GlobalResearch
Center for Research on Globalization

“Rogue Hacker” and Black Ops

Behind the Cyberattacks on America and South Korea

By Tom Burghardt
Global Research, July 12, 2009
Antifascist Calling... 12 July 2009

Region: USA
Theme: Police State & Civil Rights

The iconic American investigative journalist I.F. Stone once said, “All governments are run by liars and nothing they say should be believed.” Stone’s credo is all the more relevant today when it comes to the pronouncements of intelligence agencies and their corporate masters, particularly where official enemies are concerned.

A widespread computer attack that began July 4 took down several U.S. Government, South Korean and financial web sites, the *Associated Press* **reported**.

Multiple media reports claim that the Treasury Department, the Department of Homeland Security (DHS), Secret Service, Federal Trade Commission and Department of Transportation web sites were struck by a distributed denial of service (DDOS) assault that began last Saturday.

According to ***Computerworld***, “a botnet comprised of about 50,000 infected computers has been waging a war against U.S. government Web sites and causing headaches for businesses in the U.S. and South Korea.” The magazine reported July 7, “on Saturday and Sunday the attack was consuming 20 to 40 gigabytes of bandwidth per second, about 10 times the rate of a typical DDoS attack, one security expert said after being briefed by the US-CERT on Tuesday. ‘It’s the biggest I’ve seen’.”

This is particularly embarrassing to the DHS since the agency’s U.S. Computer Emergency Readiness Team (**U.S.-CERT**) is responsible for preventing illegal hacking forays on government networks.

Attacks were also reported on the White House, the Department of Defense, the State Department, *The Washington Post*, U.S. Bancorp, the New York Stock Exchange and Nasdaq. Affected sites in South Korea included those of the presidential Blue House, the Ministry of Defense, the National Assembly, Shinhan Bank, the newspaper *Chosun Ilbo*. South Korea’s top Internet Service Provider, Naver.com crashed on Tuesday, according to the *Associated Press.*

Despite the unsophisticated nature of the cyber incursion that employed a variant of the MyDoom virus, unnamed “senior U.S. officials” told ***The Wall Street Journal*** that American and South Korean officials are “probing North Korea’s possible role.” The same anonymous sources said that the botnet attack “coincided with North Korea’s latest missile launches and followed a United Nations decision to impose new sanctions.”

That the cyber assault also “coincided” with a holiday fireworks accident that killed 5 workers in North Carolina, multiple deaths due to drunk driving on U.S. highways or an

Italian railway disaster that claimed 21 lives, is hardly “evidence” of Pyongyang’s shadowy hand.

Nevertheless, South Korea’s National Intelligence Service (NIS), the successor organization to the Korean Central Intelligence Agency (KCIA), was quick to blame the troglodytic Stalinist regime for the blitz. However, the opposition Democratic Party “accused the spy agency of spreading unsubstantiated rumors to whip up support for a new anti-terrorism bill that would give it more power.”

In a media statement NIS said: “This is not a simple attack by an individual hacker, but appears to be thoroughly planned and executed by a specific organization or on a state level.”

But given the nature of the event, not all cybersecurity specialists are convinced of a North Korean provenance. Amit Yoran, the former director of DHS’ National Cybersecurity Division told ***Federal Computer Week***: “I think at this point it is highly unlikely, highly improbable that any reliable attack-attribution data is available. It’s a very intense process and it could take weeks. … The analysis here–both technical and nontechnical–is not trivial and takes time.”

In other words, NIS pronouncements should be taken with the proverbial grain of salt. After all, this is an agency with a repressive pedigree and its own dodgy agenda. “Trained-up fierce” by the CIA and the Pentagon, the South Korean intelligence service has been involved in some of the worst human rights abuses in East Asia.

According to a series of **reports** by investigative journalist Tim Shorrock, the agency was involved in the mass murder of their own citizens. In 1980, the Army’s feared “Black Beret” Special Forces and the KCIA were given a “green light” by Washington to suppress a pro-democracy uprising in the southern city of Kwangju in which some 2,000 students and workers were massacred; hundreds more were “disappeared,” tortured and imprisoned.

And with hostilities between Washington, Seoul and Pyongyang steadily on the rise, one cannot rule out the possibility that the cyberattacks are an exploitable *entré* by enterprising security agencies for further escalating the current crisis. Recent U.S. history is replete with examples of “intelligence and facts … being fixed around the policy.”

