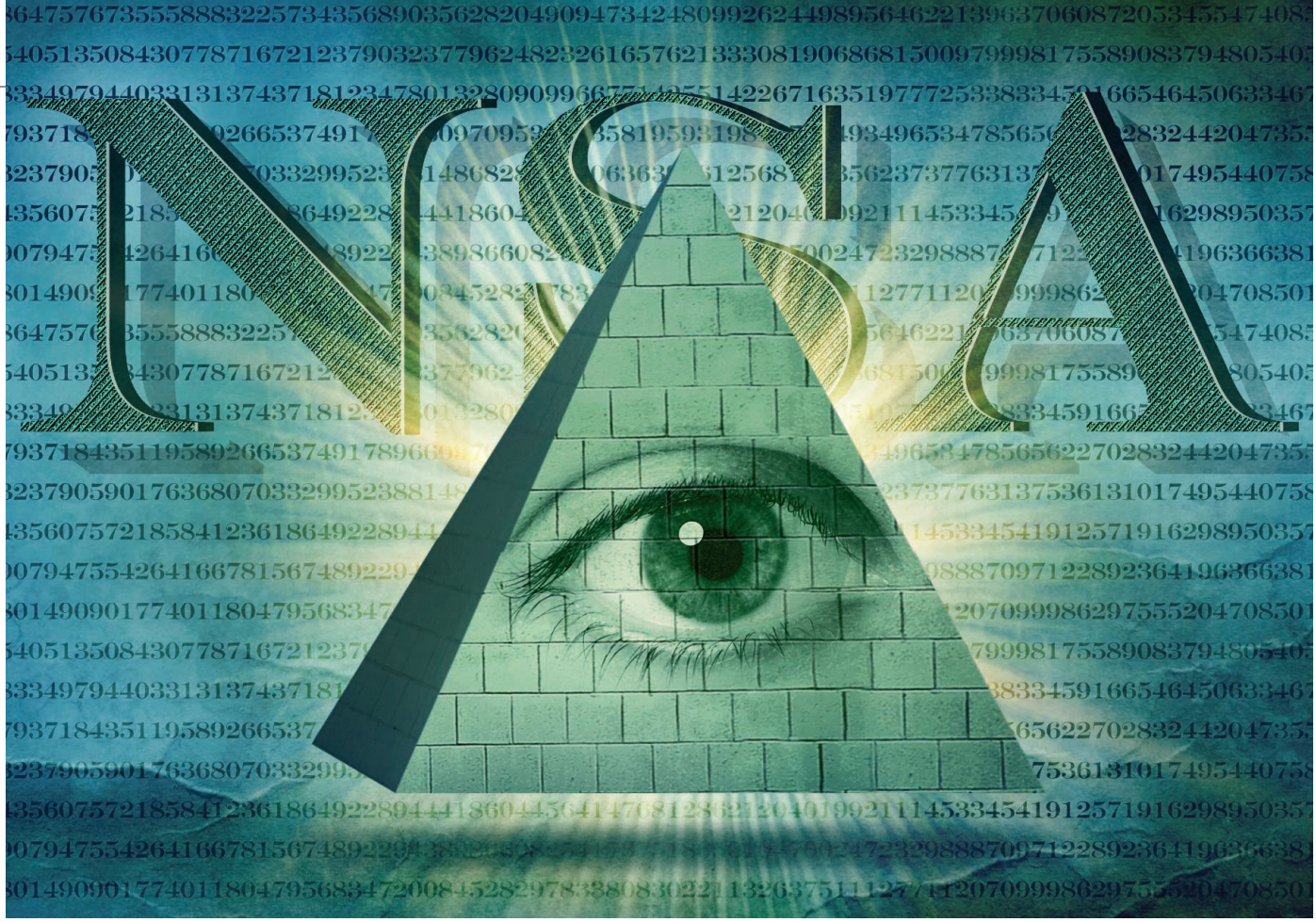


BREACH OF TRUST

After the Snowden revelations, U.S. mathematicians are questioning their long-standing ties with the secretive National Security Agency

By **John Bohannon**

Each year, recruiters from the National Security Agency (NSA), said to be the largest employer of mathematicians in the United States, visit a few dozen universities across the country in search of new talent. It used to be an easy sell. "One of the appealing aspects that they pitch is that you'll be working on incredibly hard and interesting puzzles all day," says one mathematician who requested anonymity. In the wake of the terrorist attacks of 11 September 2001, he adds, "I felt that if there was any way I could use my mathematical ability to prevent such a thing from ever happening again, I was morally obligated to do it." Several times over the past decade, he has set aside his university research to work for the agency.

