GlobalResearch
Center for Research on Globalization

Back from the Dead: The Internet 'Kill Switch'

By Tom Burghardt
Global Research, May 30, 2011
Antifascist Calling... 30 May 2011

Region: USA
Theme: Police State & Civil Rights

by ***Antifascist Calling…***

The American author William Faulkner once wrote: "The past is never dead. It's not even past."

And like a horde of flesh-eating zombies shuffling out of a parking garage to feast on what's left of our freedoms, the Obama administration has promised to revive a proposal thought dead by most: the internet "kill switch."

On May 12, the White House released a 52-page **document** outlining administration plans governing cybersecurity. The bill designates the Department of Homeland Security as the "lead agency" with authority to initiate "countermeasures" to protect critical infrastructure from malicious attacks.

But as with other aspects of U.S. policy, from waging aggressive wars to conducting covert actions overseas, elite policy planners at the Pentagon and at nominally civilian agencies like DHS hide *offensive* plans and operations beneath layers of *defensive* rhetoric meant to hoodwink the public.

The term "countermeasure" is described by the White House as "automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system or information systems owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected." (Section 1. Department of Homeland Security Cybersecurity Authority, May 12, 2011, p. 1)

In other words, the proposal would authorize DHS and presumably other federal partners like the National Security Agency, wide latitude to monitor, "modify or block" data packets (information and/or communications) deemed a threat to national security.

It isn't a stretch to conclude that such "automated actions" would be predicated on the deployment of systems such as "Einstein 3" or the NSA's top secret "Perfect Citizen" program throughout the nation's electronic communications architecture.

NSA's Einstein 3 project we're told is designed to prevent malicious attacks on government systems and, controversially, private sector networks. Using NSA hardware and the signatures of previous attacks as a road map, Einstein 3 routes 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," ***The Washington Post*** reported.

According to multiple media reports, AT&T, one of the Agency's private partners in Bush and now, Obama administration warrantless wiretapping programs variously known as "Stellar Wind," "Pioneer," its data-mining portion and "Pinwale," the agency's secret email collection program, was the Bush administration's choice to test the system. In fact, before agreeing to participate in the pilot project AT&T attorneys sought assurances from the Justice Department "that it would bear no liability for participating," the *Post* averred.

Since 2009, under Obama, Einstein 3 testing has proceeded apace.

Last summer, ***The Wall Street Journal*** revealed that NSA and a private corporate partner, the giant defense firm Raytheon, were standing up a new program known as "Perfect Citizen."

According to investigative journalist Siobhan Gorman, the black project "would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack."

An email from a Raytheon insider that the *Journal* obtained recounted that "the overall purpose of the [program] is our Government…feel[s] that they need to insure the Public Sector is doing all they can to secure Infrastructure critical to our National Security." It concluded with this ominous warning: "Perfect Citizen is Big Brother."

While NSA initially downplayed serious threats to privacy, claiming that "Perfect Citizen" is no more intrusive than traffic cameras on a busy street, ***The Register*** cautioned that "mission creep" was a distinct possibility, given that sensitive, private information could migrate "outside an infrastructure-security context."

How would such programs and proposals play out in the real world?

According to ***Government Computer News*** "proposed cybersecurity legislation released by the Obama administration earlier this month is similar to legislation now pending in the Senate, but it does not contain the explicit emergency powers contained in the bill introduced by Joseph I. Lieberman (I-Conn.) and Susan M. Collins (R-Maine)."

Pretty good so far? Not so fast! GCN reports, "instead, it seems to rely on a 77-year-old law that gives the president broad authority to shut down communications networks."

Got that? There's no need for a legislative fix to expand the president's power to pull the plug, only in the event of an unspecified "national emergency" of course, since the White House *already* possesses the means to do just that, the **Communications Act of 1934**.

The Act, amended in 1996, specifically empowers the president "during the continuance of a war in which the United States is engaged," control over media under circumstances determined by the Executive Branch. Accordingly, Section 706 [47 U.S.C. 606] authorizes the president "if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to this Act."

But the law goes further and in fact authorizes the president "whenever in his judgment the

public interest requires, to employ the armed forces of the United States to prevent any such obstruction or retardation of communication."

This would seem to open the door even further to intrusions into domestic affairs by the National Security Agency and U.S. Cyber Command, which after all are Pentagon *combat support agencies*, charged with carrying out electronic communications warfare.

