GlobalResearch
Center for Research on Globalization

NSA Infects 50,000 Computer Systems Worldwide

By Stephen Lendman
Global Research, November 26, 2013

Theme: Intelligence, Police State & Civil Rights

Dutch newspaper NRC Handelsblad reported it, headlining "NSA infected 50,000 computer networks with malicious software."

It cited leaked Edward Snowden information. His revelations are the gift that keeps on giving. Activists representing him keep important information coming.

It's vital. Everyone needs to know. Unchecked NSA spying threatens fundamental freedoms. They're fast disappearing.

Their on the chopping block for elimination. Police state lawlessness runs America. It's too great a threat to ignore.

According to NRC, NSA hacked over 50,000 computer networks. It installed malware. It facilitates surveillance.

It's "designed to steal sensitive information." Snowden provided documents prove it. A 2012 management presentation showed NSA uses "Computer Network Exploitation (CNE) in more than 50,000 locations."

It secretly infiltrates computer systems through malware. Belgian telecom provider Belgacom was hacked.

Britain's Government Communications Headquarters (GCHQ) installed malware in its network. It did so to gain access to its customers' telephone and data traffic.

It did it through a false Linkedin page. It was done through unwitting company employees.

NSA has a "special department." It has over 1,000 military and civilian hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers.

It's top secret. It's called the Office of Tailored Access Operations (TAO). It identifies computer systems and supporting telecommunications networks to attack.

It successfully penetrated Chinese computer and telecom systems for around 15 years. It does the same thing globally.

Most NSA employees and officials know little or nothing about TAO. Its operations are extraordinarily sensitive. Only those needing to know are kept informed.

Special security clearances are required to gain access to its top secret work spaces. Armed guards keep others out.

Entering requires a correct six digit code. Retinal scanner checks are used. TAO targets foreign computer systems.

It collects intelligence by hacking, cracking passwords, compromising computer security systems, stealing hard drive data, and copying all subsequent emails and text messages.

NSA calls doing so Computer Network Exploitation (CNE). In October 2012, Obama issued a secret presidential directive. It selected overseas targets for cyber attacks.

His Offensive Cyber Effects Operations (OCEO) claimed to "offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

Washington "identif(ies) potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power."

It operates domestically the same way. NSA director Keith Alexander heads US Cyber Command (Cybercom). He's waging global cyberwar.

US Cyber Command (USCYBERCOM) has full operational control. It's a cyber hit squad. It's part of the US Strategic Command.

Rules of engagement are classified. Anything goes is policy. Cyber-warriors are freewheeling. They operate globally. Cyber-preemption reflects greater police state power.

TAO personnel penetrate, steal, damage, destroy or otherwise compromise targeted sites. It's perhaps the most important component of NSA's Signal Intelligence (SIGINT) Directorate.

NRC said TAO operations installed about 20,000 "implants" by early 2008. By mid-2012, they "more than doubled to 50,000."

NSA prioritizes cyber operations. "Computer hacks are relatively inexpensive." They give NSA information otherwise not available.

Malware "can remain active for years without" detection. " 'Sleeper cells' can be controlled remotely and be turned on and off at will."

Implants are digital sleeper cells. A "push of a button" activates them. NSA has been conducting these type operations since the late 1990s.

Dutch intelligence services AIVD and MIVD "displayed interest in hacking." In early 2013, a Joint Cyber Unit (JSCU) was created.

It's an inter-agency operation. It uses experts with a range of IT skills. It doesn't go as far as NSA. Dutch law prohibits it. For how long remains to be seen.

Last August, the Washington Post headlined "The NSA has its own team of elite hackers." It discussed TAO operations.

It may "have had something to do with (developing) Stuxnet and Flame malware program."

Washington and Israel were involved.

In spring 2010, Iranian intelligence discovered Stuxnet malware contamination. It infected its Bushehr nuclear facility. At the time, operations were halted indefinitely.

Israel was blamed. So was Washington. Had the facility gone online infected, Iran's entire electrical power grid could have been shut down.

Flame is a more destructive virus. Internet security experts say it's 20 times more harmful than Stuxnet. Iran's military-industrial complex is targeted.

So is its nuclear program. Maximum disruption is intended. Whether plans to do so continue remains to be seen. Iran is alerted to the possibility.

Leaksource calls itself the "#1 source for leaks around the world." Last August, it headlined "Codename GENIE: NSA to Control 85,000 'Implants' in Strategically Chosen Machines Around the World by Year End," saying:

According to "top secret documents" the Washington Post obtained, "US intelligence services carried out 231 offensive cyber-operations in 2011."

Doing so represents "the leading edge of a clandestine campaign that embraces the Internet as a theater of spying, sabotage and war."

Snowden leaked information revealed it. GENIE involves using computer specialists. They break into foreign networks. They do so to "put (them) under surreptitious US control."

"Budget documents say the $652 million project has placed 'covert implants,' sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions," said Leaksource.

GENIE's next phase involves an automated online system code-named "TURBINE." It's able to potentially manage "millions of implants."

It elevates intelligence gathering to a higher level. It lets it engage in widespread "active attack(s)."

Teams of FBI, CIA, and Cyber Command operatives work at NSA's Remote Operations Center (ROC).

Their missions overlap. So does NSA's National Threat Operations Center. It focuses on cyberdefense.

Snowden was involved as a Booz Allen Hamilton contractor. He learned NSA's best hacking techniques.

The agency designs most of its implants. It spends millions of dollars annually on "additional covert" "software vulnerabilities" purchases.

It gets them from "private malware vendors." They represent a growing source. They're largely European based.

China, Russia, Iran and North Korea are called the “most challenging targets” to penetrate.

Other prioritized countries include so-called terrorist safe havens. They include Afghanistan, Pakistan, Yemen, Iraq and Somalia.

NSA’s goal is sweeping. It wants to revolutionize data gathering. It wants to access “anyone, anywhere, anytime.”

It intends to “identify new access, collection and exploitation methods by leveraging global business trends in data and communication services.”

It wants total information control worldwide. It wants to go where no previous spy agency went before. It wants no operational restraints. It intends to keep doing whatever it wants.

Congress is a willing facilitator. Fake fix legislation facilitates NSA lawlessness. It codifies collecting phone records of hundreds of millions of Americans.

It permits the same thing online. It’s already out of committee. It’s heading for Senate passage.

Obama will sign into law whatever Congress sends him. He supports mass surveillance.

He’s waging war on fundamental freedoms. Police state lawlessness is official US policy. Obama is its leading exponent.

Stephen Lendman *lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net.*

His new book is titled “Banker Occupation: Waging Financial War on Humanity.”

http://www.claritypress.com/LendmanII.html

Visit his blog site at sjlendman.blogspot.com.

Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network.

It airs Fridays at 10AM US Central time and Saturdays and Sundays at noon. All programs are archived for easy listening.

http://www.progressiveradionetwork.com/the-progressive-news-hour

http://www.dailycensored.com/nsa-infects-50000-computer-systems-worldwide/

Articles by: **Stephen Lendman**

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.