Lately, however, that sense of moral clarity has clouded for some mathematicians, and the recruiters' task has become more complicated. In 2013, former NSA contractor Edward Snowden began releasing documents revealing, among other things, that the agency has been harvesting e-mail and phone records from ordinary American citizens on a massive scale. NSA may have also purposefully compromised a mathematical standard used widely for securing personal computers the world over.

The revelations unsettled the anonymous mathematician. "For people who share my motivations," he says, "the ethics of the NSA's mission matter a great deal." The news has also roiled the mathematics community and led some to question its long, symbiotic relationship with the spy agency, which nurtures budding mathematicians in school, supports the field with research and training grants, and offers academic mathematicians the chance to take part in the murky world of spy craft. Mathematician David Vogan of the Massachusetts Institute of Technology in Cambridge, who finishes his term as president of the American Mathematical Society (AMS) this week, has urged the society to rethink its long-running, close-knit ties with the agency—though he won little support from other AMS officials.

In a sign of the difficulty of convincing the most talented mathematicians and computer scientists to work for the agency, NSA Director Admiral Michael Rogers has hit the road himself to make the pitch. "Many of you are potential future employees that I want to compete for," he told an audience at Stanford University in Palo Alto, California, last November. "The biggest challenge for us ... is getting people in the door in this environment." A student in the audience asked

IMAGE: WILLIAM DUKE

what NSA offers to researchers who may be "disillusioned by the U.S. government." In a reply that may not have helped, Rogers listed both the chance to "serve the nation" and "the opportunity to do some neat stuff that you can't legally do anywhere else."

"THE NSA NEEDS MATHEMATICIANS like a papermaker needs trees," Vogan says. The number of mathematicians employed by the agency cannot be verified. But its total staff is known to be in the tens of thousands, and its official mission—to design cryptologic systems for protecting U.S. information while exploiting weaknesses in the information systems of foreign countries—is deeply mathematical. Since NSA was established in 1952, it has engaged in a mathematical arms race, with ever more sophisticated code-making and code breaking. As NSA has long affirmed, it has a vested interest in maintaining a healthy domestic mathematics community.

Like the rest of its activities, the full extent of NSA's involvement with academia is secret. "We do not release specific budgets for programs," the agency's public affairs office said in response to e-mail queries from *Science*. Even the total annual budget that Congress provides the agency is classified information; estimates have ranged from $8 billion to $25 billion.

Only one line item in the NSA budget is publicly reported each year, and only because it involves a grants program for which AMS provides peer review. Through its Mathematical Sciences Program, the agency will spend $4 million this year on research grants, summer internships for undergraduates, sabbaticals for university professors to work at NSA, and mathematical conferences. It's a pittance compared with the more than $400 million that mathematicians receive each year from other federal agencies. But for a handful of areas that benefit, such as number theory and probability, "it's not a trivial amount of money," Vogan says.

The fruits of NSA support are readily found in academic journals. "It is expected that you will acknowledge the funding in your papers," says Egon Schulte of Northeastern University in Boston, whose research in combinatorics is supported by an NSA grant. That makes it possible to directly track the academic output of NSA funding.

An analysis by *Science* of academic papers indexed on Google Scholar (see graph, below) shows that NSA-supported research output grew steadily through the Cold War and the fall of the Soviet Union, dropped briefly between 1999 and 2002, then mushroomed in the wake of the 9/11 terrorist attacks. In 2013, more than 500 papers acknowledged NSA support.

But direct grants for individual researchers are only a tiny portion of NSA's support for mathematics. Documents that the agency shared with *Science* describe a broad range of academic programs, from STEM (science, technology, engineering, and mathematics) education in schools to research labs at universities. NSA experts give classroom talks and judge science fairs. A small competitive grants program supports science summer camps and high school math clubs and computer labs. And an NSA program called GenCyber brings some of the most talented high school students and their teachers to universities to focus on "cyber-related education and careers" with help from NSA experts.

The outreach helps the agency develop a close relationship with the brightest mathematicians at the start of their careers. "What we found is that the sooner you get in contact with students, the better chance you have to employ them," NSA's then-director of human resources, Harvey Davis, told Congress in a 2002 hearing. Davis also pointed to the agency's cozy ties with higher education. "We are locked in with key professors who make decisions at the universities as well as the math community throughout the country."

