GlobalResearch
Center for Research on Globalization

World Wide Wiretap

Recent cyber attacks provide pretext for sweeping internet snooping by US government

By James Corbett
Global Research, July 10, 2009
The Corbett Report 10 July 2009

Region: USA
Theme: Police State & Civil Rights

Last Friday, while most Americans were preparing for a weekend of fireworks and hot dogs, the Obama Administration had an ominous message: they are going ahead with a Bush-era plan to allow the NSA even more power to invade, intercept and analyze the data of anyone visiting a government website, ostensibly to help prevent a major cyber attack.[1] The timing of the announcement, the day before a holiday long weekend, seemed unusual, but less than 24 hours later just such an attack began to unfold on a series of websites in America and South Korea, including those of the White House, Pentagon, New York Stock Exchange, Treasury Department, Secret Service and The Washington Post, amongst others.

The attack itself turns out to have been fairly innocuous[2]–a run of the mill DDOS (distributed denial of service) attack that did not even employ the latest malware–but you wouldn't know that from reading the sensational reporting in the controlled corporate media. The VOA reports that the 'internet attackers' have struck again.[3] "US State Department under cyberattack for fourth day" blares a headline from the AFP.[4]

Blame for the attack is now falling on North Korea, but what North Korea has to gain by taking down The Washington Post's website is anybody's guess (perhaps Kim Jong-il was giving his own pronouncement on the recent revelation that the Post was selling access to high-level politicians to lobbyists for $250,000 a pop[5]). The big winner in this attack, it seems, is the federal government, which has been preparing to unveil an Internet surveillance spy grid for years, but have virtually no mandate to do so from a public that has become tired of invasive government snooping.

Various government stooges have been trying to drum up support for their Orwellian police state fantasy for years by warning of the coming 'cybergeddon' at the hands of 'cyber terrorists.' In 2003, former National Security Agency (NSA) director Mike McConnell was going on international fearmongering trips warning of attacks "equivalent to the attack on the World Trade Center in New York" unless a new agency were created to deal with the threat.[6] The'cyber 9-11′ meme has carried on ever since, with hysterical coverage of Chinese cyber warriors[7] and teenage hackers[8] attempting to rally the public into supporting a new front in the "War on Terror:" cyberspace.

Of course, exactly as was the case of 9/11, which was used as a pretext for tabling and passing (before anyone had time to read it) the voluminous, labyrnthine constitution-destroying Patiot Act, so too will the 'cyber 911' be used to justify an iPatriot Act that will destroy any vestige of legal red tape preventing the government from tracking, tracing and controlling every movement of every citizen in cyberspace forever. That this legislation exists and is in fact merely waiting for a large cyberterrorist incident to justify rushing it into

law was actually admitted last year by former Counter Terrorism Czar Richard Clarke to Lawrence Lessig.[9] “I was having dinner with Richard Clarke and I asked him if there is an equivalent [to the Patriot Act],” Lessig recounted to a technology conference in California last year.”‘Is there an i-Patriot Act just sitting waiting for some substantial event as an excuse to radically change the way the internet works?’ He said ‘of course there is’.”

The three prongs of the attack on Internet freedom and privacy come from the military, the NSA and the Executive/Legislative branches of government. In 2003, the military labeled the Internet itself an enemy weapons system[10] and ever since then there has been growing momentum behind various military, intelligence and governmental schemes to track and trace all movements of all Internet users, American or foreign. Last year, the Air Force attempted to establish its own cyber command[11], resulting in military turf wars that last month spawned a new U.S. Cyber Command and the further militarization of cyberspace.[12] The military has even threatened a military responsea gainst any would-be hackers of government systems[13] (unless you are North Korean, evidently).

