# Spooked

*Researchers and lawmakers must work to rebuild trust in secure Internet standards.*

When John Hopkins University ordered cryptography researcher Matthew Green to take down a blog post last week, it found that its action only made the material more visible. The university quickly backed down, but the global media began to pay attention to the post, which discussed revelations that the US National Security Agency (NSA) has compromised or got around the encryption techniques on which the security of Internet communications, electronic health records, e-commerce and banking are based.

The allegations — the latest in a series of disclosures about NSA activities — and Green's analysis of them should make one sit up and listen. "Not only does the worst possible hypothetical I discussed appear to be true, but it's true on a scale I couldn't even imagine," he wrote.

NSA mathematicians have been among the leading contributors to encryption research and the development of standards meant to protect the security of the Internet, often working closely with academic researchers and key bodies such as the respected US National Institute of Standards and Technology (NIST). But according to allegations made by *The New York Times*, *The Guardian* and public-interest-journalism website *ProPublica* in early September, based on documents provided by NSA whistle-blower Edward Snowden, the agency has also worked to weaken or create vulnerabilities in encryption standards.

Other allegations include collaborating with technology companies to provide entry points into their products, as well as forcing Internet companies to hand over encryption keys or hacking these from servers to defeat security.

On 9 September, NIST took the unprecedented step of opening a review of two of the suspect standards, and went so far as to warn users not to apply one of the standards until vulnerabilities had been double-checked by cryptographers. The Internet Engineering Task Force (IETF), an open international body that develops the core standards of the Internet, is now looking at how it can harden Internet protocols to reinforce security and privacy against NSA-type attacks, and will take up the issue at its next meeting, in Vancouver, Canada, in November. This week, cryptographers at the University of Bristol, UK, published an open letter that called for a parliamentary enquiry into how security has been compromised.

Just as toxic subprime loans in the mid-2000s poisoned trust among financial institutions, leading to the financial crisis, the NSA's actions have poisoned people's trust in all the groups that make up the Internet ecosystem, from the giants of Google and Yahoo to telecoms companies, cloud-computing providers and the makers of chips and routers. US technology companies are likely to be the first to suffer, but the NSA's actions have corrupted the very fabric of the Internet.

***"Mathematicians in the NSA, and external academics working with the agency, should examine their consciences."***

Writing in *The Guardian*, cryptography researcher and security expert Bruce Schneier has called for scientists and engineers to take back the Internet, and for more whistle-blowers to come forward to detail how the NSA and authoritarian states are sabotaging electronic freedoms.

Certainly, mathematicians in the NSA, and external academics working with the agency, should examine their consciences. Mathematical associations and universities with links to the NSA should be more public and vocal about the revelations.

Like the IETF, Schneier wants scientists to re-engineer the Internet to make it more secure. Some technical improvements can be made — open-source code, which can be reviewed by anyone, is likely to be a major benefactor and facilitator — and the trust and security paradigms of developing Internet protocols have without doubt been irreversibly changed. But the Internet was not designed to be secure, and as the IETF points out on its blog, the scale of the NSA attacks was "not envisaged during the design of many Internet protocols".

As Schneier and the IETF acknowledge, technology is only part of the solution. Regulation of surveillance on the Internet and attacks on civil liberties are as much, or more, a question of policies. It has become abundantly clear over the past few months that there is but a fig leaf of oversight to protect against abuse of civil liberties by the NSA. The balance between security and civil liberties has gone off the charts in the wrong direction. ■

# Book smart

*Novelist Thomas Pynchon shows that science and art can combine, with mutual benefit.*

Some writers use metaphors in science. Some go further and make a metaphor of science itself — not the practical art of observation and empirical testing, but the often-tricky concepts at the heart of the pursuit. Such writing is difficult, and scientists and non-scientists alike can struggle with the result. But when done well, the language of research and the grammar of the natural world can sing a song as sweet as anything in literature. The supposed differences between the two cultures dissolve, leaving only those who get it and those who do not.

Many of those who do — both scientists and non-scientists — will be eagerly awaiting the latest book from Thomas Pynchon, *Bleeding Edge* (Penguin). It is reviewed on page 312 by Sean Carroll, a theoretical physicist at the California Institute of Technology in Pasadena who is himself a writer and a self-confessed Pynchon fan. Set against the terrorist attacks of 11 September 2001 in New York, *Bleeding Edge* is one of Pynchon's more straightforward books. As Carroll notes, it is "told linearly, from the point of view of an acknowledged main character, with something approximating an explicit goal".

That itself is a description of science, albeit a misleading one. Despite the appeal of a simple narrative, of cause and effect, and the dogged pursuit of truth by heroic individuals, most *Nature* readers will know — and no doubt lament — that science is not like that. Pynchon knows that too, and revels in our attempts to impose order on a chaotic, unruly reality.

Pynchon, Carroll notes, often uses imagery and symbolism from science and engineering. Stephen Hawking says that he was told that each equation printed in a popular-science book would halve its readership, so imagine the reaction of the editor on receiving the manuscript of Pynchon's 1973 classic novel *Gravity's Rainbow* (Viking), complete with a description of the first elements of the Poisson distribution. Organic chemistry, behaviour modification, double integrals and rocket dynamics all underpin both that story and the language that Pynchon chooses to tell it.

Some physicists consider Pynchon one of their own. The author studied for (but never finished) a degree in engineering physics at Cornell University in Ithaca, New York, and worked as a technical writer for the aerospace company Boeing. Biologists have credited his idea of a 'counterforce' — an organizing principle (also known as life) that counters the universal descent into entropy — as the spark that ignited their careers.

Those who get it see something special in Pynchon's work. There are few novelists who can claim to successfully unite the two cultures, but Pynchon does it by dispensing with metaphor and turning to science itself. ■

**➲ NATURE.COM**
To comment online, click on Editorials at:
go.nature.com/xhunqv