At the 55 universities designated by NSA as Centers of Academic Excellence, a full-time NSA "representative" is embedded on campus. According to the documents provided to *Science*, they serve as the "gateway" for the agency to "influence research and research partnerships that will impact the cyber world and workforce in the future." NSA's target campuses include well-known private institutions such as Princeton University, New York University, and Carnegie Mellon University, as well as many public ones such as North Carolina State University, Pennsylvania State University, and the University of California, Davis.

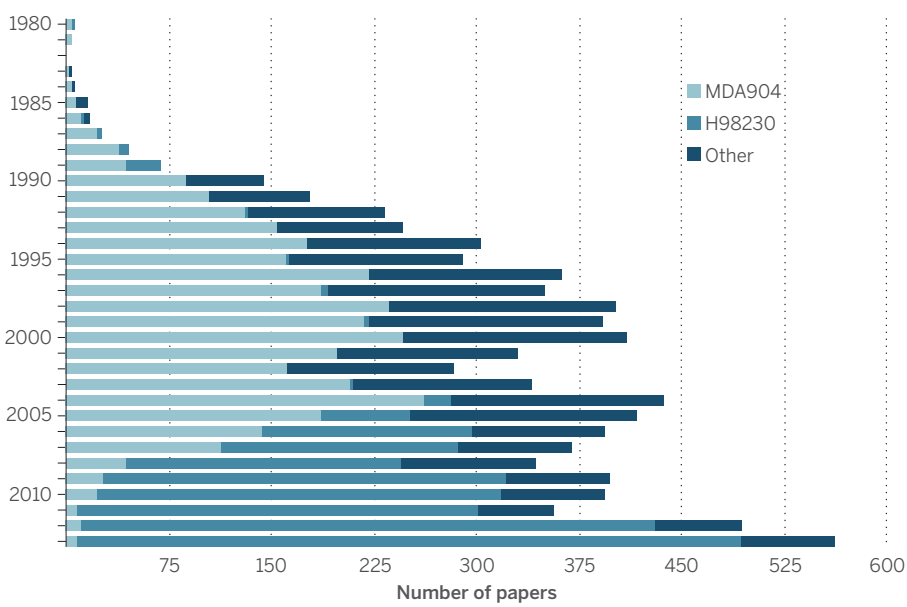
Some universities also receive significant funding from NSA to support research and training. For example, NSA is creating what it calls lablets, research groups within academic departments focused on cybersecurity. According to press releases from the universities, each has received between $2.5 million and $4.5 million so far, but again, the total budgets are unclear.

This close relationship with academia stirred little controversy until recently, says Thomas Hales, a mathematician at the University of Pittsburgh in Pennsylvania. "Everyone knows colleagues who have worked for the NSA." After stints at the agency, "they seem to get amnesia about what they were working on," he quips, but with few exceptions, "no one really cared." That changed in 2013, when mathematicians got a glimpse of how the agency was using some of their work.

IN THE WAKE of the Snowden revelations, most of the media attention has focused on NSA's large-scale harvesting of data from U.S. citizens. But it is a more obscure exploit

Follow the money

The number of research papers indexed by Google Scholar that acknowledge NSA support was falling at the time of the 11 September 2001 terrorist attacks, then rebounded strongly. *Science* performed this analysis using an open-source program called scholar.py created by Christian Kreibich of the International Computer Science Institute. The two main NSA grant codes that emerge are MDA904 and H98230.



GRAPH: JOHN BOHANNON/*SCIENCE*

that concerns Hales and many other mathematicians: what they see as an attack on the very heart of modern Internet security.

When you check your bank account online, for example, the information is encrypted using a series of large numbers generated by both the bank server and your own computer. Generating random numbers that are truly unpredictable requires physical tricks, such as measurements from a quantum experiment. Instead, the computers use mathematical algorithms to generate pseudorandom numbers. Although such numbers are not fundamentally unpredictable, guessing them can require more than the world's entire computing power. As long as those pseudorandom numbers are kept secret, the encoded information can safely travel across the Internet, protected from eavesdroppers—including NSA.

