NSA: The finder and keeper of countless US secrets

June 9 2013, by Kimberly Dozier

In this Sept. 23, 2010, file photo Army Gen. Keith B. Alexander, then-commander of the U.S. Cyber Command, testifies about cyberspace operations during a hearing on Capitol Hill in Washington. "More times than we can count, we've made history, without history even knowing we were there," reads a quote on the National Security Agency's web page by current NSA director Alexander. The NSA's experts include mathematicians, and cryptologists, who do everything from breaking codes to learning and translating multiple foreign languages, as well as computer hackers who engage in offensive attacks. (AP Photo/Manuel Balce Ceneta, File)

An email, a telephone call or even the murmur of a conversation captured by the vibration of a window—they're all part of the data that can be swept up by the sophisticated machinery of the National Security Agency.

Its job is to use the world's most cutting edge supercomputers and arguably the largest database storage sites to crunch and sift through immense amounts of data. The information analyzed might be stolen from a foreign official's laptop by a CIA officer overseas, intercepted by a Navy spy plane flying off the Chinese coast, or, as Americans found out this past week, gathered from U.S. phone records.

Code-breakers at the Fort Meade, Maryland-based NSA use software to search for keywords in the emails or patterns in the phone numbers that might link known terrorist targets with possible new suspects. They farm out that information to the 16 U.S. intelligence agencies and to law enforcement, depending on who has the right to access which type of information, acting as gatekeeper, and they say, guardian of the nation's civil liberties as well as its security.

The super-secret agency is under the spotlight after last week's revelations of two surveillance programs. One involves the sweeping collection of hundreds of millions of phone records of U.S. customers. The second collects the audio, video, email, photographic and Internet search usage of foreign nationals overseas—and probably some Americans in the process—who use major Internet companies such as Microsoft, Google, Apple, and Yahoo.

The NSA was founded in 1952. Only years later was the NSA publicly acknowledged, which explains its nickname, "No Such Agency."

According to its website, NSA is not allowed to spy on Americans. It is supposed to use its formidable technology to "gather information that America's adversaries wish to keep secret," and to "protect America's vital national security information and systems from theft or damage by others," as well as enabling "network warfare, a military operation," that includes offensive cyberoperations against U.S. adversaries.

The agency also includes the Central Security Service, the military arm of code-breakers who work jointly with the agency. The two services have their headquarters on a compound that's technically part of Fort Meade, though it's slightly set apart from the 5,000-acre (2,000-hectare) Army base.

Visible from a main highway, the tightly guarded compound requires the highest of clearances to enter and is equipped with electronic means to ward off an attack by hackers.

Other NSA facilities in Georgia, Texas, Colorado and Hawaii duplicate much of the headquarters' brain and computer power in case a terrorist attack takes out the main location, though each one focuses on a different part of the globe.

A new million-square-foot (90,000-square-meter) storage facility in Salt Lake City will give the agency untold additional capacity to store the massive amounts of data it collects, as well as adding to its analytical capability.

"NSA is the elephant of the U.S. intelligence community, the biggest organization by far with the most capability and (literally) the most memory," said former senior CIA official Bruce Riedel, who now runs the Brookings Intelligence Project.

NSA's experts include mathematicians and cryptologists, a term that

means everything from breaking codes to learning and translating multiple foreign languages. There also are computer hackers who engage in offensive attacks like the one the U.S. and Israel are widely believed to have been part of, planting the Stuxnet virus into Iranian nuclear hardware, damaging Iran's nuclear development program in 2010.

In this June 6, 2013 file photo National Security Agency plaques are seen at the compound at Fort Meade, Md. The NSA was founded in 1952 but only publicly acknowledged years later, which explains its nickname "No Such Agency." It includes the Central Security Service, the military arm of code breakers who work jointly with NSA. Visible from a main highway, the tightly guarded compound requires the highest of clearances to enter, and is equipped with various electronic means to ward off an attack by hackers. (AP Photo/Patrick Semansky, File)

Then there are "siginters," the signals intelligence experts who go to war

zones to help U.S. troops break through encrypted enemy communications or work with a CIA station chief abroad, helping tap into a foreign country's phone or computer lines.

