, for "Cyber Insider Threat," the agency's masters hope to "greatly increase the accuracy, rate and speed with which insider threats are detected and impede the ability of adversaries to operate undetected within government and military interest networks."

Just another day in our collapsing American Empire!

During an Executive Leadership Conference last week in Williamsburg, Virginia, deep in the heart of the Military-Industrial-Security corridor, Bob Dix, vice president for U.S. government and critical infrastructure protection for Juniper Networks cautioned that the United States is facing a "cyber epidemic."

According to ***Government Computer News***, Dix told the contract-hungry hordes gathered at the American Council for Technology/Industry Advisory Council's (**ACT-IAC**) conclave that "overall cyber defense isn't strong enough."

All the more reason then for the secret state to *weaken* encryption standards that might help protect individual users and critical infrastructure from malicious hacks and network intrusions, as the Obama administration will soon propose.

As I **reported** earlier this month, along with watering-down those standards, the

administration is seeking authority from Congress that would force telecommunication companies to redesign their networks to more easily facilitate internet spying.

Add to the mix the recent "**Memorandum of Agreement**" between the National Security Agency and the Department of Homeland Security that will usher in a "synchronization of current operational cybersecurity efforts," and it's a sure bet as I **averred**, that the Pentagon has come out on top in the intramural tussle within the security apparat.

During the ACT-IAC **conference**, greedily or lovingly sponsored (you make the call!) by "Platinum" angels AT&T, CACI, HP, Harris Corp. and Lockheed Martin, Sherri Ramsay, the director of NSA's Threat Operations Center, told the crowd: "Right now, we're a soft target, we're very easy."

Dix chimed in: "Nothing we're talking about today is new. What's new is the threat is more severe."

Music to the ears of all concerned I'm sure, considering the "cumulative market valued at $55 billion" over the next five years and the 6.2% annual growth rate in the "U.S. Federal Cybersecurity Market" that ***Market Research Media*** told us about.

Never mind that the number of "incidents of malicious cyber activity" targeting the Defense Department has actually *decreased* in 2010, as security journalist Noah Shachtman reported in ***Wired***.

If we were inclined to believe Pentagon claims or those of "former intelligence officials" (we're not) that the United States faces an "unprecedented threat" from imperial rivals, hackers and terrorists, then perhaps (just for the sake of argument, mind you) their overwrought assertions and fulsome pronouncements *might* have some merit.

After all, didn't NSA and U.S. Cyber Command director, General Keith Alexander tell the U.S. Senate during confirmation hearings in April that he was "alarmed by the increase, especially this year" in the number of breaches of military networks?

And didn't former Director of National Intelligence Mike McConnell, currently a top executive with the spooky Booz Allen Hamilton firm, whose cyber portfolio is well-watered with taxpayer dollars, pen an alarmist screed in ***The Washington Post*** claiming that "the United States is fighting a cyber-war today, and we are losing"?

Not to be outdone in the panic department, Deputy Defense Secretary William J. Lynn warned in a recent piece in the Council On Foreign Relations flagship publication, ***Foreign Affairs***, that "the frequency and sophistication of intrusions into U.S. military networks have increased exponentially," and that "a rogue program operating silently, [is] poised to deliver operational plans into the hands of an unknown adversary."

Oh my!

However, as Shachtman points out, "according to statistics compiled by the **U.S.-China Economic and Security Review Commission** … the commission notes in a draft report on China and the internet, '2010 could be the first year in a decade in which the quantity of logged events declines'."

Better hush that up quick or else those government contractors "specializing in the most attractive niche segments of the market" as ***Washington Technology*** averred earlier this month, might see the all-important price per share drop, a *real* national crisis!

Panic sells however, and once the terms of the debate have been set by interested parties out to feather their nests well, it's off to the races!

After all as ***Defense Systems*** reported, "as cyberspace gains momentum the military must adjust its approach in order to take on an increasingly high-tech adversary."

Indeed, Major General Ed Bolton, the Air Force point man heading up cyber and space operations thundered during a recent **meet-and-greet** organized by the Armed Forces Communications Electronics Association at the Sheraton Premier in McClean, Virginia that "we are a nation at war, and cyberspace is a warfighting domain."

