Digital age expanded the NSA's mission

July 8 2013, by Ken Dilanian

It wasn't long ago that the National Security Agency, the intelligence agency responsible for intercepting global communications, seemed overwhelmed by the Internet.

"We in the NSA are encountering problems with the flood of information," Eric Haseltine, then the NSA director of research, said in a 2004 speech. "We can either be drowned by it, or we can get on our surfboard and let it propel us."

NSA chose the surfboard. Or rather, many of them.

Determined to identify and track al-Qaida terrorists and to prevent another attack after Sept. 11, 2001, the NSA set about vastly enlarging its ability to capture, store and exploit the ocean of texts, emails, videos and other electronic communications.

"They took on a new mission that required sifting vast amounts of data to find a few important signals," said Stewart Baker, who was the NSA's general counsel from 1992 to 1994 and held top Homeland Security Department jobs in the George W. Bush administration.

Today the NSA secretly siphons an almost unimaginable number of foreign government, corporate and private communications from the World Wide Web, according to the trove of classified material disclosed by Edward Snowden, the fugitive former NSA contractor. One document leaked last week revealed that NSA computers take in 500 million "communications connections" per month in Germany alone.

That has made the NSA, already the largest U.S. intelligence agency in terms of personnel, even more important for policymakers.

About 60 percent of the president's daily brief, the highly classified intelligence summary delivered to the White House each morning, was based as of 2000 on "signals intelligence," or intercepted communications, according to a declassified NSA document from December of that year.

The NSA portion has increased since then, former officials say.

"Over the last 10 years, because of the Internet gold mine, signals intelligence has become the primary vehicle for U.S. intelligence collection," said James Lewis, director of the technology and public policy program at the nonpartisan Center for Strategic and International Studies in Washington.

The Snowden disclosures have revealed that the NSA intercepts foreign Internet traffic that passes through digital pipelines or servers in the U.S., both by directly tapping high-capacity fiber-optic cables that much of the world uses and by using secret court warrants to obtain material from Google, Yahoo, Apple, Microsoft and other U.S. technology, online storage and social media companies.

Two unidentified U.S. companies in particular "enable NSA to access large volumes of foreign-to-foreign communications transiting the United States through fiber-optic cables, gateway switches, and data networks," according to a 2009 draft report from the NSA inspector general that was among the Snowden documents.

The NSA also targets computer systems, fiber-optic companies and telecom providers in other countries, officials said.

Modern spying "isn't just the passive collection of signals someone else decides to transmit," former NSA Director Michael Hayden said in an email. "With the modern Web we're often able to 'commute' to the target. And frankly, I think we're the best in the world at it."

American emails and other communications inevitably are swept into the Internet, current and former intelligence officials say.

Unless a court specifically authorizes eavesdropping, communications that are inadvertently captured from "U.S. persons" must by federal policy be discarded or subject to special handling known as "minimization" to restrict who can learn the American's identity.

The Guardian recently disclosed another secret NSA program, code named EvilOlive, that collects Internet metadata - not content, but email headers showing the "to" and "from" fields, and computer addresses when one end of the communication was in the U.S.

"This milestone ... allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories," the NSA reported in December, according to The Guardian.

Joel Brenner, former NSA senior counsel, suggests such surveillance is far from foolproof. "What makes anybody think that the NSA can get it all, and secondly, that they can look at it all?" he asked.

According to the Snowden disclosures, the agency also collects and stores toll records of nearly all telephone calls by Americans. NSA officials say they only use the metadata - phone numbers, length of a call and other details, but not the callers' names or recordings of any conversations - in investigations of terrorism or foreign espionage.

Gen. Keith Alexander, head of the NSA, recently testified that the

classified collection systems had helped avert or disrupt more than 50 potential terrorist incidents around the globe, including about 10 in the U.S.

Getting the data has always been easier than making sense of it. So the NSA developed its own tools to tap the vast pools of information.

In 2008, agency engineers created Accumulo, a data storage and retrieval system based on Google's Big Table system. Sqrrl Data, a start-up company in Cambridge, Mass., this month began a commercial version of Accumulo for real-time data mining. Most of the founders are former NSA employees.

Accumulo allowed the NSA to examine disparate data sets and find connections, said a former NSA operator who worked with it.

"You got better answers immediately," he said.

But the NSA suffers from "stovepiping" of operations, said the former operator, who was not authorized to discuss the operations publicly.

Phone intercepts are a separate program from email metadata, which is distinct from analysis of cyber threats. Like any large bureaucracy, he said, the NSA is not as nimble as a start-up.

"It's like turning an aircraft carrier," he said.

©2013 Tribune Co.
Distributed by MCT Information Services

Citation: Digital age expanded the NSA's mission (2013, July 8) retrieved 26 April 2024 from https://phys.org/news/2013-07-digital-age-nsa-mission.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.