Skip to main content

Guardian Unlimited

Read today's paper
Sign in | Register

Go to:

technology

Home | Technology blog | Ask Jack blog | Gamesblog | Games | Opinion | Innovations | Inside IT

Online

Search this site

Iraq conflict special

# Electronic Pearl Harbor

Should we be more worried about terrorists using digital weapons rather than chemical and biological attacks? Dickon Ross investigates

**Thursday February 20, 2003**
**The Guardian**

That's been two hours you've been unable to get on-line now. So much for always-on, you think, as you go to fill the kettle. You turn the tap and - nothing, there's no water. And that's when the lights go out. Now the phone line is down, too. There's always the mobile - but why is it dialling 999 all by itself?

This is the kind of scenario that government and private computer experts will be studying as they look into the growing possibility of a "cyber-terrorist" attack on what is known as our "critical information infrastructure" - the electronic systems vital for government, armed forces, business, finance, telecommunications, utilities, or emergency services.

There have been warnings from parts of the IT community that terrorists could attempt something like this for at least 10 years, but now governments are taking it much more seriously. Last week the FBI issued an alert warning that the threat of war with Iraq, and increased tension with North Korea, could lead to increased numbers of attacks on US infrastructure. Meanwhile Erkki Liikanen, European Commissioner for the Information Society, announced the formation of the European Network and Information Security Agency, a new body to improve cross-border cooperation and offer advice on computer security.

"Network security has become a key concern, especially in the aftermath of the September 11 events," he says. "The malfunctioning of networks and information systems concerns everybody: citizens, businesses and public administrations."

The Cabinet Office, too, has announced a new unit, the Central Sponsor for Information Assurance, to be headed by its e-envoy, Andrew Pinder. This unit "brings together IT security expertise from across government," says the department, and "it will be working with the public and private sectors to ensure that risks to the national information infrastructure are appropriately managed."

The language is reserved, the discussions kept within a close circle of specialists, but security experts say the government is taking the threat seriously. In the United States, repeated warnings of an "electronic Pearl Harbor" from terrorism and technology experts have given the subject more public prominence. The White House is due to release a national strategy to secure cyberspace within the next few weeks. The UK's parallel effort, the "national information assurance plan", was revealed last May but is "still in its early stages", a spokesman for the e-envoy's office admitted.

This scenario is not just a dim vision of the future. The National Security Agency simulated a cyber-terrorist attack with 35 hackers in 1997. They managed to hack into department of defense networks, "turn-off" sections of the power grid, "shut down" parts of the 911 emergency service and even managed to "hack" into a Navy cruiser's systems.

But it's the events of September 11 2001 that have turned cyber-terrorism from a theoretical threat into a very real one. The warning signs are there for all of us to see in al-Qaida's public statements, says Richard Clarke, chairman of the president's critical infrastructure board. He was America's first counter-terrorism coordinator and has now advised three presidents on cyber-security. His argument is quite simple: before September 11, al-Qaida tended to talk about taking human lives - killing as many people as possible. But afterwards its rhetoric shifted towards threats against the economic infrastructure of the west. This is too dispersed and diverse to bring down with bombs, he argues, but it could do a lot of damage in cyberspace.

Clarke is not alone. There will be a major attack this year, says research firm IDC after polling its 700 analysts to make predictions for 2003. Network Associates vice president Terry Benzel told the House of Representatives science committee: "People will die, the nation's economy will be crippled and protec tive services systems will be weakened."

Al-Qaida is just one group interested in waging cyber-terrorism. A CIA report for the Senate Intelligence Committee adds Sunni extremists, Hezbollah and Aleph (formerly Aum Shinrikyo, responsible for the Tokyo underground poison gas attack) to the list. Clarke says Iraq, Iran, North Korea, China and Russia are already training people in cyber-warfare. "There are a lot of different people who can conduct cyber-warfare," says Clarke. "There are countries that are creating cyber-warfare units. There are criminal groups engaging in cyber-crime. There are also some terrorist groups we know are looking at using cyber-attack tools."

A Home Office spokesman said assessments by its national infrastructure security coordination centre, which works with intelligence services such as GCHQ to gather information, conclude there is "no imminent threat" of a cyber-terrorist attack, "but that issue is kept under onstant review."

The motive for most hackers and virus writers has always been one of ego or intellectual challenge rather than financial gain or political belief. But now ideologically motivated hacking is rising fast, says UK computer security consultancy Mi2g. Its study of major hacker groups active in 2002 notes: "Attacks on the west show a spurt of growth mainly coming from radical groups and individuals based in predominantly Islamic countries." It reports that there were 5,589 attacks on the UK last year, with ideologically motivated attacks coming from Egypt, Pakistan, Morocco and Turkey. Mi2g says there were surges of attacks before both the Bali bomb in October and the arrests of suspected terrorists in Italy last month. "The true extent of the shared agenda between hacktivisim and terrorism is only now becoming visible," says the report. "There is a requirement for government-funded network monitoring to go deeper into ideological hacking and to establish the common connections between digital attacks and physical terrorism."

