


Cyberwar Hype Intended to Destroy the Open Internet

By [Ryan Singel](#)  March 1, 2010 | 6:56 pm | Categories: [Cybarmageddon!](#)



The biggest threat to the open internet is not Chinese government hackers or greedy anti-net-neutrality ISPs, it's Michael McConnell, the former director of national intelligence.

McConnell's not dangerous because he knows anything about SQL injection hacks, but because he knows about social engineering. He's the nice-seeming guy who's willing and able to use fear-mongering to manipulate the federal bureaucracy for his own ends, while coming off like a straight shooter to those who are not in the know.

When he was head of the country's national intelligence, he [scared President Bush with visions of e-doom](#), prompting the president to sign a comprehensive secret order that unleashed tens of billions of dollars into the military's black budget so they could start making firewalls and building malware into military equipment.

And now McConnell is back in civilian life as a vice president at the secretive defense contracting giant [Booz Allen Hamilton](#). He's out in front of Congress and the media, peddling the same [Cybaremageddon!](#) gloom.

And now he says we need to *re-engineer* the internet.

We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options — and we must be able to do this in milliseconds. *More specifically, we need to re-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable.* The technologies are already available from public and private sources and can be further developed if we have the will to build them into our systems and to work with our allies and trading partners so they will do the same.

Re-read that sentence. He's talking about changing the internet to make everything anyone does on the net traceable and geo-located so the National Security Agency can pinpoint users and their computers for retaliation if the U.S. government doesn't like what's written in an e-mail, what search terms were used, what movies were downloaded. Or the tech could be useful if a computer got hijacked without your knowledge and used as part of a botnet.

The Washington Post gave McConnell free space to declare that we are [losing some sort of cyberwar](#). He argues that the country needs to get a Cold War strategy, one complete with the online equivalent of ICBMs and Eisenhower-era, secret-codenamed projects. Google's allegation that Chinese hackers infiltrated its Gmail servers and targeted Chinese dissidents proves the United States is "losing" the cyberwar, according to McConnell.

But that's not warfare. That's espionage.

McConnell's op-ed then pointed to breathless stories in *The Washington Post* and *The Wall Street Journal* about thousands of malware infections from the well-known Zeus virus. He intimated that the nation's citizens and corporations were under unstoppable attack by this so-called new breed of hacker malware.

despite the masterful PR about the Zeus infections from security company NetWitness (run by a former Bush Administration cyberczar Amit Yoran), the world's largest security companies McAfee and Symantec downplayed the story. But the message had already gotten out — the net was under attack.

Brian Krebs, one of the country's most respected cybercrime journalists and occasional Threat Level contributor, [described](#) that report: "Sadly, this botnet documented by NetWitness is neither unusual nor new."

Those enamored with the idea of "cyberwar" aren't dissuaded by fact-checking.

They like to point to Estonia, where a number of the government's websites were rendered temporarily inaccessible by angry Russian citizens.

They used a crude, remediable denial-of-service attack to temporarily keep users from viewing government websites. (This attack is akin to sending an army of robots to board a bus, so regular riders can't get on. A website fixes this the same way a bus company would — by keeping the robots off by identifying the difference between them and humans.) Some like to say this was an act of cyberwar, but [if it that was cyberwar](#), it's pretty clear the net will be just fine.

In fact, none of these examples demonstrate the existence of a cyberwar, let alone that we are losing it.

But this battle isn't about truth. It's about power.

For years, McConnell has wanted the NSA (the ultra-secretive government spy agency responsible for listening in on other countries and for defending *classified* government computer systems) to take the lead in guarding all government and private networks. Not surprisingly, the contractor he works for has massive, secret contracts with the NSA in that very area. In fact, the company, [owned by the shadowy Carlyle Group](#), is reported to pull in \$5 billion a year in government contracts, many of them Top Secret.

Now the problem with developing cyberweapons — say a virus, or a massive botnet for denial-of-service attacks, is that you need to know where to point them. In the Cold War, it wasn't that hard. In theory, you'd use radar to figure out where a nuclear attack was coming from and then you'd shoot your missiles in that general direction. But online, it's extremely difficult to tell if an attack traced to a server in China was launched by someone Chinese, or whether it was actually a teenager in Iowa who used a proxy.

That's why McConnell and others want to change the internet. The military needs targets.

But McConnell isn't the only threat to the open internet.

Just last week the National Telecommunications and Information Administration — the portion of the Commerce Department that has long overseen the Internet Corporation for Assigned Names and Numbers — said it was time for it to revoke its hands-off-the-internet policy.