Along these lines the Air Force and CYBERCOM are working out "the policy, doctrine and strategies" that will enable our high-tech warriors to integrate cyber "in combat, operation plans and exercises," Bolton explained.

And according to Brigadier General Ian Dickinson, Space Command's CIO, industry will "help the military take on an evolving war strategy–and [close] a gap between traditional and cyber-era defense," *Defense Systems* informed us.

"That's something we worry about," Space Command's Col. Kim Crider told AFCEA, perhaps over squab and a lobster tail or two, "integrating our non-kinetic capabilities with space operations."

"We think it's a good opportunity to partner with industry to develop and integrate these capabilities," Crider said, contemplating perhaps his employment opportunities after retiring from national service.

And why not, considering that AFCEA's board of directors are chock-a-block with executives from cyberfightin' firms like Booz Allen, SAIC, Raytheon, Northrop Grumman, Boeing and General Dynamics.

Perhaps too, the generals and full bird colonels on the Sheraton dais need reminding that "integrating our non-kinetic capabilities with space operations," has already been a matter of considerable import to U.S. Strategic Command's Gen. Kevin Chilton.

In 2009, the STRATCOM commander informed us that "the White House retains the option to respond with physical force–potentially even using nuclear weapons–if a foreign entity conducts a disabling cyber attack against U.S. computer networks."

That would certainly up the ante a notch or two!

Chilton said, "I think you don't take any response options off the table from an attack on the United States of America," ***Global Security Newswire*** reported. "Why would we constrain ourselves on how we respond?"

Judging by the way the U.S. imperial war machine conducts itself in Iraq and Afghanistan, there's no reason that the general's bellicose rhetoric shouldn't be taken seriously.

“I think that’s been our policy on any attack on the United States of America,” Chilton said. “And I don’t see any reason to treat cyber any differently. I mean, why would we tie the president’s hands? I can’t. It’s up to the president to decide.”

Even short of nuclear war a full-on cyber attack on an adversary’s infrastructure could have unintended consequences that would boomerang on anyone foolish enough to unleash military-grade computer worms and viruses.

All the more reason then to classify *everything* and move towards transforming the internet and electronic communications in general into a “warfighting domain” lorded-over by the Pentagon and America’s alphabet-soup intelligence agencies.

As ***The Washington Post*** reported on September 29, the secret state announced that “it had spent $80.1 billion on intelligence activities over the past 12 months.”

According to the *Post*, the “National Intelligence Program, run by the CIA and other agencies that report to the Director of National Intelligence, cost $53.1 billion in fiscal 2010, which ended Sept. 30, while the Military Intelligence Program cost an additional $27 billion.”

By comparison, the total spent by America’s shadow warriors exceeds Russia’s *entire* military budget.

Despite releasing the budget figures, the Office of Director and National Intelligence and Defense Department officials refused to disclose any program details.

What percentage goes towards National Security Agency “black” programs, including those illegally targeting the communications of the American people are, like torture and assassination operations, closely guarded state secrets.

And with calls for more cash to “inoculate” the American body politic against a looming “cyber epidemic,” the right to privacy, civil liberties and dissent, are soon destined to be little more than quaint relics of our former republic.

As security expert Bruce Schneier **points out** “we surely need to improve cybersecurity.” However, “words have meaning, and metaphors matter.”

> “If we frame the debate in terms of war” Schneier writes, “we reinforce the notion that we’re helpless–what person or organization can defend itself in a war?–and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime.”

As well, using catchy disease metaphors like “epidemic” to describe challenges posed by high-tech espionage and cyber crime evoke disturbing parallels to totalitarian states of the past.

Such formulas are all the more dangerous when the “antibodies” proposed by powerful military and corporate centers of power will be deployed with little in the way of democratic oversight and control and are concealed from the public behind veils of “national security” and “proprietary business information.”

Tom Burghardt *is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and* ***Global Research****, an , his articles can be read on* ***Dissident Voice****,* ***The Intelligence Daily****,* ***Pacific Free Press****,* ***Uncommon Thought Journal****, and the whistleblowing website* ***WikiLeaks****. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press*** *and has contributed to the new book from* ***Global Research****, The Global Economic Crisis: The Great Depression of the XXI Century.*

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/