Fitting North Korea into the Frame

While the cyberassault “seemed to have come from South Korea,” *The Wall Street Journal* reports that American and South Korean officials are “trying to assess whether this is some random attack or the North Koreans might be working through a proxy, said the official.”

Just as likely however, someone or some entity may be trying to fit the repressive Stalinist regime into the frame.

Maneuvering to transform the thin gruel of fact into a meatier stew, Rodger Baker, the director of East Asian analysis at **Stratfor**, a private think-tank that describes itself as “the world leader in global intelligence” told ***Reuters*** the “timing of the cyber attacks raised suspicions about North Korea because it was around the U.S. Independence Day holiday and Pyongyang conducting missile tests.”

Another "expert," Nicholas Eberstadt, a senior researcher at the rightist American Enterprise Institute (**AEI**), linked the cyber blitz to a recent flurry of missile tests as well as to North Korea's recent test of a nuclear device. He told ***Asia Times***: "The general purpose was clear. When one looks at the nuclear chessboard, their security is integrally tied to cyber-warfare. … This strategy fits in integrally with tests of atomic devices."

Eberstadt's proof? He has none, but handily furnishes us with a speculative worst-case scenario that has the North launching a massive artillery and missile attack on major U.S. bases "in tandem with a full-scale cyber-offensive." In other words, Eberstadt has conjured up a digital bogeyman to scare the kiddies.

Such pronouncements are all the more remarkable given the decrepit state of the North's technological infrastructure. *Computerworld* **reported** July 10, there "are just over a million telephone lines installed in the country of 26 million people, home PCs are rare and Internet access is heavily restricted."

While the country has made IT expertise a priority, the publication averred that "North Korea's sophistication in hacking makes it less likely to be behind the attacks."

Despite something as trivial as evidence, Rep. Peter Hoekstra (R-MI), ranking Republican on the House Intelligence Committee, urged President Obama to launch a cyber attack against North Korea.

Hoekstra told the right-wing **America's Morning News** radio show on Friday, "some of the best people in America" had been investigating the attacks and have concluded that "all the fingers" point to North Korea as the culprit.

That Hoekstra's comments were showcased by the radio mouthpiece of *The Washington Times*, speak volumes to the agenda being pushed here.

The far-right news outlet is a wholly-owned subsidiary of clerical-fascist, the Rev. Sun Myung Moon and his Unification Church empire. With long-standing ties to Japanese and Korean fascists and war criminals, including reputed *yakuza* capo tutti capos Ryoichi Sasakawa and Yoshio Kodama, "Moon's Korea-based church got its first boost as an international organization when Kim Jong-Pil, the founder of the Korean Central Intelligence Agency, brokered a relationship between Moon and … Japan's leading rightist financiers," according to a definitive series of **reports** by investigative journalist Robert Parry.

Added Hoekstra, North Korea should be "sent a strong message."

"Whether it is a counterattack on cyber, whether it is, you know, more international sanctions … but it is time for America and South Korea, Japan and others to stand up to North Korea or the next time … they will go in and shut down a banking system or they will manipulate financial data or they will manipulate the electrical grid, either here or in South Korea," Hoekstra said. "Or they will try to, and they may miscalculate, and people could be killed."

Hoekstra's provocative statements echo remarks offered up by STRATCOM commander General Kevin Chilton. In May, Chilton suggested that "the White House retains the option to respond with physical force–potentially even using nuclear weapons–if a foreign entity conducts a disabling cyber attack against U.S. computer networks," according to a

disturbing **report** published by *Global Security Newswire*.

And with a vested interest in blaming their historic enemy for the cyberstrike, enterprising defense and security grifters on the southern side of the 38th parallel–and in Washington–have been hyping reports that the Stalinist regime is building a "cyber division" within the North Korean army.

Indeed, ***Bloomberg News*** reported that "South Korea's Defense Ministry plans to spend 489 billion won ($382 million) next year to beef up its defense against cyber warfare, the ministry said in a budget report today."

Who might benefit from such a large expenditure of *public* funds? Why *private* U.S. defense and security corporations of course!

Amongst the largest U.S. firms doing business with the South Korean Ministry of Defense, one finds the usual suspects. These include Boeing, Lockheed Martin, Northrop Grumman, General Dynamics, L3 Communications and Booz Allen Hamilton to name but a few of the dozens of corporations with a stake in the South Korean military bazaar. That all of the above-named entities are heavily-leveraged in the emerging cybersecurity market is hardly a coincidence.

