US and UK ‘crack online encryption’

US and UK intelligence have reportedly cracked the encryption codes protecting the emails, banking and medical records of hundreds of millions of people.

Disclosures by leaker Edward Snowden allege the US National Security Agency (NSA) and the UK’s GCHQ successfully decoded key online security protocols.

They suggest some internet companies provided the agencies backdoor access to their security systems.

The NSA is said to spend $250m (£160m) a year on the top-secret operation.

It is codenamed Bullrun, an American civil-war battle, according to the documents published by the Guardian in conjunction with the New York Times and ProPublica.

The British counterpart scheme run by GCHQ is called Edgehill, after the first major engagement of the English civil war, say the documents.

‘Behind-the-scenes persuasion’

The reports say the UK and US intelligence agencies are focusing on the encryption used in 4G smartphones, email, online shopping and remote business communication networks.

The encryption techniques are used by internet services such as Google, Facebook and Yahoo.

Under Bullrun, it is said that the NSA has built powerful supercomputers to try to crack the technology that scrambles and encrypts personal information when internet users log on to access various services.

The NSA also collaborated with unnamed technology companies to build so-called back doors into their software – something that would give the government access to information before it is encrypted and sent over the internet, it is reported.

As well as supercomputers, methods used include "technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications", the New York Times reports.

The US reportedly began investing billions of dollars in the operation in 2000 after its initial efforts to install a "back door" in all encryption systems were thwarted.

'Gobsmacked'

During the next decade, it is said the NSA employed code-breaking computers and began collaborating with technology companies at home and abroad to build entry points into their products.

The documents provided to the Guardian by Mr Snowden do not specify which companies participated.

The NSA also hacked into computers to capture messages prior to encryption, and used broad influence to introduce weaknesses into encryption standards followed by software developers the world over, the New York Times reports.

When British analysts were first told of the extent of the scheme they were "gobsmacked", according to one memo among more than 50,000 documents shared by the Guardian.

NSA officials continue to defend the agency's actions, claiming it will put the US at considerable risk if messages from terrorists and spies cannot be deciphered.

But some experts argue that such efforts could actually undermine national security, noting that any back doors inserted into encryption programs can be exploited by those

outside the government.

It is the latest in a series of intelligence leaks by Mr Snowden, a former NSA contractor, who began providing caches of sensitive government documents to media outlets three months ago.

In June, the 30-year-old fled his home in Hawaii, where he worked at a small NSA installation, to Hong Kong, and subsequently to Russia after making revelations about a secret US data-gathering programme.

A US federal court has since filed espionage charges against Mr Snowden and is seeking his extradition.

Mr Snowden, however, remains in Russia where he has been granted temporary asylum.