In the event of a declared "national" or, in today's language, a "cyber emergency," the president "may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication and the removal therefrom of its apparatus and equipment, or he may authorize the use or control of any such station and/or its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners."

Substitute the word "internet" for "radio" and "network" for "station" and it becomes all-too-clear that presidential authority for an internet "kill switch" is already a reality.

And in the context of America's "War on Terror," described by war criminal and former Secretary of Defense Donald Rumsfeld as a conflict having "no known metrics" to determine its endpoint, "war time" powers to be exercised solely at the discretion of the president over the nation's communications infrastructure too, seem to be virtually limitless and without constraints imposed either by Congress or the federal judiciary as recent "state secrets" rulings readily attest.

Right-wing senator Collins cried foul, saying that Executive Branch authority under the Communications Act "is far broader than the authority in our bill," claiming that legislation she and neocon hawk Lieberman introduced would "carefully constrain" the president's power over the internet.

Sure, just as the War Powers Act "constrained" the president from carrying out preemptive wars against countries which haven't attacked the United States but have the singular misfortune of possessing valuable resources (can you say oil, Iraq and Libya), lusted after by American multinationals.

During last week's hearings before the Senate Homeland Security and Governmental Affairs Committee, outgoing DHS Undersecretary for the National Protection and Programs Directorate, Philip R. Reitinger, told the Committee that the administration "would use the authority that [1934 law] brings to bear in the right way."

"Trust us," top Obama administration officials explain. We wouldn't do anything that threatens the free flow of information, not to mention privacy rights or civil liberties, would we?

This from a White House that's expanded the already formidable, and illegal, warrantless wiretapping **programs** of the previous regime while continuing to withhold secret legal memos cobbled together by the Office of Legal Counsel; memos justifying everything from the seizure of personal records to electronic communications by various intelligence fiefdoms under the Patriot Act, as I **reported** last week.

Reitinger, who'll leave his post next month, reportedly to "spend more time with his family," or more likely, before taking a plum position with one of the innumerable defense firms staking out the lucrative cybersecurity market, said that White House authority during a "cyber emergency," say a sudden revolt by outraged citizens against capitalist depredations like the ones which shook Tunisia and Egypt earlier this year or are currently exploding across Spain are "one of the areas that would need to be negotiated," GCN reported.

Of course, congressional grifters are not talking about political upheavals *per se*, although the response by repressive governments such as Egypt to citizens clamoring for more rights, no doubt with encouragement by certain three-lettered U.S. agencies, helped the former Mubarak regime reach their decision to flip the switch and cut off cell phone and internet access for a time.

As Washington's cyber scare gathers steam, one of the "more controversial elements of any new cybersecurity law," the right-wing ***Washington Times*** avers, are "what powers the president should have over the Internet in the event of a catastrophic attack on vital U.S. assets."

"Clearly, if something significant were to happen, the American people would expect us to be able to respond and respond appropriately," Reitinger said.

"Experts," according to the *Washington Times*, "say that in the event of a major cyber-attack, authorities might have only a short time to respond and might need to temporarily divert some Internet traffic or take it off-line."

Wringing her hands, Collins said she was "baffled" by administration plans to rely on the 1934 law.

Reitinger said that while presidential powers embedded in the Communications Act "were not designed with the current environment that we have in mind," he insisted "there are authorities there."

And where "authorities" exist, you can be certain that the National Security State will find the means to use them, or invent new ones, in secret and without disclosing the fact either to Congress or the public.

During hearings before the House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet, Obama administration officials "faced pointed questions" over White House proposals, the ***National Journal*** reported.

"Lawmakers," reporter Josh Smith wrote, "worried that the administration's plan provides too much government control in cybersecurity issues."

In a replay of the repulsive FISA Amendments Act (FAA), the White House plan "would grant legal immunity to companies who cooperate with federal cyber investigations." North Carolina Democrat Melvin Watt was skeptical, saying that Obama's proposal was similar to FAA's retroactive immunity clause that handed out get-out-of-jail-free cards to telecom companies that collaborated with the secret state's driftnet spying operations.

Watt said, "these companies could then do something that's unconstitutional just because you say it's not. People get very uncomfortable with the idea that the government can just call up someone, demand information, and then provide them immunity."