The Korean Herald **reported** in its July 10 edition that "some experts here [are] now fingering hackers in the United States" as the culprits. Hong Min-pyo, the CEO of the security software firm Shiftworks who forensically examined the virus, "raised the possibility of the distributed denial of service attacks originating from a locale in the United States, which also was hit by the attacks."

Unlike corporate media here in the *heimat*, the *Herald* referenced critics who warned "against politicizing the latest cyber infections," including opposition Democratic Party lawmakers who "protested the passing of the anti-cyber terrorism bill citing invasion of privacy and internet censorship." The opposition demanded the government "offer concrete evidence to prove that North Korea was involved in the latest attacks."

But given the right-wing political offense currently underway in Seoul and Washington, opposition lawmakers may have a very long wait.

A Sociopath with a Keyboard and a Grudge … or Something More Sinister?

The unsophisticated nature of the attack should have alerted the media that any number of bad actors, particularly cybercriminals who specialize in transforming computers into zombie machines, or botnets, for their own nefarious purposes were prime suspects.

Computerworld **reported** July 8, that "an updated version of the MyDoom virus is responsible for a large DDOS (distributed denial of service) attack that took down major U.S. Web sites over the weekend and South Korean Web sites on Wednesday, according to Korean computer security company AhnLab."

Since its 2004 appearance, MyDoom has become "the fasted-spreading e-mail worm in Internet history." When a PC is infected with MyDoom, malicious code enables the program to harvest email addresses and mail itself out endlessly, the publication reports. According to AhnLab, the latest version contains an additional file with a list of web sites to be attacked.

Computerworld **reported** July 9, that infected systems also contain a destructive Trojan "programmed to encrypt user data or reformat the hard drive of a PC," thus erasing the evidence.

Joe Stewart, a researcher with **SecureWorks** who examined the code, told *Computerworld* that the botnet "does not use typical antivirus evasion techniques and does not appear to have been written by a professional malware writer."

Stewart told the publication that it is unusual to see low-profile state web sites being hit. "Who goes around targeting a site like the FAA or the U.S. Treasury? It's not something that most people would think to attack."

When contacted Friday for an update, Stewart told *Computerworld* there is "still zero evidence of North Korean involvement." Though relatively lengthy in duration, Stewart believes the attack could have been launched by a single person.

Who then might attack "low-profile web sites" such as the Federal Trade Commission for example?

According to ***Wired***, the FTC shut down an Internet Service Provider for its illegal and highly-lucrative hosting practices.

Identified as a "Black Hat" firm variously known as "Pricewert," "3fn.net" and "APS Telecom" the company was **accused** by the FTC June 3 of "actively recruiting" to its hosting service "thousands of 'rogue' web sites distributing 'illegal, malicious, and harmful electronic content including child pornography, spyware, viruses, trojan horses, phishing, botnet command and control servers, and pornography featuring violence, bestiality, and incest'."

Wired reported that the company "had thousands of servers" in the San Jose, Calif. area and the firm "actively shields its criminal clientele by either ignoring take-down requests issued by the online security community or shifting its criminal clients to other internet protocol addresses controlled by Pricewert so that they may evade detection."

The Washington Post **reported** June 3, that "Botnet experts … have found that 3FN housed many of the command and control networks for 'Cutwail,' one of the world's largest spam botnets. As late as mid-April, Joe Stewart, a botnet expert and director of malware research at SecureWorks, tracked nearly a dozen Cutwail control networks hosted at 3FN."

Which raises an uncomfortable question for security "experts" hyping North Korea's alleged "cybersecurity threat:" were the past week's attacks the work of a sociopath with a keyboard and a grudge, particularly if one of his/her botnets lost the critical command and control hubs that make spam, an illicit drugs market and Internet porn profitably sizzle?

While we may never know who actually launched the incursions, we just might have a slight inkling of who'll benefit. As *Antifascist Calling* **reported** July 6, plans are already afoot to roll-out Einstein 3, a Bush-era surveillance program to screen state computer traffic on private-sector networks.

In partnership with the Department of Homeland Security and the National Security Agency, communications, defense and security firms such as AT&T, General Dynamics, L3 Communications, MCI, Qwest, Sprint and Verizon stand to make billions from contracts

under the government's Managed Trusted Internet Protocol Services (MTIPS) program with its built-in "Einstein domain."

How's *that* for timing!

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****.*

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