DIRTY DEALING

Security: Indecent exposure

Thursday 21 November 2002

The IT-dependent structures of the developed world are extremely vulnerable to cyber-terrorism, says Peter Lilley.

The aftermath of the terrorist attacks in the US in 2001 have focused the world's attention on terrorism and weapons of mass destruction. However, I have more sleepless nights worrying about the misuse of the digital world than aluminium pipes being exported to Iraq.

In simple terms the digital threat posed by terrorists and rogue nations is a very real one - because every attack they might consider has already been successfully mounted. The only saving grace is that the people who have mounted such attacks before are a mix of crackpots, eccentrics and petty criminals.

While certainly not wishing to make light of such a serious subject, some of the previous offenders (and their motives) beggar belief. Take, for example, the resident of Brisbane, Australia, who was jailed in October 2001 for the seemingly obscure crime of hacking into council computers that control sewage. He succeeded, among other things, in getting a sewage pumping station to overflow thousands of litres of "material" and pump raw sewage into public waterways. In all he was found guilty of 30 charges, including computer hacking, theft and environmental vandalism. His motive was revenge against his former employer (the installer of the sewage system) and the council which had turned down his job application.

Why are we still debating whether it is possible to hack into critical infrastructures when the first jail sentences for such offences were handed down in 1990? Four members of the Legion of Doom (a US hacking group) were arrested for stealing the technical specifications of the 911 emergency telephone network of the telecoms company BellSouth. The company spent $3m (£1.9m) on improved security as it was found that the hackers had also stolen passwords, logins and connection addresses.

The simple undeniable truth of the matter is that digital attackers can paralyse each and every key element of national and international critical infrastructures. For instance:

- **electricity supplies** - power grids and associated facilities could be brought down by logic bombs or worms. This would cause local, regional or even national power black-outs and voltage oscillations.
- **Water supplies** - in most western countries the process of collecting and distributing water is highly technology-reliant. Attacks could disrupt or cut off water supplies. At the other end of the cycle, cyber-attacks could disturb, divert or destroy sewage systems, facilitating the spread of disease.

- **train** - logic bombs or hacking of traffic control systems could cause crashes or paralyse logistics and transport networks.
- **air traffic** - both planes and air traffic control systems can be attacked. On-board systems could be made to malfunction; air traffic control systems could be brought down or made to give false information.
- **telecommunications** - both civil and military - can be easily attacked causing malfunctions or shutdowns.
- **civil administration** - civil records and law enforcement systems are prime targets for attack which could result in chaos and disruption.
- **Hospitals and associated emergency services** - many medical and administrative support functions are heavily IT-dependent.
- **Financial Institutions** - sniffer programs can monitor and track the transfer of funds together with other confidential information; hackers can crack systems to steal money or cause chaos by transferring funds and assets to incorrect locations; logic bombs and denial of service attacks can cause difficulties within institutions or the market as a whole.
- **Weapons** - ironically one of the most potent effects of a digital attack would be to hack into the sophisticated control systems of high tech weaponry such as missiles, surveillance aircraft and satellites - or any piece of hardware that could be used for offensive purposes.

Potential digital terrorists could do worse than take a leaf out of organised crime's books. Colombian drug cartels are believed to have hired IT "experts" to install and run a secure communications system; the US government believes that the IRA and the Basque terrorist group ETA use technology extensively to implement their objectives; Amsterdam-based criminal gangs employ crackers to monitor and disrupt the systems of police surveillance teams. To add to this the Italian Mafia, Mexican drug cartels, the Japanese Yakuza, Chinese triads, Turkish gangs, Russian Mafia and criminals operating from West Africa are all active in cyber-space.

This is not the place to suggest the steps each organisation should take to secure its systems to ensure that they are not used as an offensive weapon. However I wonder whether both national and corporate attempts at digital security are akin to one security product available in the US - a gargoyle which, placed next to your computer, is supposed to ward off modern day evils such as viruses, hackers and system errors. Just one version has sold more than 100,000 units, which either means that this number of people have computers wide open to attack, or the rest of us need a gargoyle immediately to protect us like these 100,000 wise users.

Peter Lilley is the head of Proximal Consulting and the author of Hacked, Attacked & Abused; Digital Crime Exposed, (Kogan Page). Contact pl@proximalconsulting.com