But Clarke argues that we should be worrying about how to protect our critical systems, rather than where the next attack will come from. Every new technology is a potential target for cyber-terrorists. Viruses in Spain and Japan have tricked mobile phones into dialling the local emergency numbers. "Now, if you're a terrorist, the first thing you might want to do before an attack is take down the 911 system," says Clarke.

There are also concerns over the latest hot technology known as wireless local area networking (WLAN, or Wi-Fi in the US). This is now appearing in notebooks, laptops and PDAs for business people to get online access in "hot spots" such as cafes, airports or even on the street outside companies that have it installed. The Worldwide Wireless Wardrive, whose members drive around to find these "hot spots", found that most access

points don't even have the most basic wireless security software turned on.

More households are signing up for broadband internet services because they offer faster access and an "always on" connection. "This, of course, increases the vulnerability of systems and multiplies the probability of some sort of cyber-attack," says Erkki Liikanen.

The legend of the internet is that it was designed to survive a nuclear blast - it will always survive one part going down because it will just find another path through other servers. Yet research at Arizona State University published last week found that it is not as bomb-proof as we assume. Only a few thousand computers transmit most of the data over the internet, they found, and it is in fact vulnerable to a "virtual cascade" of overload failures that could make the whole system crash. "Our work suggests that attack on this small fraction of highly loaded computers may make the entire network collapse," says mathematics researcher Adilson Motter.

"Policies not designed for the 21st century are failing," says Mi2g chairman DK Matai. "Wireless networks, private mobile phones, instant messaging and remote access email accounts are helping to bypass elaborate security procedures every day. Executives need to rethink their strategy."

Mike Barwise, consultant at Computer Security Awareness, says hackers are persistent, pay attention to detail and share information. "If the defence had those attributes then it would be a level playing field," he says.

But he adds: "There's a risk of fulfilling the terrorist purpose ourselves. If we spread the terror ourselves they can sit back and relax."

Indeed, the computer security industry is sharply divided over the seriousness of the cyber-terrorism threat, and there are dissenting voices. Just as with nuclear, biological or chemical weapons, critics ask for the evidence that terrorists have the digital weapons to launch a cyber-attack.

"Before we make assertions we must justify them with evidence," says Barwise, and he reckons we don't yet have a lot of evidence that terrorists either do or don't have the skills. Most attacks are by "grafitti writers" on websites, he says, and then come the less common hacks into systems for financial fraud or other personal gain. Rarest of all are what he calls the "uber-hackers": the one or two per hundreds of thousands of hackers who are good enough to hack into government sys tems and yet cover their tracks. "That isn't prevalent," he says, "and

it's difficult to see how serious damage could be caused by someone not equipped with insider knowledge - they've got to now about the technical aspects of the system they're trying to damage."

This is why Peter Sommer, of the London School of Economics Computer Security Research Centre, dismisses the idea of an impending "electronic Pearl Harbor". The number of people in government who know the sort of sensitive security information that terrorists would need is very few, he says.

Matai says data attacks are more of a nuisance than a terror but "command and control" attacks on water, power, transport, telecommunications or aviation hubs could be fatal. Once inside the control systems, hackers may choose to turn off power or water supplies, open dams or empty sewage into rivers. And that's just the possibilities that counter-terrorism officials have been able to imagine.

These kind of attacks require much more sophistication but hackers are growing in numbers and capabilities, says Matai, and "will be there over the coming two to three years." Command and control hacks require insider knowledge, he adds. "Hacking is a remote crime but it does require local presence for serious damage to be caused."

Al-Qaida's style is to patiently plan coordinated attacks and it's not too hard to imagine that it is at least training or preparing hackers and virus writers around the world for a large scale, coordinated assault that piles attack upon attack until systems fall over. It would be cheap and involve little risk of those involved ever being caught.

The US may retaliate with a counter cyber-attack. The rules of cyber-warfare are in a legal black hole because the Geneva convention forbids attacks on non-combatants.

Last week the Washington Post reported that President Bush had signed a secret directive for government to develop guidance on when, and how, the US would launch cyber-attacks against enemy networks. Mi2g says it is inevitable that governments develop cyber-warfare weapons because in cyberspace as in the real world, attack is a strong form of defence. And there are always counter attacks in response to cyber-attacks, says Matai: "During the Nato-Serbia war in 1999, the blended [virtual and physical] attacks on Serbia's telephone and power utilities were followed by counter-attacks on Nato Command and the US DoD's email and internet servers.

"In the case of the looming attack on Iraq," says Matai, "the concern in blending cyber warfare techniques would be the

likely impact felt by the US, UK, Canada and Australia in particular from counter-cyber-attack."

The trigger for the world's first cyber-war could be a real war in Iraq. One prolific virus writer in Malaysia, with links to al-Qaida, says he has prepared a "megavirus" that he will release if and when Iraq is attacked. His portfolio of work includes a virus called Nedal - "Laden" spelt backwards.

· Comments to **online.feedback@guardian.co.uk**

Special report: computer security

**The issue explained**
04.05.2004: Viruses and worms

**Useful links**
Cert Coordination Centre
Computer Security Resource Centre
Encyclopaedia of Internet Security
McAfee Security
MessageLabs
Sophos
Vmyths

---

Printable version | Send it to a friend | Save story