PATRICK SEMANSKY/AP

The National Security Agency is the largest employer of mathematicians in the United States.

SECURITY

Researchers split over NSA hacking

Cryptographers condemn US National Security Agency's tapping and tampering, but mathematicians shrug.

BY ANN FINKBEINER

The US National Security Agency (NSA) has upset a great many people this year. Since June, newspapers have been using documents leaked by former intelligence worker Edward Snowden to show how the secretive but powerful agency has spied on the communications of US citizens and foreign governments. Last month, the media reported that the NSA, which is based in Fort Meade, Maryland, had undermined Internet security standards. The revelations have sparked international outrage at the highest levels — even the president of Brazil cancelled a visit to the United States because of the spying.

Yet amid the uproar, NSA-supported mathematicians and computer scientists have remained mostly quiet, to the growing frustration of others in similar fields. "Most have never met a funding source they do not like," says Phillip Rogaway, a computer scientist at the University of California, Davis, who has sworn not to accept NSA funding and is critical of other researchers' silence. "And most of us have little sense of social responsibility."

Mathematicians and the NSA are certainly interdependent. The agency declares that it is the United States' largest maths employer, and Samuel Rankin, director of the Washington DC office of the American Mathematical Society, estimates that the agency hires 30–40 mathematicians every year. The NSA routinely holds job fairs on university campuses, and academic researchers can work at the agency on sabbaticals. In 2013, the agency's mathematical sciences programme offered more than US$3.3 million in research grants.

Furthermore, the NSA has designated more than 150 colleges and universities as centres of excellence, which qualifies students and faculty members for extra support. It can also fund research indirectly through other agencies, and so the total amount of support may be much higher. A leaked budget document says that the NSA spends more than $400 million a year on research and technology — although only a fraction of this money might go to research outside the agency itself.

Many US researchers, especially those towards the basic-research end of the spectrum, are comfortable with the NSA's need for their expertise. Christopher Monroe, a physicist at the University of Maryland in College Park, is among them. He previously had an NSA grant for basic research on controlling cold atoms, which can form the basis of the qubits of information in quantum computers. He notes that he is free to publish in the open literature, and he has no problems with the NSA research facilities in physical sciences, telecommunications and languages that sit on his campus. Monroe is sympathetic to the NSA's need to track the development of quantum computers that could one day be used to crack codes beyond the ability of conventional machines. "I understand what's in the newspapers," he says, "but the NSA is funding serious long-term fundamental research and I'm happy they're doing it."

Dena Tsamitis, director of education, outreach and training at Carnegie Mellon University's cybersecurity research centre in Pittsburgh, Pennsylvania, also wants to maintain the relationship. She oversees visitors and recruiters from the NSA but her centre gets no direct funding. She says that her graduate students understand the NSA's public surveillance to be "a policy decision, not a technology decision. Our students are most interested in the technology." And the NSA, she says — echoing many other researchers — "has very interesting technology problems".

The academics who are professionally uneasy with the NSA tend to lie on the applied end of the spectrum: they work on computer security and cryptography rather than pure mathematics and basic physics. Matthew Green, a cryptographer at Johns Hopkins University in Baltimore, Maryland, says that these researchers are unsettled in part because they are dependent on protocols developed by the US National Institute of Standards and Technology (NIST) to govern most encrypted web traffic. When it was revealed that the NSA had inserted a 'back door' into the NIST standards to allow snooping, some of them felt betrayed.

"I understand what's in the newspapers, but the NSA is funding serious long-term fundamental research and I'm happy they're doing it."

"We certainly had no idea that they were tampering with products or standards," says Green. He is one of 47 technologists who on 4 October sent a letter to the director of a group created last month by US President Barack Obama to review NSA practices, protesting because the group does not include any independent technologists.

Edward Felten, who studies computer security at Princeton University in New Jersey, says that the NSA's breach of security standards means that cryptographers will need to change what they call their threat model — the set of assumptions about possible attacks to guard against. Now the attacks might come from the home team. "There was a sense of certain lines that NSA wouldn't cross," says Felten, "and now we're not so sure about that." ■

© 2013 Macmillan Publishers Limited. All rights reserved