But the agency appears to have created its own back door into encrypted communications. The computer industry, both in the United States and abroad, routinely adopts security standards approved by the National Institute of Standards and Technology (NIST). But in 2006, NIST put its seal of approval on one pseudorandom number generator—the Dual Elliptic Curve Deterministic Random Bit Generator, or DUAL_EC_DRBG—that was flawed. The potential for a flaw was first identified in 2007 by Microsoft computer security experts. But it received little attention until internal NSA memos made public by Snowden revealed that NSA was the sole author of the flawed algorithm and that the agency worked hard behind the scenes to make sure it was adopted by NIST.

"[A]n algorithm that has been designed by NSA with a clear mathematical structure giving them exclusive back door access is no accident," Hales wrote in an open letter published by AMS in February 2014. He tells *Science* that since then, "my conclusions have been reinforced by other sources." For example, a July 2014 NIST report suggested that NIST was all but following orders from the intelligence agency. "NSA's vastly superior expertise on elliptic curves led NIST to defer to NSA regarding DUAL_EC," the report said. Research by academic mathematicians has also revealed that the flaw is easier to exploit if the targeted computer uses other security products that were designed at the request of NSA. NIST dropped its support for the faulty standard in April last year. NSA has not made a public statement about it.

Some defended the agency. In an open letter in AMS's online journal, *Notices of the American Mathematical Society*, Richard George, who describes himself as a mathematician who worked for NSA for 41 years, declared that his NSA colleagues "would not dream of violating U.S. citizens' rights," although "there may be a few bad apples in any set of people." As for NSA's engineering of a back door into personal computers, George wrote: "I have never heard of any proven weakness in a cryptographic algorithm that's linked to NSA; just innuendo."

In the pages of *Notices*, the revelations triggered a sharp debate about whether the society should cut its ties with the agency. Alexander Beilinson, a mathematician at the University of Chicago in Illinois who helped spur the discussion, argued that the society should completely wash its hands of NSA. The scale of the domestic spying and software tampering makes the United States seem like "a bloated version of the Soviet Union of the time of my youth," he says. Vogan, AMS's president, was outraged as well. "The NSA may have deliberately broken commercial encryption software," he says. "I see this activity as parallel to falsification of medical research for profit: as an individual wrong action, which damages permanently the position of science in the world."

But after all was said and done, no action was taken. Vogan describes a meeting about the matter last year with an AMS governing committee as "terrible," revealing little interest among the rest of the society's leadership in making a public statement about NSA's ethics, let alone cutting ties. Ordinary AMS members, by and large, feel the same way, adds Vogan, who this week is handing over the presidency to Robert Bryant, a mathematician at Duke University in Durham, North Carolina. For now, U.S. mathematicians aren't willing to disown their shadowy but steadfast benefactor. ■

IMAGE: WILLIAM DUKE

THE PRIVACY ARMS RACE

Game of drones

By **David Shultz**

Lately, drones seem to be everywhere. They're monitoring endangered wildlife, launching missiles, mapping rainforests, and filming athletes. They can fly high above a neighborhood or just hover outside a bedroom window. The Defense Advanced Research Projects Agency has already built robotic fliers not much larger than an insect; once batteries become small enough, they may become quite literally a fly on the wall. The opportunities—and potential violations of privacy—seem endless. But current and new laws may offer some protection.

In the United States, the Supreme Court has concluded that nobody owns the airways and anyone can take pictures in public. As a result, citizens have been convicted of growing marijuana in their own backyards based on naked-eye observations made from planes flying overhead in "public navigable airspace." On the other hand, a newly proposed law in California would make it illegal for paparazzi to use drones to snap pictures of celebrities on their own property.

Existing laws also ban a peeping Tom from setting up in a tree at the edge of your property and peering into your bathroom window with binoculars; the same laws are likely to extend to flying a drone outside the same window. The Fourth Amendment, which protects citizens inside their homes from unreasonable searches and seizures without a warrant, may shield Americans from miniature government drones searching for illicit substances. But the extent of the protection will likely hinge on the finer points of the law.

The Federal Aviation Administration is now producing new regulations for unmanned aircraft systems that will limit when and where commercial drones can fly; these may also help protect privacy in some cases. Many other countries, too, are debating how to balance privacy and freedom as drones proliferate.

Creepy as it is to be watched from aircraft controlled by others, drones are hardly privacy worry No. 1, says John Villasenor, a policy analyst at the Brookings Institution in Washington, D.C., because there are ways to collect far more information easily. "Drone privacy is a legitimate concern," Villasenor says. "But there are other technologies, such as mobile phones and the use of data gathered by mobile apps running on those phones, that, for me at least, raise far more pressing privacy issues." ■