GlobalResearch
Center for Research on Globalization

“Emergency Control” of the Internet

By Tom Burghardt
Global Research, August 30, 2009
Antifascist Calling 30 August 2009

Region: USA
Theme: Police State & Civil Rights

You have to hand it to congressional Democrats. Mendacious grifters whose national security agenda is virtually indistinguishable from Bushist Republicans, when it comes to rearranging proverbial deck chairs on the Titanic, the party of “change” is second to none in the “all terrorism all the time” department.

While promising to restore the “rule of law,” “protect civil liberties” while “keeping America safe,” in practice, congressional Democrats like well-coiffed Republican clones across the aisle, are crafting legislation that would do Dick Cheney proud!

As the Cybersecurity Act of 2009 (**S.773**) wends its way through Congress, civil liberties’ advocates are decrying provisions that would hand the President unlimited power to disconnect private-sector computers from the internet.

CNET **reported** August 28, that the latest iteration of the bill “would allow the president to ‘declare a cybersecurity emergency’ relating to ‘non-governmental’ computer networks and do what’s necessary to respond to the threat.”

Drafted by Senators Jay Rockefeller (D-WV) and Olympia Snowe (R-ME), “best friends forever” of the National Security Agency (NSA) and the telecommunications industry, they were key enablers of Bush-era warrantless wiretapping and privacy-killing data mining programs that continue apace under Obama.

As *The New York Times* **revealed** in June, a former NSA analyst described a secret database “code-named Pinwale, that archived foreign and domestic e-mail messages.” The former analyst “described being trained in 2005 for a program in which the agency routinely examined large volumes of Americans’ e-mail messages without court warrants. Two intelligence officials confirmed that the program was still in operation.”

Antifascist Calling has noted on more than one occasion, that with “cyberterrorism” morphing into al-Qaeda 2.0, administration policies designed to increase the scope of national security state surveillance of private communications will soon eclipse the intrusiveness of Bushist programs.

As Cindy Cohn, the Legal Director of the Electronic Frontier Foundation (**EFF**) **wrote** earlier this month, commenting on this summer’s public relations blitz by former NSA boss Michael Hayden and Office of Legal Counsel torture-enabler John Yoo’s defense of the so-called Presidential Surveillance Program,

While the details are unknown, credible evidence indicates that billions of everyday communications of ordinary Americans are swept up by government computers and run through a process that includes both data-mining and review of content, to try to figure out

whether any of us were involved in illegal or terrorist-related activity. That means that even the most personal and private of our electronic communications–between doctors and patients, between husbands and wives, or between children and parents–are subject to review by computer algorithms programmed by government bureaucrats or by the bureaucrats themselves. (Cindy Cohn, "Lawless Surveillance, Warrantless Rationales," American Constitution Society, August 17, 2009)

Both Rockefeller and Snowe are representative of the state's "bipartisan consensus" when it comes to increasing the power of the intelligence and security apparatus and were instrumental in ramming through retroactive immunity for telecoms who illegally spy on the American people. If last year's "debate" over the grotesque FISA Amendments Act (FAA) is an indication of how things will go after Congress' summer recess, despite hand-wringing by congressional "liberals," S.773 seems destined for passage. CNET revealed:

When Rockefeller, the chairman of the Senate Commerce committee, and Olympia Snowe (R-Maine) introduced the original bill in April, they claimed it was vital to protect national cybersecurity. "We must protect our critical infrastructure at all costs–from our water to our electricity, to banking, traffic lights and electronic health records," Rockefeller said. (Declan McCullagh, "Bill Would Give President Emergency Control of Internet," CNET News, August 28, 2009)

But as we witness practically on a daily basis, hysterical demands for "protection" from various "dark actors" inevitably invokes an aggressive response from militarized state security apparatchiks and their private partners.

As *Antifascist Calling* **reported** in July (see: "Behind the Cyberattacks on America and South Korea. 'Rogue' Hacker, Black Op or Both?"), when North Korea was accused of launching a widespread computer attack on U.S. government, South Korean and financial web sites, right-wing terrorism and security specialists perched at **Stratfor** and the American Enterprise Institute (**AEI**)–without a shred of evidence–linked the cyber blitz to a flurry of missile tests and the underground detonation of a nuclear device by North Korea.

Adding to the noise, Rep. Peter Hoekstra (R-MI), the ranking Republican on the House Intelligence Committee went so far as to urge President Obama to respond–by launching a cyberattack against the bankrupt Stalinist regime.

Despite provocative rhetoric and false charges that might have led to war with disastrous consequences for the people of East Asia, as it turned out an unknown sociopath used an updated version of the MyDoom e-mail worm to deploy a botnet in the attack. As *Computerworld* **reported**, the botnet "does not use typical antivirus evasion techniques and does not appear to have been written by a professional malware writer." Hardly a clarion call for bombing Dear Leader and countless thousands of Koreans to smithereens!

In this context, the Cybersecurity Act of 2009 goes much further than protecting "critical infrastructure" from over-hyped cyberattacks.