"More times than we can count, we've made history, without history even knowing we were there," reads a quote on the NSA's Web page by the current director, Gen. Keith Alexander.

NSA workers are notoriously secretive. They're known for keeping their families in the dark about what they do, including their hunt for terrorist mastermind Osama bin Laden. NSA code-breakers were an essential part of the team that tracked down bin Laden at a compound in Pakistan in 2011.

Their mission tracking al-Qaida and related terrorist groups continues, with NSA analysts and operators sent out to every conflict zone and overseas U.S. post, in addition to surveillance and analysis conducted at headquarters outside Washington.

The director of national intelligence, James Clapper, said in a statement Saturday that the NSA's programs do not target U.S. citizens. But last week's revelations show that the NSA is allowed to gather U.S. phone calls and emails and to sift through them for information leading to terrorist suspects, as long as a judge signs off. Lawmakers are questioning the scope of the information gathered, and how long and how much of it is kept.

"Does that data all have to be held by the government?" asked Sen. Angus King, a member of the Senate Intelligence Committee.

King, a Maine independent, was briefed on the program this past week, but would not discuss how long the government holds on to the phone records. "I don't think there is evidence of abuse, but I think the program

can be changed to be structured with less levels of intrusion on the privacy of Americans," he said.

While NSA has deferred any public comment to Clapper, it offered an internal article written by director of compliance John DeLong, who's is in charge of making sure NSA protects Americans' privacy.

DeLong writes that privacy protections are being written into the technology that sifts the information, "which allows us to augment—not wholly replace—human safeguards." The NSA also uses "technology to record and review our activities. ... Sometimes, where appropriate, we even embed legal and policy guidance directly into our IT architecture."

In this Sept. 23, 2010, file photo Army Gen. Keith B. Alexander, then-commander of the U.S. Cyber Command, center right, arrives at a Capitol Hill committee hearing in Washington to testify about cyberspace operations.

Alexander now directs the National Security Agency, whose job it is to use the world's most cutting edge supercomputers and arguably the largest database storage sites to crunch and sift through terabytes of data, whether it was stolen from a foreign official's laptop by a CIA officer overseas, or intercepted by a Navy spy plane flying off the Chinese coast, or, as Americans found out this week, secreted from your personal phone records. (AP Photo/Manuel Balce Ceneta, File)

What that means is that the data sifting is mostly done not by humans, but by computers, following complicated algorithms telling them what to look for and who has a right to see it.

"Through software, you can search for key words and key phrases linking a communication to a particular group or individual that would fire it off to individual agencies that have interest in it," just like Amazon or Google scans millions of emails and purchases to track consumer preferences, explained Ronald Marks, a former CIA official and author of "Spying in America in the Post 9/11 World."

Detailed algorithms try to determine whether something is U.S. citizen-related or not. "It shows analysts, 'we've got a US citizen here, so we've got to be careful with it,'" he said.

Another way counterterrorist officials try to protect U.S. citizens is through centers where operators from the military, CIA, NSA, FBI, Treasury and others sit side by side. When one comes across information that his or her agency is not supposed to access, it's turned over to someone in the center who's authorized to see it.

But the process isn't perfect, and sometimes what should be private information reaches agencies not authorized to see it.

"When information gets sent to the CIA that shouldn't, it gets destroyed, and a note sent back to NSA saying, 'You shouldn't have sent that,'" Marks said. "Mistakes get made, but my own experience on the inside of it is, they tend to be really careful about it."

Analysts need that level of detail because they are no longer looking for large networks, but small cells or individuals that carry out "lone wolf" attacks, as the Boston Marathon bombing is thought to have been.

"If we are going to fight a war or low intensity conflict that has gone down to the level of individual attacks by cells of one or two people, if you are looking for total risk management, this is the kind of thing you're going to have to do," Marks said.