

9

NETWORKS AND COMPUTER SECURITY

Additional Resources

Additional references, news snippets and mini articles to add to and update the material in chapter 9: Networks and Computer Security.

Edward Snowden: Leaked National Security Agency (NSA) Documents

In Chapter 9, I briefly discuss allegations that were current in 2012 about Chinese espionage (and cyber warfare preparations) against US and Western military and commercial systems, see for example Hopkins (2012) – there was of course the suspicion that the US, the West and other countries had similar programmes. See:

<http://www.theguardian.com/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle>

In 2013 there emerged a whistleblower, Edward Snowden who worked, as a contractor, for one of the US intelligence agencies, the National Security Agency (NSA). His revelations, that don't seem to have been contested, revealed massive surveillance operations on all kinds of electronic communications (telephone, e-Mail, web-access, etc). The aim (or stated aim) is to detect and foil terrorist activity but the data capture of the NSA systems is essentially non-selective (and then sophisticated search software is used to identify communications that could be relevant). The revelations also reveal that Britain's GCHQ is working in close cooperation with the US's NSA on these programmes. The Guardian has taken the lead in exposing these surveillance activities; here is a link to one of the many articles published in the Guardian:

<http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations>

The revelations have left the US and UK governments scrabbling to justify their surveillance activity. The justifications offered by the UK government can be summarised as:

- ◆ This surveillance is an essential, anti-terrorist tool and it saves lives.
- ◆ Citizens (data subjects) who have nothing to hide have nothing to fear

Possibly so, but governments the world over have agendas that do not necessarily fit in with the (legitimate) aspirations of all their citizens. At the same time as the Snowden revelations, there are also revelations about police infiltration and agent provocateur activities in various pressure groups.

In addition to concerns about the use of this surveillance material by governments and their agencies there is also the basic principle of privacy – should governments be snooping on and tracking everything we say and do? Coupled with this, whatever the intention, one thing we can be sure of is that all of this information will not be secure all of the time. Personal data held on by citizen is subject to unauthorised access and abuse all of the time – there is no reason to believe this data will be different.



Learning resources – *An Introduction to Information Systems* by David Whiteley