GlobalResearch
Center for Research on Globalization

The National Security Agency: A Global Superpower

By Wayne Madsen
Global Research, June 14, 2013
Strategic Culture Foundation 13 June 2013

Theme: Intelligence, Police State & Civil Rights

Recent revelations that the U.S. National Security Agency is conducting massive meta-data vacuuming of the phone calls and Internet transactions of tens of millions of Americans and, perhaps, billions of people around the world, with little or no effective oversight by President Obama, the U.S. Congress, or the federal court system means that the intelligence agency has become, in its own right, a global superpower.

NSA acts like a virtual «state within a state». The director of NSA, a four-star flag officer, also wears the hat of Commander of the U.S. Cyber Command, the chief cyber-warfare echelon within the Department of Defense. Just as any nation-state, NSA also has alliances with similar signals intelligence and cyber-warfare agencies around the world, including Britain's Government Communications Headquarters (GCHQ), Australia's Defense Signals Directorate (DSD), Communications Security Establishment Canada (CSEC), and the Government Communications Security Board (GCSB) of New Zealand. These English-speaking partners are known as the «Five Eyes» countries and the signals intelligence alliance began after World War II and grew in scope during the Cold War.

NSA also has «third party» intelligence sharing agreements with a number of other signals intelligence agencies, but these smaller agencies are like NSA;'s very own colonial territories. Third party signals intelligence agencies of countries like Germany, Japan, South Korea, Denmark, Norway, Italy, Spain, and Thailand are expected to feed their intelligence «take» into the massive computer databases NSA maintains at its headquarters in Fort Meade, Maryland, but these Third Party entities receive very little intelligence in return. In fact, the Five Eyes «Second party» partners of NSA receive relatively little intelligence from NSA in exchange for the massive amounts of intercepted communications they make available to NSA. Even more secretive are NSA's «Fourth Party» partners, including neutral Sweden, Finland, Austria, and Switzerland and, in what may pose a problem for Snowden, last reportedly in Hong Kong, the People's Republic of China has been a «Fourth Party» partner of NSA since the early 1980s. NSA maintained two eavesdropping stations in western China directed against the nuclear testing facilities of the Soviet Union and then Russia.

It has been a common practice for NSA and its international partners to keep secret the activities of the NSA from even prime ministers. New Zealand Labor Party Prime Minister David Lange, who served in office from 1984 to 1989, stated that he and other ministers «were told so little « about the activities of NSA and GCSB and that this raised the question as to whom those concerned with international electronic surveillance saw themselves ultimately responsible. Later found in Lange's archived papers was a 31-page TOP SECRET UMBRA HANDLE VIA COMINT CHANNELS ONLY GCSB report on New Zealand's communications intercepts on behalf of NSA of targets in the South Pacific and Antarctica.

In 1975, when Australian Labor Party Prime Minister Gough Whitlam demanded information on the activities of NSA bases in Alice Springs and Woomera, Australia, the U.S., working with Australian intelligence, prevailed upon the Australian Governor General Sir John Kerr, to depose Whitlam and appoint the conservative and pro-U.S. opposition leader as prime minister. In effect, NSA ensured that a democratically-elected government was overthrown in a bloodless and seemingly constitutional coup d'état.

NSA's intelligence collections programs, including the PRISM meta-data vacuuming and storage and retrieval system exposed by NSA contractor whistleblower Edward Snowden, allegedly operate under U.S. government «oversight». However, the congressional oversight, the Intelligence Committees of the U.S. Senate and House of Representatives, are mere rubber stamp entities, as is the chief judicial oversight body, the Foreign Intelligence Surveillance Court (FISC). The FISC, which was established by the Foreign Intelligence Surveillance Act of 1978 in response to the surveillance abuses of the NSA, FBI, and CIA during the Lyndon Johnson and Richard Nixon presidencies, was tasked with ensuring that any use of NSA to conduct domestic surveillance was subject to a court order from the FISC. However, the FISC is a secret court and its decisions are classified. It has rarely denied a government request for a surveillance warrant in its entire history.

