GlobalResearch
Center for Research on Globalization

Obama's National Cybersecurity Initiative: Privacy and Civil liberties are Damned

Puts NSA in the Driver's Seat

By Tom Burghardt
Global Research, March 08, 2010
Antifascist Calling... 7 March 2010

Region: USA
Theme: Intelligence

On March 2, the Obama administration issued a sanitized version of the Comprehensive National Cybersecurity Initiative (CNCI), releasing portions that discussed intrusion detection systems on federal networks.

The announcement was made by former Microsoft executive Howard A. Schmidt, appointed cybersecurity coordinator by President Obama in December. The partial unveiling came during the RSA Security Conference in San Francisco, an annual industry conference for security professionals.

CNCI's 2008 launch was shrouded in secrecy by the Bush administration. Authority for the program is derived from a classified order issued by President Bush. However, the contents of National Security Presidential Directive 54, also known as Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23) have never been released for public scrutiny.

"Virtually everything about the initiative is highly classified," the Senate Armed Services Committee wrote in a 2008 report, "and most of the information that is not classified is categorized as 'For Official Use Only.'"

The Armed Services Committee joined their colleagues on the Senate Select Committee on Intelligence and urged that CNCI "should be scaled back because policy and legal reviews are not complete, and because the technology is not mature."

The Senate questioned the wisdom of a highly-secretive program that "preclude public education, awareness and debate about the policy and legal issues, real or imagined, that the initiative poses in the areas of privacy and civil liberties. ... The Committee strongly urges the [Bush] Administration to reconsider the necessity and wisdom of the blanket, indiscriminate classification levels established for the initiative."

The Electronic Privacy Information Center (EPIC) has filed suit against the government in federal court after EPIC's Freedom of Information Act request to the National Security Agency was rejected by NSA.

According to EPIC's complaint, CNCI has been described as "a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks." The agency refused to release the documents, stating that they "have been withheld in their entirety" because they are "exempt from release" on grounds of "national security."

Tuesday's summary provided no additional information on NSPD 54/HSPD 23, nor did the Obama administration release information on the Pentagon's strategy for waging offensive cyberwarfare.

The declassified portion of CNCI published March 2 discussed previously acknowledged intrusion protection programs, specifically Einstein 2 and Einstein 3, designed to inspect internet traffic entering government systems to detect potential threats.

As Antifascist Calling disclosed last July, the Einstein program in all probability is related to the much larger, ongoing and illegal NSA communications intercept program known as Stellar Wind, first exposed in 2005 by The New York Times.

And Stellar Wind, as I reported in another piece last July, is intimately related to what has come to be known as the "President's Surveillance Program," or PSP.

According to a 38-page declassified report by inspectors general of the CIA, NSA, Department of Justice, Department of Defense and the Office of the Director of National Intelligence, presidential authorization for the secret state's driftnet surveillance program was derived by an Office of Legal Counsel (OLC) Memorandum penned November 2, 2001, by torture-enabler John C. Yoo.

Despite long-standing prohibitions on military and CIA involvement in civilian law enforcement activities, Yoo wrote that electronic surveillance in "direct support of military operations" did not trigger constitutional rights against illegal searches and seizures, because the Fourth Amendment "is primarily aimed at curbing law enforcement abuses."

Yoo's tortured reading of the Foreign Intelligence Surveillance Act (FISA) claimed that the law "cannot restrict the President's ability to engage in warrantless searches that protect the national security."

While this particular memorandum was withdrawn, Congress granted the Executive Branch carte blanche for illegal spying under provisions of the despicable FISA Amendments Act of 2008 (FAA), supported by then-candidate and now president, Barack Obama.

Indeed, the administration has yet to lay out for the American people current guidelines that would guarantee such abuses are not continuing. Why? Because the PSP is ongoing and now, under the rubric of "cybersecurity," illegal spying by NSA and other secret state agencies continues apace.

As it now stands according to CNCI, Einstein will be tied directly into giant NSA data bases that contain the trace signatures of previous cyberattacks. The agency's immense electronic warehouses will continue to be fed information streamed to the agency by the nation's telecommunications providers.

Under FAA, telecommunications and internet firms are not liable for past or future violations of Americans' constitutional guarantees; indeed, these firms are partners in state-sanctioned surveillance operations.

Like their predecessors in the Oval Office, the Obama administration has obstructed the federal courts from examining the nature of the PSP, or lawbreaking by high government officials. In case after case brought by civil libertarians and privacy advocates, Obama's Justice Department has successfully argued that citizen lawsuits cannot be heard or

Executive Branch programs reviewed by any court on grounds that sensitive "state secrets" would be disclosed.