At the same time, the NSA is jockeying to launch a new system dubbed Einstein that would see all telecoms route data traveling to or from government networks through an NSA monitoring box.[14] This is on top of existing programs like pinwale[15] and Stellar Wind[16] which have already given them legal access to secretly spy on billions of communications records. Now Mike McConnell is back on the fearmongering trail telling anyone who will listen that if the NSA doesn’t have the authority to examine everyone search history, private emails and file transfers, then there will be a (you guessed it) “cyber 9/11.”[17]

The third prong of the attack comes from America’s own elected representatives. Even back in 2007 the powerful thinktank known as the Center for Strategic and International Studies was already preparing for the coming Obama presidency, convening a year-long panel that issued a report called “Securing Cyberspace for the 44th Presidency”[18] which contained the following chilling passage under the heading “Regulate cyberspace:”

“Voluntary action is not enough. The United States must assess and prioritize risks and set minimium standards for securing cyberspace in order to ensure that the delivery of critical services in cyberspace continues if the United States is attacked.”

Now, Jay Rockefeller is attempting to do just that with a bill that would kick start this process of setting ‘minimum standards’ for cybersecurity over to an advisory panel filled with globalists, corporate chieftains and hand-picked academics[19]. Rockefeller tried to drum up his own support for the bill by reaching new heights of hysterical fearmongering over the net, even going so far as to say the Internet should never have existed.[20] Obama is getting in on the act as well, threatening to pick a new ‘Cyber Czar’ who is conspicuous for having taken every opportunity during his time in Congress to vote for the expansion of NSA spying programs and authorities.[21]

The entire cyberterror hysteria seems to have reached a peak in the last month, with the announcement of U.S. cyber command, the impending vote on Rockefeller’s bill and the naming of Obama’s cyber czar expected to occur in the near future. Up until this week, there has only been one problem: there has been no clear mandate for any of this hysterical rush toward increased government snooping and regulation on the Internet. The American public is becoming disgusted with Obama's continuation of the NSA spying program[22] and have been unwilling to get behind giving up their online liberties in

exchange for protection from the threat of teenage hackers and Russian spambots. The former head of the National Cybersecurity Center resigned this March citing "threats to the democratic process from the NSA's attempts to dominate all governmental cybersecurity efforts.[23] Wired even ran a story detailing how the U.S. Cyber Command is an agency without a purpose, function or mission that has been trying to find a reason for existing.[24]

Now along comes a relatively unsophisticated DDOS attack from what may or may not be North Korea (there is no proof for the origin of the attack other than the government's say-so) and suddenly it all seems justified: the creation of new branches of the military to deal with cyber warfare and even create sophisticated new cyberweapons for destroying hackers and rogue governments; the NSA programs to track and trace all searches, file transfers and communications of seemingly everyone on the planet; Rockefeller's legislation to appoint big business and globalists to advise on mandatory communications regulations. It seems that Obama and the NSA have more to gain from these attacks than do the North Koreans.

Of course, the capability (and presumably the intention) to monitor every electronic communication passing through the United States in real time has long existed. What we are seeing now is the revelation of long-established policies and technologies to a public that may have rejected them before. The Communications Assistance for Law Enforcement Act (CALEA) of 1994[25] already mandated that every communications device in the country be accessible by law enforcement, and it has now been mainstream news for years that the FBI can (and has) dialled into cellphones to listen in on any conversations taking place within reach of the microphone…even if the power is turned off.[26] In 2006, an AT&T whistleblower revealed an NSA spy room directly in the data hub monitoring every email, every phone call and every fax traveling through that hub.[27] In 2008, it was admitted that part of the NSA's efforts to catch Al-CIAda included agents passing around particularly humorous phone sex conversations between US military overseas and their wives back home.[28]

No, the capability of spying on all communications of all Americans is not being developed now; that has already happened. Right now we are witnessing the implementation of the phase in which the capability to track and trace all communications are being introduced to the public and justified on the grounds of national security. Expect to see an increasing number of media-hyped 'cyber attack' stories before the cyber 9/11 makes the iPatriot Act a reality.

