# NSA pursues quantum technology

January 31 2014

In this month's issue of *Physics World*, Jon Cartwright explains how the revelation that the US National Security Agency (NSA) is developing quantum computers has renewed interest and sparked debate on just how far ahead they are of the world's major labs looking to develop the same technology.

In 2006 the NSA openly announced a partnership with two US institutions to develop quantum computers. However, according to documents leaked by whistle-blower Edward Snowden, and published last month by the Washington Post, the NSA also wishes to develop the technology so that it is capable of breaking modern Internet security.

The $79.7m project, dubbed "Penetrating Hard Targets", could be made possible by the extraordinary potential of quantum computers to factorize large numbers in a short space of time, quickly deciphering encryption keys that are used to protect sensitive information.

For the NSA, this could mean deciphering banking transactions, private messages and government files; however, many physicists are not surprised and believe this is exactly the type of technology that the NSA is expected to develop.

Speaking to *Physics World*, Raymond Laflamme, a leading quantum information theorist at the University of Waterloo in Canada, said "If you put my level of surprise on a scale from zero to 10, where 10 is very, very surprised, my answer would be zero."

For many other physicists the news has confirmed the need to stay ahead of the game and develop more sophisticated encryption techniques, some of which also take advantage of quantum phenomena.

Quantum key distribution (QKD) is one such technique, which guarantees the security of an encryption key based on fundamental aspects of quantum mechanics, whereby the process of trying to measure or access an encryption key made from various quantum states will automatically destroy it.

The latest leaked documents, however, also reveal that the NSA is attempting to exploit practical loops in QKD under a programme known as "Owning the Net".

Cartwright concludes that quantum computers are still expected to be many years away, with the control of qubits – the packets of information that quantum computers would process – a major sticking point for physicists; however, the extent to which the NSA has developed the technology remains largely unknown.

Also in this issue of *Physics World*, and online today, 31 January, Matin Durrani, editor of the magazine, provides further details of the UK's £270m investment into quantum technology that was announced by the chancellor George Osborne in last year's Autumn Statement.

The initiative, which will begin in 2015, will focus on areas such as chip-scale atomic clocks for improved GPS communication, quantum-enabled sensors, quantum communication and quantum computing, while some £4m will go on equipment for the new Advanced Metrology Laboratory being built at the National Physical Laboratory.

The quantum-physics initiative, which has involved careful behind-the-scenes negotiations between the UK physics community, government

and industry, was formally put to Osborne last year by a group of physicists led by Professor Sir Peter Knight from Imperial College London.

Provided by Institute of Physics