The Washington Post disclosed last July, that under a classified Bush administration program "NSA data and hardware would be used to protect the networks of some civilian government agencies. Part of an initiative known as Einstein 3, the plan called for telecommunications companies to route the Internet traffic of civilian agencies through a monitoring box that would search for and block computer codes designed to penetrate or otherwise compromise networks."

Despite President Obama's pledge in May 2009 announcing White House cybersecurity policy, that his administration will not continue Bush-era surveillance practices under the PSP, Tuesday's partial release of CNCI signals just the opposite.

Indeed, Einstein 3 is based on technology developed for a NSA program called Tutelage that detects and halts security breaches. However, its filtering software can read the content of email and other electronic communications.

While the White House claims that the Department of Homeland Security (DHS) is the lead agency overseeing government efforts to protect state networks and critical infrastructure–the electrical grid, telecommunications networks, internet service providers, and the banking and financial sectors from malicious attacks–NSA's role has raised red flags amongst privacy and civil liberties advocates.

As EPIC pointed out in their lawsuit, in March 2009 Rod Beckstrom resigned from his position as DHS National Cybersecurity Center director, citing the secretive role that NSA will play in these efforts, stating that "NSA currently dominates most national cyber efforts."

This is a critical point. As a Defense Department agency, NSA's primary role is the interception of Communications- and Signals Intelligence (COMINT/SIGINT). As an Executive Branch agency answerable not to Congress but to the Secretary of Defense and the President, the near nonexistent democratic oversight of NSA will be further undermined by CNCI.

This is made clear in the document released Tuesday by the White House: "The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions."

DHS claims are undermined by Einstein 3's ability to perform deep packet inspections that "read the content of email and other communications" as The Wall Street Journal reported last summer.

The document claims that "Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens."

This assertion is undercut however, when the White House states that "DHS will be able to adapt threat signaturesdetermined by NSA in the course of its foreign intelligence and DoD

information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission." (emphasis added)

In practice, the same sources and methods deployed by NSA to conduct foreign intelligence, unrestricted by the agency's charter or U.S. law, will most certainly continue to target communications by U.S. citizens.

Although White House cybersecurity coordinator Schmidt states that "transparency is particularly vital in areas, such as the CNCI, where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity," as Secrecy News points out "without a clear delineation of legal authorities and implementation mechanisms, the scope for meaningful public discussion seems limited."

Despite the fact that Congress stood up the Privacy and Civil Liberties Oversight Board as an independent agency in 2007 "to monitor and defend civil liberties in information sharing and counterterrorism activities," Secrecy News' Steven Aftergood disclosed that the Board "has remained vacant since that time" and thus, is "unable to fulfill its assigned task;" a telling commentary on the administration's largely rhetorical promise of "openness"!

Cybersecurity: Another Day, Another Endless "War"

As long time readers of Antifascist Calling are well aware, while hacking, online thievery and sociopathic behavior by criminals is a troubling by-product of the "information superhighway," state officials and shadowy security corporations have framed the debate in terms of yet another in a series of endless "wars."

Mike McConnell, a former NSA Director, Bush regime Director of National Intelligence and currently an executive vice president with the spooky Booz Allen Hamilton corporation (a post he held for a decade before signing-on for the "War on Terror") penned an alarmist screed for The Washington Post February 28.

McConnell, whose firm stands to reap billions of dollars in taxpayer largesse under CNCI, claimed that "The United States is fighting a cyber-war today, and we are losing."

Drawing a spurious and half-baked (though self-serving) parallel between the Cold World nuclear stand-off with the former Soviet Union and today's cybercriminals, McConnell declared that a "credible" cyber-deterrent analogous to the doctrine of Mutually-Assured Destruction (MAD) would serve the United States "well."

Ever the Cold warrior, McConnell avers that the U.S. needs 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."

"More specifically," McConnell writes, "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment–who did it, from where, why and what was the result–more manageable."

In other words, the secret state's role in monitoring each and every electronic communication, email, text message, web search, phone conversation or financial transaction must be subject to a pervasive and all-encompassing surveillance by securocrats or we won't be "safe."

Indeed, as McConnell and his shadowy firm are well aware since they helped develop them, "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."

Reckless advocacy such as this is the kiss of death for any notion of privacy, let alone the constitutional right to dissent. As Wiredinvestigative journalist Ryan Singel wrote last week, "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."

Why? Singel insists, "McConnell's not dangerous because he knows anything about SQL injection hacks, but because he knows about social engineering." And during his stint as DNI, "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."

Self-serving rhetoric by the likes of McConnell about an alleged "cyber-armageddon" are not only absurd but the height of corporatist venality.

As investigative journalist Tim Shorrock revealed in his essential book Spies for Hire and for CorpWatch, Booz Allen Hamilton, a wholly-owned subsidiary of the shadowy private equity firm, The Carlyle Group, "is involved in virtually every aspect of the modern intelligence enterprise, from advising top officials on how to integrate the 16 agencies within the Intelligence Community (IC), to detailed analysis of signals intelligence, imagery and other critical collections technologies."

Clocking-in at No. 10 on Washington Technology's "Top 100" list of Federal Prime Contractors, Booz Allen pulled down some $2,779,421,015 in contracts in 2009.

According to Shorrock, "BAH is one of the NSA's most important contractors, and owes its strategic role there in part to Mike McConnell, who was Bush's director of national intelligence." During an earlier stretch with BAH, "McConnell and Booz Allen were involved in some of the Bush administration's most sensitive intelligence operations, including the infamous Total Information Awareness (TIA) program run by former Navy Admiral John Poindexter of Iran-Contra fame."

In his Washington Post op-ed, McConnell wrote that "we must hammer out a consensus on how to best harness the capabilities of the National Security Agency," and that the "challenge" is to shape "an effective partnership with the private sector so information can move quickly back and forth from public to private–and classified to unclassified–to protect the nation's critical infrastructure."

Super spook McConnell claims this will be accomplished by handing "key private-sector leaders (from the transportation, utility and financial arenas) access to information on emerging threats so they can take countermeasures." However, the "private" portion of the "public-private" surveillance "partnership" must have a quid pro quo so that private sector sharing of privileged, highly personal, network information with the secret state doesn't invite "lawsuits from shareholders and others."

In other words, privacy and civil liberties be damned!

As Ryan Singel points out, "the contractor he works for has massive, secret contracts with

the NSA" and McConnell now proposes that NSA "take the lead in guarding all government and private networks."

But McConnell, and Booz Allen's advocacy goes far further than simple advocacy in developing a defensive cyber strategy. Indeed, BAH, and a host of other giant defense and security firms such as Lockheed Martin, are actively developing offensive cyber weapons for the Pentagon.

According to Washington Technology, Lockheed Martin will continue to work with the Defense Advanced Research Project Agency (DARPA) in that Pentagon agency's development of a National Cyber Range under CNCI.

That program is suspected of being part of Pentagon research to develop and field-test offensive cyber weapons. According to DARPA, "the NCR will provide a revolutionary, safe, fully automated and instrumented environment for U.S. cybersecurity research organizations to evaluate leap-ahead research, accelerate technology transition, and enable a place for experimentation of iterative and new research directions."

"Now the problem with developing cyberweapons–say a virus, or a massive botnet for denial-of-service attacks," Singel writes, "is that you need to know where to point them."

"That's why," the Wired journalist avers, "McConnell and others want to change the internet. The military needs targets."

Add to the mix a Senate bill that would hand the president "emergency" powers over the Internet and a clear pattern of where things are headed begins to emerge.

With giant ISP's such as Google already partnering-up with the NSA and other secret state agencies, the question is how long will it be before an American version of China's Golden Shield enfolds the heimat within its oppressive tentacles?

Described by privacy advocates as a massive, ubiquitous spying architecture, the aim of the Golden Shield is to integrate a gigantic online data base with an all-encompassing surveillance network, one that incorporates speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies.

And considering that the Empire has reportedly stood-up a giant data base of dissidents called "Main Core," whose roots lie in programs begun during the Reagan administration, assurances by the Obama administration that Americans' privacy rights will be protected as CNCI is rolled-out ring hollow. According to exposés by investigative journalists Christopher Ketchum and Tim Shorrock, writing respectively in Radar Magazine and Salon, Main Core is a meta data base that contains personal and financial data on millions of U.S. citizens believed to be threats to national security.

The data, which comes from the NSA, FBI, CIA, and other secret state sources, is collected and stored with neither warrants nor court orders. The name is derived from the fact that it contains "copies of the 'main core' or essence of each item of intelligence information on Americans produced by the FBI and the other agencies of the U.S. intelligence community," according toSalon.

While the total cost of CNCI is classified, rest assured it will be the American people who foot the bill for the destruction of our democratic rights.

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