And under the proposal, the federal courts would be barred from determining whether or not to grant immunity to cooperating firms accused of handing over the personal details of their customers to the government; that too, would be left to the Executive Branch.

As I have written many times (most recently **here**, **here** and **here**), the National Security Agency and U.S. Cyber Command, along with private partners who stand to make billions hyping the cyber threat, are driving U.S. policy.

During recent hearings, Richard J. Butler, Deputy Assistant Secretary of Defense for Cyber Policy said that the "Defense Department is sharing cybersecurity information, capabilities and expertise with the Homeland Security Department," the ***Armed Forces Press Service*** reported.

According to Butler, cybersecurity requires a "whole government approach," and that the "Defense and Homeland Security departments already are doing that," citing last fall's **Memorandum of Agreement** between NSA and DHS that "laid the foundation for the collaboration … to share operational planning and technical development."

"Since then," Butler said, "the collaboration has grown into joint coordination at U.S. Cyber Command and the National Security Agency at Fort Meade, Md., and the sharing of information, capabilities, and employees."

Just how real is the threat?

In an essential paper published last month, ***Loving the Cyber Bomb?***, George Mason University researchers Jerry Brito and Tate Watkins wrote that despite a "steady drumbeat of alarmist rhetoric coming out of Washington about potential catastrophic cyber threats," the rhetoric of "'cyber doom' employed by proponents of increased federal intervention, however, lacks clear evidence of a serious threat that can be verified by the public."

"As a result," Brito and Watkins averred, "the United States may be witnessing a bout of threat inflation similar to that seen in the run-up to the Iraq War."

"Additionally," the researchers cautioned, "a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve to not only supply cybersecurity solutions to the federal government, but to drum up demand for them as well."

"The official consensus," Brito and Watkins wrote, "seems to be that the United States is facing a grave and immediate threat that only quick federal intervention can address."

As we have seen, most recently during rushed congressional votes that reauthorized expiring sections of the constitution-shredding USA Patriot Act, the Executive Branch will do everything in its power to continue hyping unverified threats, thus concealing just how far we've traveled along the road towards a National Surveillance State.

After all, as ***Wired*** reported last week, if "you think you understand how the Patriot Act allows the government to spy on its citizens … Sen. Ron Wyden says it's worse than you know."

The Oregon Democrat, a member of the Senate Intelligence Committee, told journalist Spencer Ackerman that there's "a gap between what the public thinks the law says and

what the American government secretly thinks the law says."

During testimony last March before the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, the Justice Department's top national security official, Todd Hinnen, **told** congressional grifters that Section 215, the "business records" provision "has been used to obtain driver's license records, hotel records, car rental records, apartment leasing records, credit card records, and the like."

However, Hinnen testified that Section 215 has "also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed," behind closed doors.

Neither the FBI nor the Justice Department will comment on what that secret interpretation of the law might entail. However, security and privacy researcher Christopher Soghoian **averred** that the secret state's "sensitive collection program" is likely "related to warrantless, massive scale collection of geo-location information from cellular phones."

"Clearly," Soghoian writes, "there are many unanswered questions–we do not know what kind of data collection is occurring, and why it is problematic enough to cause four senators to speak up publicly. However, given that four senators have now spoken up, this strongly suggests that there is something seriously rotten going on."

Commenting on the rush to pass Patriot Act legislation, **CNET News** investigative journalist Declan McCullagh averred: "It's true that exabytes upon exabytes of data could, in theory, be helpful in investigating terrorism and other crimes. This was the motivation behind the Total Information Awareness idea, after all. But it's also true that nobody in the U.S. Congress believed that they were giving the FBI such sweeping authority when enacting the law nearly a decade ago."

Magnify those concerns by a factor of ten or even a thousand when it comes to the formidable array of surveillance capabilities already deployed by the National Security Agency.

And if the interpretation of the Communications Act favored by top Obama administration officials gain traction in Congress then, as the **ACLU** recently warned "there are [cybersecurity] proposals out there that would permit information grabs that make the Patriot Act look quaint."

*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 independent research and media group of writers, scholars, journalists and activists based in Montreal, he is a Contributing Editor with **Cyrano's Journal Today**. 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.*

The original source of this article is Antifascist Calling...
Copyright © Tom Burghardt, Antifascist Calling..., 2011

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca