

# Cyber terrorism and the threat to democracy

**Prof. Simon Rogerson**

**Originally published as ETHcol in the IMIS Journal Volume 13  
No 4 (August 2003)**

At a recent Parliamentary Information Technology Committee (PITCOM) meeting the threat from cyber terrorism was discussed. Concerning our vulnerability, one speaker, Paul King from Cisco Systems explained that, I would estimate conservatively that if you are on the internet you are scanned every 20 seconds. The question is whether you notice. If they are scanning you, what is it for? The record I have for being scanned is an unclassified UK defence network which within four seconds of going live on the internet it was being scanned.

The second speaker, Dame Pauline Neville-Jones, Chairman of Qinetiq said, As we place more reliance on mobile computing, on electronic service delivery, as we move towards the so called pervasive computing paradigm, and as the availability of these technologies increases to a still wider proportion of the population, we shall find it considerably harder to protect against their misuse. All freedom in society is ultimately founded on trust - trust that in allowing you freedom to act, you will not harm my interests or curtail my freedom. Trust in the computing world is no different - indeed it is vital: the user must trust the system to be willing to use it on a repeated basis. New technologies may well increase the opportunities for the destruction of that trust.

Dame Pauline continued, the complexity involved in providing adequate security in the sort of computing environment I have described is of a different order from that faced today. Hence my caution in stating that while the threat from cyber terrorism is comparatively low today, the situation is not stable and is likely to be moving adversely "The crimes will not have changed much in nature but the range of possibilities for committing them and the difficulty of protecting against them and tracking down the felons will increase manifold."

It seems we must all be vigilant against such threats particularly when they are against the very foundations of society. When asked about the potential risks from cyber terrorism to the electronic voting for the May local government elections and whether they should take place, the two speakers had different perspectives.

King replied, "We should definitely carry on. These are pilots and will be watched very closely, and it's only from projects like this that we will learn. I think they are safe because they are well resourced." Whilst Neville-Jones responded, "Some basic things

need dealing with and I don't know if that has been done. Apart from that I think the issue will surround how far and how fast you can go down this road. I would want to be more confident than I am now that the systems are not open to misuse before using them for a large scale election."

There is a groundswell of expert opinion that electronic voting using the Internet is dangerous. Lee Dembart in the International Herald Tribune reported on 28 April 2003 that, In all electronic elections in Europe and most of the United States so far, security experts say, the systems used were vulnerable to attack and could have been manipulated in undetectable ways that would have made it impossible to determine that the results of an election had been changed, either by accident or design.

Specifically, the experts say, Internet voting could be crippled by a "denial of service" attack against the computer servers recording the vote, for which there is no known defense, and could disenfranchise large numbers of voters. In addition, they say, since voters use their own computers, election officials have no control over what software is installed on those machines or what viruses might be lurking in it that are activated only during an election to change votes.

Whilst Simon Parker writing in the Guardian on 30 April 2003 pointed out that, A security assessment carried out for the government suggests that, by making the voting system accessible across the globe, e-voting will "dramatically" increase the potential for trouble. Individual hackers, criminals, political activists and foreign intelligence services are among those who might try to rig the vote or destroy the technology used to run the election."

Finally, in their press release of 1 May 2003 the Foundation for Information Policy Research (FIPR) warned that electronic voting systems such as those being trialled in local government elections may lead to major problems, and could severely damage the public's confidence in the electoral process.

FIPR warned that election integrity can be assured only if e-voting machines produce a paper audit trail that can be verified by voters and later by election scrutineers. This is not the case when votes are cast from telephones or insecure home PCs, as in the trials taking place in 18 local authorities during today's local elections. Voting machines must be squarely under the control of local election officials, who have a better chance of ensuring they are free from viruses or other malicious software that might monitor and corrupt a user's vote.

Without such precautions, FIPR claimed it will be impossible to prove afterwards that an election was carried out correctly. If problems occur, levels of public mistrust could make Florida voters' worries about "hanging chad" look trivial.

There is second important issue that of scaling related to the cyber terrorist and electronic voting. Lee Dembart explained that, Several experts noted that if people intended to rig

an electronic election, they would not waste their time and effort on a minor local election with little consequence, thereby tipping off the authorities to the vulnerability of their election system. Such people would ignore small, pilot project elections, such as those currently under way, in order to increase the authorities' confidence in the system. They would wait until a big election, such as a national one, before attacking.

Simon Parker concurred with this view writing that, At De Montfort University's centre for computing and social responsibility, Leicester, researcher Ben Fairweather says: "I don't think we know for certain that an electronic general election is possible at the moment. It might be possible, but one of the big problems is that piloting it at the local level you're not facing the challenges you'll face in the real thing." Few people, he suggests, would bother trying to rig or hack a local e-voting pilot, but a general election would be a far more tempting target."

Are these concerns well grounded? In July 2003, the Electoral Commission will be publishing a review of all the pilots. Richard Allan MP has written a submission for the report concerning the Internet pilot held in Sheffield. His submission seems to bear out the opinion of experts.

He wrote, "One polling station (Hunters Bar School, Broomhill Ward) never received its ISDN line installation. This meant that it could do no online checking all day and had to work from a hastily supplied paper register. There was no way to verify if people voting at that station had voted online or elsewhere meaning that anyone in that ward could vote twice - once at Hunters Bar School and once by any other method.

There were problems with several of the ISDN lines during the day. I encountered engineers at a couple of sites who told me they had been drafted in urgently as the main election contractors, BT, did not have the personnel available to deal with the call-outs. Each time an ISDN line went down no online checking could be carried out.

The most worrying result of the cumulative problems was the lack of security evident in this election in terms of ensuring that people only voted once.

All Broomhill residents could easily have voted twice all day. Most residents in other wards could have voted twice by visiting a polling station that was not performing checks at some point in the day.

People who had no right at all to vote in a ward election could have done so by going to a polling station with no online checking and giving any reasonable sounding name and address.

I am confident that these failures would have been sufficient to lead to a challenge to the result if any party had lost by just a few votes in this election."

The message is clear when using technology to support the fabric of society we must be cautious and ensure that cyber terrorism threats are effectively counteract to the satisfaction of the citizens of society.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson  
Director  
Centre for Computing and Social Responsibility  
Faculty of Computing Sciences and Engineering  
De Montfort University  
The Gateway  
Leicester  
LE1 9BH  
Tel:(+44) 116 257 7475  
Fax:(+44) 116 207 8159  
Email:<srog@dmu.ac.uk>  
Home Page: ( <http://www.ccsr.cse.dmu.ac.uk> )