Of course, it should be obvious by now that those in charge of multi-billion dollar agencies are in positions to directly materially benefit from just such large, stunning cyber attacks, opening the door to the false-flag mentality by which attacks are to be welcomed for their transformative nature.[29] Certainly the NSA is not building a $1.6 billion-dollar data center to sit on their hands waiting for an attack[30], nor are the governments of the UK[31], Canada[32], Ireland[33] and many other countries suddenly considering draconian new e-spying legislation for the fun of it.

For those who are interested in how a cyber false-flag terrorist attack could be generated, the PTECH story[34] remains a crucial piece of the puzzle. The technology exists for those in the know to commit sophisticated, convincing and devestating attacks through the government's own cyber infrastructure. The only question is who has the means, motive and opportunity to use it.

Notes

[1]http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html
[2]http://www.informationweek.com/news/showArticle.jhtml?articleID=218401127
[3]http://www.voanews.com/english/2009-07-09-voa18.cfm
[4]http://rawstory.com/news/afp/US_State_Department_under_cyberatta_07092009.html
[5]http://www.politico.com/news/stories/0709/24441.html
[6]http://www.smh.com.au/articles/2003/04/21/1050777200225.html
[7]http://www.worldtribune.com/worldtribune/WTARC/2009/ea_china0377_05_12.asp
[8]http://www.securityfocus.com/columnists/38
[9] http://www.infowars.net/articles/august2008/050808i911.htm
[10] http://www.globalresearch.ca/index.php?context=va&aid=7980
[11] http://www.wired.com/dangerroom/2008/06/marlborough-mas/
[12] http://www.wired.com/images_blogs/dangerroom/2009/06/cybercommand.pdf
[13] http://www.presstv.ir/detail.aspx?id=94143&sectionid=3510203
[14] http://blog.executivebiz.com/nsa-at-chertoff-weighs-in/3134
[15] http://www.harpers.org/archive/2009/06/hbc-90005232
[1 6]
http://www.thepeoplesvoice.org/TPV3/Voices.php/2009/05/11/a-8216-stellar-winda-8217-routinely-eave
[17] http://www.wired.com/threatlevel/2008/01/feds-must-exami/
[18] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
[19] href=http://www.nextgov.com/nextgov/ng_20090626_2244.php
[20] href=http://www.youtube.com/v/Ct9xzXUQLuY
[21] href=http://www.wired.com/threatlevel/2009/06/cyber_privacy/
[2 2]
http://antifascist-calling.blogspot.com/2009/04/obamas-justice-department-moves-to.html
[23] href=http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf
[2 4]
http://www.wired.com/dangerroom/2009/06/foggy-future-for-militarys-new-cyber-command/
[25]http://www.askcalea.net/
[26]http://www.youtube.com/watch?v=0G1fNjK9SXg
[27]http://www.wired.com/science/discoveries/news/2006/04/70619
[28] http://abcnews.go.com/Blotter/story?id=5987804&page=1
[29] http://www.corbettreport.com/articles/20090706_scheuer_false_flag.htm
[3 0]
http://www.datacenterknowledge.com/archives/2009/07/01/nsa-plans-16-billion-utah-data-center/
[31] http://news.bbc.co.uk/2/hi/uk_news/8087530.stm
[3 2]
http://www.cbc.ca/technology/story/2009/06/19/tech-internet-communications-electronic-police-bills-surveillance-follo-privacy.html
[33] http://www.examiner.ie/Ireland/idsnausnmh/rss2/
[34] http://www.corbettreport.com/index.php?ii=88&i=Documentation

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **James Corbett**

About the author:

James Corbett is a Film Director and Producer based in Okayama, Japan. He started The Corbett Report (www.corbettreport.com) website in 2007 as an outlet for independent critical analysis of politics, society, history, and economics. It operates on the principle of open source intelligence and provides podcasts, interviews, articles and videos about breaking news and important issues from 9/11 Truth and false flag terror to the Big Brother police state, eugenics, geopolitics, the central banking fraud and more.