NSA eyes encryption-breaking 'quantum' machine

January 3 2014

The shadow of US Army General Keith Alexander, commander of US Cyber Command and director of the National Security Agency (NSA), is seen as he delivers keynote remarks September 25, 2013 during the Cybersecurity Summit in Washington, DC

The US National Security Agency is making strides toward building a "quantum computer" that could break nearly any kind of encryption, The Washington Post reported Thursday.

The Post said leaked documents from fugitive ex-NSA contractor Edward Snowden indicate the computer would allow the secret intelligence agency to break encryption used to protect banking, medical, business and government records around the world.

Quantum computing has been a goal among commercial firms such as IBM because it could harness the power of atoms and molecules, vastly increasing speed and security of computers and other devices.

But experts cited by the newspaper said it was unlikely that the NSA would be close to creating such a machine without the scientific community being aware of it.

"It seems improbable that the NSA could be that far ahead of the open world without anybody knowing it," Scott Aaronson of the Massachusetts Institute of Technology told the daily.

The NSA declined to comment on the report.

The Post said the leaked documents indicate that the agency carries out research in large, shielded rooms known as Faraday cages designed to prevent electromagnetic energy from entering or exiting.

Because of its vast computing power, a working quantum computer would break the strongest encryption tools in use today for online activities, including banking and emails.

Some technology firms such as Google and Yahoo have said in recent weeks that they were stepping up efforts to encrypt their communications following reports that the NSA had been able to break or circumvent many of the current encryption standards.

A September report by The New York Times, ProPublica and The

Guardian, also based on leaked documents, said US and British spy agencies are able to decipher data even with the supposedly secure encryption to make it private.

The documents indicated that the NSA, working with its British counterpart GCHQ, accomplished the feat by using supercomputers, court orders and some cooperation from technology companies.

If the reports are accurate, the highly secretive program would defeat much of what is used to keep data secure and private on the Internet, from emails to chats to communications using smartphones.

IBM researchers said last year they had made advances in quantum computing that has the potential to outperform any existing supercomputer.

The new type of computing uses information encoded into quantum bits or qubits, putting into use a theory that scientists have been discussing for decades.

Quantum computing expands on the most basic piece of information that a typical computer understands—a bit, and thereby can perform millions of calculations at once.

Citation: NSA eyes encryption-breaking 'quantum' machine (2014, January 3) retrieved 25 April 2024 from https://phys.org/news/2014-01-nsa-eyes-encryption-breaking-quantum-machine.html