That's according to a [February 24 speech](#) by Assistant Commerce Secretary Lawrence E. Strickling.

In fact, "leaving the Internet alone" has been the nation's internet policy since the internet was first commercialized in the mid-1990s. The primary government imperative then was just to get out of the way to encourage its growth. And the policy set forth in the Telecommunications Act of 1996 was: "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."

This was the right policy for the United States in the early stages of the Internet, and the right message to send to the rest of the world. But that was then and this is now.

Now the NTIA needs to start being active to prevent cyberattacks, privacy intrusions and copyright violations, according to Strickling. And since NTIA serves as one of the top advisers to the president on the internet, that stance should not be underestimated.

Add to that — a bill looming in the Senate would [hand the president emergency powers over the internet](#) — and you can see where all this is headed. And let the past be our guide.

Following years of the NSA illegally spying on Americans' e-mails and phone calls as part of a secret anti-terrorism project, Congress voted to legalize the program in July 2008. That vote allowed the NSA to legally turn America's portion of the internet into a giant listening device for the nation's intelligence services. The new law also gave legal immunity to the telecoms like AT&T that helped the government illegally spy on American's e-mails and internet use. Then-Senator Barack Obama voted for this legislation, despite earlier campaign promises to oppose it.

As anyone slightly versed in the internet knows, the net has flourished because no government has control over it.

But there are creeping signs of danger.

Where can this lead? Well, consider England, where a new bill targeting online file sharing will [outlaw open internet connections at cafes](#) or at home, in a bid to track piracy.

To be sure, we could see more demands by the government for surveillance capabilities and backdoors in routers and operating systems. Already, the feds successfully turned the Communications Assistance for Law Enforcement Act (a law mandating surveillance capabilities in telephone switches) into a tool requiring ISPs to build similar government-specified eavesdropping capabilities into their networks.

The NSA dreams of "living in the network," and that's what McConnell is calling for in his editorial/advertisement for his company. The NSA lost any credibility it had when it secretly violated American law and its most central tenet: "We don't spy on Americans."

Unfortunately, the private sector is ignoring that tenet and is helping the NSA and contractors like Booz Allen Hamilton worm their way into the innards of the net. Security companies make no fuss, since a scared populace and fear-induced federal spending means big bucks in bloated contracts. Google is no help either, recently turning to the NSA for help with its rather routine infiltration by hackers.

Make no mistake, the military industrial complex now has its eye on the internet. Generals want to train crack squads of hackers and have wet dreams of cyberwarfare. Never shy of extending its power, the military industrial complex wants to turn the internet into yet another venue for an arms race.

And it's waging a psychological warfare campaign on the American people to make that so. The military industrial complex is backed by sensationalism, and a gullible and pageview-hungry media. Notable examples include the *New York Times*'s John "We Need a New Internet" Markoff, *60 Minutes*' "Hackers Took Down Brazilian Power Grid," and the *WSJ*'s Siobhan Gorman, who ominously warned in an a piece lacking any verifiable evidence, that Chinese and Russian hackers are already [hiding inside the U.S. electrical grid](#).

Now the question is: Which of these events can be turned into a Gulf of Tonkin-like fakery that can create enough fear to let the military and the government turn the open internet into a controlled, surveillance-friendly net.

What do they dream of? Think of the internet turning into a tightly monitored AOL circa the early '90s, run by CEO Big Brother and COO Dr. Strangelove.

That's what McConnell has in mind, and shame on *The Washington Post* and the [Senate Commerce, Science and Transportation Committee](#) for giving McConnell venues to try to make that happen — without highlighting that McConnell has a serious financial stake in the outcome of this debate.

Of course, the net has security problems, and there are pirated movies and spam and botnets trying to steal credit card information.

But the online world mimics real life. Just as I know where online to buy a replica of a Coach handbag or watch a new release, I know exactly where I can go to find the same things in the city I live in. There are cons and rip-offs in the real world, just as there are online. I'm more likely to get ripped off by a restaurant server copying down the information on my credit card than I am having my card stolen and used for fraud while shopping online. "Top Secret" information is more likely to end up in the hands of a foreign government through an employee-turned-spy than from a hacker.

But cyber-anything is much scarier than the real world.

The NSA can help private companies and networks tighten up their security systems, as McConnell argues. In fact, they already do, and they should continue passing along advice and creating guides to locking down servers and releasing their own secure version of Linux. But companies like Google and AT&T have no business letting the NSA into their networks or giving the NSA information that they won't share with the American people.