Among other measures, Section 18, "Cybersecurity Responsibilities and Authority," hands the Executive Branch, specifically The President, the power to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network." This does not simply apply to federal networks, but may very well

extend to the private communications ("critical infrastructure information system or network") of citizens who might organize against some egregious act by the state, say a nuclear strike against a nation deemed responsible for launching a cyberattack against the United States, as **suggested** in May by the head of U.S. Strategic Command (STRATCOM) General Kevin Chilton.

As I **reported** in June (see: "Cyber Command Launched. U.S. Strategic Command to Oversee Offensive Military Operations"), the military's newly-launched U.S. Cyber Command (CYBERCOM) is a "subordinate unified command" overseen by STRATCOM. Would "message force multipliers" embedded in the media or Pentagon public diplomacy specialists carrying out psychological operations (PSYOPS) here in the *heimat*, become the sole conduit for critical news and information during said "national emergency"?

Additionally, under Section 18's authority The President "shall designate an agency to be responsible for coordinating the response and restoration of any Federal Government or United States critical infrastructure information system or network affected by a cybersecurity emergency declaration under paragraph (2)." What agency might Senator Rockefeller have in mind for "coordinating the response"? As *Antifascist Calling* **revealed** in April (see: "Pentagon's Cyber Command to Be Based at NSA's Fort Meade"), CYBERCOM will be based at NSA headquarters and led by Lt. General Keith Alexander, the current NSA director who will oversee Pentagon efforts to coordinate both defensive and offensive cyber operations.

How might an out-of-control Executive Branch seize the initiative during an alleged "national emergency"? Paragraph 6 spells this out in no uncertain terms: "The President may order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security."

The draconian bill has drawn a sharp rebuke from both civil libertarians and the telecommunications industry. Larry Clinton, the president of the Internet Security Alliance (**ISA**) told CNET: "It is unclear what authority Sen. Rockefeller thinks is necessary over the private sector. Unless this is clarified, we cannot properly analyze, let alone support the bill."

And Wayne Crews, the director of technology studies at the rightist Competitive Enterprise Institute (**CEI**) told ***Federal Computer Week***: "From American telecommunications to the power grid, virtually anything networked to some other computer is potentially fair game to [President Barack] Obama to exercise 'emergency powers'."

True enough as far as it goes, these "free market" cheerleaders are extremely solicitous however, when it comes to government defense and security contracts that benefit their clients; so long as the public is spared the burden of exercising effective control as cold cash greases the sweaty palm of the market's "invisible hand"!

As *Antifascist Calling* **revealed** in June (see: "Obama's Cybersecurity Plan: Bring on the Contractors!"), the ISA is no ordinary lobby shop. According to a self-promotional blurb on their web site, ISA "was created to provide a forum for information sharing" and "represents corporate security interests before legislators and regulators."

Amongst ISA sponsors one finds AIG (yes, *that* AIG!) Verizon, Raytheon, VeriSign, the National Association of Manufacturers, Nortel, Northrop Grumman, Tata, and Mellon. State

partners include the U.S. Department of Homeland Security, Congress, and the Department of Commerce.

Indeed ISA and CEI, are firm believers in the mantra that "the diversity of the internet places its security inescapably in the hands of the private sector," and that "regulation for consumer protection" that rely on "government mandates" to "address cyber infrastructure issues" will be "ineffective and counter-productive both from a national security and economic perspective." CEI and ISA's solution? Let's have another gulp of that tasty "market incentives" kool-aid!

In other words, hand over the cash in the form of taxpayer largess and we'll happily (and profitably!) continue to violate the rights of the American people by monitoring their Internet communications and surveilling their every move through nifty apps hardwired into wireless devices as the Electronic Frontier Foundation revealed in a new **report** on locational privacy.

Unfortunately, Clinton, Crews and their well-heeled partners seem to have forgotten an elementary lesson of history: a national security state such as ours will invariably unwind its tentacles into every corner of life unless challenged by a countervailing force–a pissed-off, mobilized citizenry.

Now that national security "change" chickens are coming home to roost, both CEI and ISA seem incredulous: you mean *us*? How's that for irony!

Lee Tien, a senior staff attorney with EFF told CNET that changes to the original version of the bill do not address pressing privacy concerns.

Tien told the publication: "The language has changed but it doesn't contain any real additional limits. It simply switches the more direct and obvious language they had originally to the more ambiguous (version)…The designation of what is a critical infrastructure system or network as far as I can tell has no specific process. There's no provision for any administrative process or review. That's where the problems seem to start. And then you have the amorphous powers that go along with it."

McCullagh avers: "Translation: If your company is deemed 'critical,' a new set of regulations kick in involving who you can hire, what information you must disclose, and when the government would exercise control over your computers or network."

And there you have it, a "cybersecurity" blacklist to accompany a potential state takeover of the Internet during a "national emergency." What will they think of next!

*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**, his articles can be read on **Dissident Voice**, **The Intelligence Daily**, **Pacific Free Press** and the whistleblowing website **Wikileaks**. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by **AK Press**.*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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