

guardian.co.uk

US cyber security is back on the agenda

Barack Obama made an initial review of US cyber security, but pressure is growing for the president to take further action

Peter Warren

guardian.co.uk, Wednesday 9 December 2009 19.05 GMT

A [larger](#) | [smaller](#)



Whisper campaign ... security officials are urging the US president to appoint a 'cyber tsar'. Photograph: Rex Features

For the past month or so a curious game has been going on in the world of rumour and uncertainty that passes for the intelligence community. At the heart of it is an attempt to force the US president, Barack Obama, to put cyber security back to the top of his agenda and to usher in increased monitoring of the internet.

Despite an initial promise of action and a demand for a report on the risks to the US technology infrastructure to be on his desk in 60 days, little in policy terms has been heard since.

Even more frustratingly for the computer-security community, Obama has also not filled the much-trumpeted post of cyber czar. Melissa Hathaway, the White House's senior acting director for cyberspace and the author of Obama's 60-day review of cyber policy, had been widely tipped for the position – but four months ago she resigned, citing personal reasons for her decision.

Damage limitation

This appears to have resulted in a turf war between the US department of homeland security, the military and the intelligence community as each compete for responsibility for the issue.

Now, in what is being seen as an attempt to jog Obama's memory, stories about the US's vulnerability to cyber attack, the threat it poses to its economy and the potential rise of cyber-terrorism have begun to appear on an almost daily basis.

exploited there would be enormous economic damage to the US.

"There has been a heightened awareness of our vulnerability to cyber attacks in the US and that has been building for over a year. People are saying, 'Look at Lehman Brothers' – if someone had taken out another banking website on the same day it would have been the straw that broke the camel's back," says Tom Reilly, a US director of ArcSight, a company set up by the investment arm of the CIA. It draws 30% of its revenue from monitoring critical infrastructure for dangerous activity for US federal government agencies and Nato.

On the subject of the cyber czar, Reilly says: "There is now a lot of impatience ... People are looking for an individual to be appointed to set policy direction, and without that framework in place there is the possibility of duplication by agencies."

The potential for exploiting the fragile confidence in financial institutions has not been lost on businesses. "The recession has been a driver in awareness," says William Beer, director of information security practice for PricewaterhouseCoopers. "For the first time, critical infrastructure vulnerability has made it onto the risk register. With Northern Rock we saw a cascade effect occurring as its systems went down ... and the fragility of systems is now seen as important to confidence."

A particularly audible warning of cyber-terrorism has come from Steven Chabinsky, the deputy assistant director of the FBI's cyber division. On 17 November, he told the Senate judiciary committee that the FBI is now investigating suspected al-Qaida sympathisers who appear to be interested in launching attacks on critical communications infrastructure.

At the same hearing, the US associate deputy attorney general, James Baker, confirmed the Obama administration had been examining the need to possibly change the laws dealing with both technology and surveillance, in order "to better protect the nation from cyber attacks". According to Stewart Baker (no relation), a former assistant secretary of policy for the department of homeland security, the concerns are legitimate.

"We have not seen a particular event that has justified this, but the fact is that our exposure to cyber attacks is growing and our exposure is growing particularly in power systems because of our move to internet-based control systems," says Stewart Baker, who admits the sudden rise in media reports is almost certainly an expression of those concerns.

"News doesn't happen without someone wanting it to happen. There is a sense in cyberspace circles that despite the talk that has occurred, and the concerns now being expressed, we are still not addressing the problems."

Any answer to these problems will come with a hefty political and financial price tag and has no guarantee of eventual success. "Some of the price will have to be paid in terms of privacy on the internet, because we are not going to be able to find those wishing to attack us without increased monitoring. That can only be achieved by giving up some of the anonymity that we see on the present internet," says Stewart Baker.

Attack by accident

Internet monitoring will be difficult to justify politically, because there is little evidence

of attacks by terrorists on communications infrastructure – the main use of the web by terrorist groups to date has been for fundraising, communication and propaganda.

"To attack critical infrastructure, terrorist groups have to have a cyber capability and the terrorists we know don't," says Dr Peter Tippet, a noted security threat expert and vice-president of intelligence and research for the computer giant Verizon. "Terrorism of cyber quality requires serious skills and another level of sophistication – it's not just the use of hacking techniques. Our recent data breach survey and all of the information we have shows that in the vast majority of hacking attacks the bad guys get there by accident.

"I am confident that most terrorist organisations have a geek somewhere but the organisations that have the sort of capability necessary to attack infrastructure are the usual suspects – Russia, China and Israel – and they are not the sort of organisations we think of as terrorists."

This isn't a position wholly shared by Prof Rohan Gunaratna, head of the Singapore-based International Centre for Political Violence and Terrorism.

"Terrorist groups at the moment prefer to harness the infrastructure, and the capability to mount successful attacks is still within the domain of government, but it is only a question of time before that capability starts to percolate to them.

"There have been power disruption events in Northern Australia and Canada, where responsibility was claimed by the Abu Hafs [al-Masri] Brigade [though they were not responsible]. The awareness of the vulnerability is being raised because groups are becoming more IT-aware," says Gunaratna, a former White House adviser.

Stewart Baker agrees with this possibility, though he also says that IT is treated with suspicion by terrorist groups.

"If a government wanted to experiment with its capability, it might want to use a proxy, but with cyberwarfare you want to have control and turning over capability to another group is always difficult. This is not like a Stinger missile, you need specialised training – almost a whole career goes into building a cyber warrior.

"So far, al-Qaida has been penetrated every time it has used electronic techniques – it knows the network is not your friend."

Peter Warren is the editor of Future Intelligence