Security companies have long relied on creating fear in internet users by hyping the latest threat, whether that be [Conficker](#) or the latest PDF flaw. And now they are reaping billions of dollars in security contracts from the federal government for their PR efforts. But the industry and its most influential voices need to take a hard look at the consequences of that strategy and start talking truth to power's claims that we are losing some non-existent cyberwar.

The internet is a hack that seems forever on the edge of falling apart. For awhile, spam looked like it was going to kill e-mail, the net's first killer app. But smart filters have reduced the problem to a minor nuisance as anyone with a Gmail account can tell you. That's how the internet survives. The apocalypse looks like it's coming and it never does, but meanwhile, it becomes more and more useful to our everyday lives, spreading innovation, weird culture, news, commerce and healthy dissent.

But one thing it hasn't spread is "cyberwar." There is no cyberwar and we are not losing it. The only war going on is one for the soul of the internet. But if journalists, bloggers and the security industry continue to let self-interested exaggerators dominate our nation's discourse about online security, we will lose that war — and the open internet will be its biggest casualty.

UPDATE: In an interesting coincidence, the Obama administration unclassified on Tuesday portions of the secret [Comprehensive National Cybersecurity Initiative](#) it inherited from President Bush, including unclassified summaries all of the 12 initiatives. Note the veiled references to deterrence. See Threat Level's [report from the RSA conference](#) on the release.

Photo: Michael McConnell, then-Director of National Intelligence, watches on in 2008 as President Bush announced the Protect America Act. White House file photo.

See Also:

- [Massive Wave of Estonia Cybarmageddon Debunking Begins](#)
- [Estonia DDoS Attacks Make Tech Reporters Into Daring War Correspondents](#)
- ['Cyberwar' and Estonia's Panic Attack](#)
- [Did Hackers Cause the 2003 Northeast Blackout? Umm, No](#)
- [No Chinese Hackers Found in Florida Outage Either](#)
- [Brazilian Blackout Traced to Sooty Insulators, Not Hackers ...](#)
- [Conficker War Room! Your Front Row Seat For Cyber Armageddon](#)
- [NSA Must Examine All Internet Traffic to Prevent Cyber Nine-Eleven ...](#)
- [Put NSA in Charge of Cyber Security, Or the Power Grid Gets It ...](#)
- [Google Asks NSA to Help Secure Its Network](#)

Tags: [cyberwar](#), [Michael McConnell](#), [NSA](#)
[Post Comment](#) | [Permalink](#)

Also on [Wired.com](#)

- [AT&T Sees iPad as Wi-Fi Driven, Not a 3G Hog](#)
- [GM Ditches an Electric Cadillac For a Plug-In Cadillac](#)
- [First Mirrors Polished for Next-Gen Space Telescope](#)
- [Flipping Off Cops Is Legal, Not Advised](#)
- [Google's China Exit Strategy: Watch This Space](#)
- [U.S. Declassifies Part of Secret Cybersecurity Plan](#)

Related Topics:

- [Computer Security](#),
- [Computer Technology](#),
- [Internet](#),
- [Michael McConnell](#),
- [Science and Technology](#),
- [Technology](#)

Comments (64)

Posted by: DikShuttle | 03/2/10 | 1:34 pm |

And since corps are taking over govts... the net will now be entirely corporate.

...as I've said from the beginning. Shoulda kept corps outta da net. BBS only! hehe.

Posted by: benaround | 03/2/10 | 2:22 pm |

lol. now I remember why I read wired.

comic relief 😊

“what a maroon” bugs bunny

Posted by: foremski | 03/2/10 | 3:48 pm |

Excellent post. And very scary. I'm not given to conspiracies but it wouldn't be difficult for vested interests to create attacks, maybe leave a few clues leading to Chinese hackers, for example, and then argue for greater controlling measures over the Internet.

Posted by: markcu2234 | 03/2/10 | 4:14 pm |

Please.....the “HYPER” is this article itself. Do you see people watching you all the time as you craft these flights of imagination?

The hyperbole of this article is that all efforts of the U.S. Govt is to serve as an agent of evil who seeks to know and see all as they violate the rights of every American on the Internet.....please.....I want some level of Government regulation of the Internet. Don't confuse regulation with the loss of freedom. In order to maintain some semblance of order, the net needs structure to ensure that those who take advantage of others through cyber crime and other malicious acts can be brought to justice.

Posted by: Ryan Singel | 03/2/10 | 4:41 pm |

@markcu2234 - The point isn't that malicious hackers should be free from prosecution. And the world is getting better at prosecuting carders and botnet herders. The point is we can do that without turning the net into yet another platform for an arms race.