Internal NSA regulations intended to protect the communications of U.S. citizens from snooping largely went by the wayside after the 9/11 attack, an event that was extremely fortuitous for surveillance enthusiasts in the NSA top hierarchy.

After 9/11, NSA began to expand its operations and capabilities. Due to commence operations in September this year is a massive $2 billion NSA computing facility in Utah, known as «NSA Utah,» that will be able to process and store in a computer space the size of 17 football fields a yottabyte of data, which is equivalent to a quadrillion gigabytes of data. NSA Utah will be the mother lode of the NSA's PRISM meta-data, including communications intercepts and direct feeds from the servers of Microsoft, Google, Apple, Skype, Yahoo, Facebook, PalTalk, AOL, Youtube, and DropBox. There are reports that Twitter will soon be pressured to join the surveillance program. As influential as some of the aforementioned companies are, they are miniscule compared to the NSA superpower.

Joining NSA Utah will be an $860 million, 600,000 square feet, High Performance Computing Center at NSA's Fort Meade «campus» headquarters. There is another new NSA massive computing center at Oak Ridge National Laboratory in Tennessee. Adding to these are massive Regional Security Operations Centers (RSOCs) at facilities known as «NSA Georgia» in Fort Gordon, «NSA Texas» in San Antonio, and «NSA Hawaii» in Kunia on Oahu. It was at Kunia where Snowden gained access to classified documents on PRISM, NSA access to Verizon phone calls and emails, and a global interception system known as BOUNDLESSINFORMANT.

Classified maps of BOUNDLESSINFORMANT Global Access Operations (GAOs) show that the number one target for NSA surveillance is Iran, followed by Pakistan, with Jordan, Egypt, and India in third, fourth, and fifth place, respectively. Kenya, the country of President Barack Obama's paternal heritage, was the number one target for NSA surveillance in sub-Saharan Africa. Germany, a «third party» partner of NSA, tops all other countries in Europe as NSA's number one target. Other major NSA targets are Afghanistan, Iraq, China, Yemen, Saudi Arabia, and the United Arab Emirates. Astoundingly, NSA spies on the United States more than it does on Russia, North Korea, Somalia, Cuba, or Venezuela.

NSA's largest foreign operational center is in Menwith Hill, England. The Menwith Hill base works closely with GCHQ, which is headquartered in a massive structure in Cheltenham, England, which is nicknamed «The Doughnut» because of its shape. Others say the building looks like an eye. Not to be left behind, CSEC is building a C$880 million, 775,000 square feet new headquarters southeast of Ottawa. Australia's DSD operates a large satellite communication intercept facility in Geraldton, West Australia.

Rather than curtail the powers of NSA after the Cold War, the U.S. Congress and Bush I, Clinton, Bush II, and Obama administrations have presided over the omniscient agency's expansion and greater powers of surveillance. NSA has an internal security force, the «Q Group,» that conducts its own investigations with or without the assistance of the FBI. NSA is the second largest employer in the state of Maryland, surpassed only by the U.S. Postal Service. NSA's clout as an employer allows the agency to run roughshod over elected state officials and members of Maryland's congressional delegation. In Maryland, there is no such thing as saying «no» to the NSA.

NSA's cyber-warriors have the capability to shut down banking networks, generate power blackouts to major metropolitan regions, throw a «kill switch» on the Internet in particular countries and regions, and manipulate vote counting and election results reporting. There is very little independent oversight of these dangerous operations.

Edward Snowden claims that an NSA operator with the necessary «authorities» or access rights can read the personal email of anyone, including the President of the United States. If a low-level technician like Snowden could read such personal email or listen in on private phone calls, the capability of NSA to blackmail politicians from Maine to California and Argentina to Zambia stands as a stark example of the power that is in the hands of the NSA director. It is also worrisome that NSA's current commander, U.S. Army General Keith Alexander, attended the elitist and secretive Bilderberg Conference in 2012, 2011, 2010, 2009, and 2008. As David Lange once asked, «to whom do those who have the power of total surveillance see themselves ultimately responsible?» NSA's General Alexander appears to be beholden more to the unelected wealthy and privileged doyens of capitalism than to either the American people or their elected representatives in the Congress.

Articles by: Wayne Madsen