# If Obama is talking about securing the net, it should be on everyone else's lips too

January 22 2015, by Bill Buchanan



The US National Cybersecurity and Communications Integration Center, putting money where Obama's mouth is. Credit: Kristoffer Tripplaar

We have spent years promoting the need for change in our approach to internet infrastructure, forcing politicians to recognise it as a serious issue. So it's great to see Barack Obama tackling the issue in his State of the Union address.

You may agree or disagree with some of things he says, but he avoids the naïve thinking that suggests "banning encryption" or bulk surveillance of everyone's communications are quick fixes for society's ills.

The internet we have created is only just past its infancy and yet it already plays an integral role in our lives. Now is the time to put it to use for the betterment of the whole of society. Putting the brakes on now could derail many of the advances we have made. It could unpick economic gains and squander its potential to reform public services. Few technologies have ever provided such benefits so widely.

## Cybersecurity at the top table

Some nations now see their internet infrastructure as a key element of a form of warfare not possible in the past. Obama said:

*No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids… We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism.*

Defending cyberspace is as important as defending traditional infrastructure assets. Virtualised ammunition delivered via the internet can be as potent as explosives – the Sony hack highlights how any organisation could be vulnerable. Given physical access to network infrastructure, there is even greater threat of large-scale data loss.

In days of pen and paper, secrets could be locked behind solid walls, but these days organisations are scarcely aware of what constitutes valuable data worth keeping secret – never mind where and how to keep them.

Obama talked about the need to update laws to be relevant, as the legal

system lags behind fast-moving technology. He said he would pass legislation that would protect the nation's infrastructure against cyber attacks and identity theft, legislation that he has attempted to push through Congress several times without success.

But, often, the perceived failure to keep step with the times leads to rushed, knee-jerk and poorly thought-out legislation. A particular problem faced by those drawing up legislation is that the same elements of IT systems can be used for good and for ill. For example, the network utility ping can be used by attackers to map out a network and identify potential targets. So some organisations bar its use, yet it's also continually used by admin staff to debug network problems. You can't tackle one without crippling the other. Also the skills gap between attackers and defenders is widening – so there is a need to ensure a workforce that is up-to-date with the range of threats it faces.

Obama also highlights the tension in the debate between privacy and the rights of society. If surveillance programs are more transparent, then at least the debate over how they fit around other rights and how acceptable it is to society can be held:

*So while some have moved on from the debates over our surveillance programs, I haven't. As promised, our intelligence agencies have worked hard, with the recommendations of privacy advocates, to increase transparency and build more safeguards against potential abuse.*

## Individual privacy vs security for all

The bottom line is the move towards encryption by default and the worry that defence agencies will not be able to intercept communications.

In USA Today, John Shinal writes that "banning encryption is the digital equivalent of banning books". Rather than David Cameron's claim that

the most important thing for a government to do is to keep its people safe, Shinal says that "the most important thing a democracy can do for its people is to keep them free."

References from Ray Bradbury's Fahrenheit 451 to George Orwell's 1984 abound, but there is yet no water-tight solution to this. Lacking the ability to read everyone's communications will not stop investigators from investigating, just as it didn't in the days before it was possible. We leave traces of our activity all over the internet, traces that investigations will pick up and use. Before the internet, people used phones – and tapping phones was the way to investigate suspects. The idea of tapping everyone's telephone conversation, guilty or not, should revolt us; the same applies when the medium changes from phone cables to internet fibre optics.

## Looking to the future

Obama's address doesn't touch on how – or whether – surveillance will continue, or how this will be balanced against privacy. But hopefully governments will put it higher up their agenda, just as many businesses have realised they must. As we become more and more dependent on the internet, it's a debate for us all to get involved in.

We have seen the internet transform our lives and for the first time it seems politicians recognise that protecting it is essential. The worry is that [politicians](link) will care more about soundbites than policies. No country can fully control the operation of the internet, but each country can do its best to bring its opportunities to their citizens.

*This story is published courtesy of* [The Conversation](link) *(under Creative Commons-Attribution/No derivatives).*