http://www.opendemocracy.net/ben-schiller/cybersecurity-politics-interests-choices

Cybersecurity: politics, interests, choices

Ben Schiller, 13 July 2011

- **Subjects:**International politics Democracy and government
  Internet democracy & power governing the net globalisation

The threat of cyber-attack is driving states and corporations to devote ever-greater resources to meet the challenge. The accompanying debate about the scale of the risk has profound implications for the future of the internet, says Ben Schiller.

Ben Schiller is a freelance journalist based in New York, specialising in United States politics, corporate malfeasance, and the future of the internet. His website is here

When cybersecurity experts are asked why their issue is receiving so much attention these days, the reply tends to be a single word: Stuxnet. The computer worm, said to have been developed by the Israelis to sabotage Iran's nuclear programme, changed everything, they say: because it showed how large-scale facilities (and not just online targets) could be vulnerable, and how nations can fight a "cyber-war" with a high degree of deniability.

"It was a seminal moment", says Chris Demchak, an assistant professor in cybersecurity at the US Naval War College. "Before Stuxnet there were so many cyber-sceptics who would say, 'oh, it's

really just cyber-crime'."

And then there is China. Some analysts argue that Beijing is mounting a sustained online effort to steal the west's economic secrets as part of an "unrestricted warfare" strategy (a term coined by two People's Liberation Army colonels in 1999 to refer to an undeclared, asymmetric war). GhostNet - a online spying conspiracy reaching into more than 100 states, uncovered in 2009 - showed how far it was prepared to go.

A series of intrusions at corporate and state agencies identified in mid-2011 - at (among others) Citibank, Sony, the CIA, Google, Lockheed Martin, and Northrop Grumman - has provoked officials in the United States and elsewhere into increasingly dark warnings. "The next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems", the new CIA director Leon Panetta told the US Senate's armed-services committee in June 2011.

The Pentagon's "Defense Strategy for Operating in Cyberspace" (May 2011) says the US now regards online espionage as "acts of war" that necessitate conventional as well as cyber-reponses. An official told the *Wall Street Journal*: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks." There is now routine talk among analysts of the internet as a fourth theatre - after land, sea, and air.

The risk-cost dynamic

But not everyone is convinced: either that the threat is as serious as advertised, or that the response - both very costly, and increasingly

militarised - is warranted. Jerry Brito, co-author of a report for the Mercatus Center at George Mason University, which compares cyber-fear rhetoric to that leading up to the Iraq war, is one. “We’re not doing a proper risk analysis based on what is likely to happen. What we’re doing is saying ‘what is the worst possible thing that could happen, and then saying we’ve got to prepare for it’,” he says.

Moreover, critics of the militarisation of cyberspace argue that it conflates different threats (crime, military, intelligence) while distorting and exaggerating the overall danger. Brito and his colleague Tate Watkins concede that cyberspace holds some dangers, particularly for the safety of corporate assets; but they point to the risks of over-reaction, including the potential to waste taxpayers’ money, sacrifice online liberties, and impair the freedoms the internet affords.

The authors argue that a lot of the so-called attacks amount to little more than “probing” by relatively unsophisticated hackers: the equivalent of a would-be burglar turning a doorknob to see if a building is vulnerable to intrusion. Moreover, the threat to power-grids is overplayed: two oft-cited blackouts (in the northeast United States in 2003, and in Brazil in 2007) have since been debunked as cyber-sabotage incidents. The source of the Brazilian incident was deposits of soot and dust on transmission lines.

Jerry Brito warns that the tendency to “threat inflation” around cyber-security risks creating its own momentum. The outcome will be a “cyber-industrial complex” constantly alert to dangers that are conjured by its own discourse and serve its institutional interests. “We’re seeing a lot of what we saw in the cold war”, he says, “where we built this massive industrial base that created its own demand.

When you look at the alarmist rhetoric, a lot of it comes from people who either work in the industry, or who receive campaign contributions."

The targets for such criticism include Booz Allen Hamilton (BAH), a consultancy with extensive ties to the US government which in 2010 won at least $400 million in cyber-security contracts. BAH's executive vice-president is Mike McConnell, former director of national intelligence (2007-09) and a leading cyber-hawk ("the United States is fighting a cyber-war today, and we are losing", he has written in the *Washington Post*).

The growth in such warnings about the nation's vulnerability in cyberspace is echoed in increased government spending. The US plans to spend $10.5 billion a year on information security by 2015. Across the world, as much as $140 billion each year may soon be dedicated by states to cybersecurity. Many defence companies have been building up their capabilities to take advantage; BAE Systems, for example, is investing heavily in its operations, as well as buying start-ups like Detica and Norkom.

A choice of futures

Peter Sommer, an LSE professor and co-author of an Organisation for Economic Cooperation and Development report on cybersecurity - *Reducing Systemic Cybersecurity Risk* (OECD, working paper, January 2011) - says that various groups - journalists, analysts, intelligence agencies, the military, and the defence and IT industries - want to define the cyberspace "problem" in their own terms, and might have different reasons to inflate the cyberspace "danger". "The military will say it's a military problem. The spooks will say it's an intelligence problem. The security agencies will want to make a

contribution. And the police will say it's a cybercrime problem, and ask for more resources", he says.

Sommer's report outlines what it sees as real risks, while dismissing some "exaggerated scenarios". For example, the study says that a cyber-attack is unlikely to cause great loss of life, or disable the banking system. "One hypothesis is that banks might get wiped out. That really is a bit of nonsense, because it's trivially easy to back up computers", Sommer says.

Sommer should know what he is talking about, for in the 1980s he wrote a genre-creating book (*The Hacker's Handbook*, under the pseudonym Hugo Cornwall) and has seen many alarms about cyber-malfeasance come and go. He says the current spasm risks wasting precious national resources, misunderstanding the real threat, and introducing a dangerous accountability gap. "You end up giving power to agencies on the agenda that they are going to protect us. While that may start out as their aim, they may look around later and say, 'we've got all this monitoring capability, we think the state is under threat and we're going to use the resources we have'."

Chris Demchak says it is impossible to make a distinction between cyber-threats to companies and those from one state to another. In practice they overlap: for example, attacks by non-state actors can harm state interests, and states can exploit methods developed by hackers. In this situation, the traditional separation between crime and national security disintegrates.

Faced with a new range of threats, Demchak says that the only option is to renationalise the internet: that is, reassert national control over regulation and tighten monitoring of the national-

internet's borders. She foresees (and she is not alone here) a global system of individual authentication, where the identity of every person online is established. She also foresees greater scrutiny of online "packets", enabling governments to inspect traffic as it comes in and out.

"The way it will work is that to go in and out of a country, you will need to have a passport. And if you want to ship something in or out, you will need to say what's in the package and have some kind of inspection", she says.

Such a prospect worries activists like Chris Palmer, technology director at the San Francisco-based Electronic Frontier Foundation. "We're going to start behaving like China and putting up walls. It's the opposite of what we want for the internet. We keep hearing all these drumbeats of 'defend against hacking', 'defend against cyberwar', 'protect our infrastructure'. They sound to me like excuses for cracking down on free expression." He says authentication would in any case be impractical on a worldwide scale.

The debate on cybersecurity is moving as states get more involved, governments more fearful, corporations more interested, and citizens - named and anonymous alike - more active. As a result, the contest over the future of the internet has only just begun.