nature

www.nature.com/nature

Vol 458 | Issue no. 7241 | 23 April 2009

Wanted: cyber-czars

The world needs stronger leadership in safeguarding the security of computation and communication networks. That includes research institutions.

Neglected though they may be compared with the financial meltdown, climate change and pandemics, cyberattacks are just as much of a global threat. Like those others, they demand coordinated action and leadership by governments, which have a duty to boost research on the topic. But the threat also needs to be tackled by research institutions, which have a key role in encouraging the adoption and sharing of best practices, and in promoting an awareness of the risks among researchers at the bench.

The much-publicized Conficker worm, which has infected as many as 15 million computers worldwide since it was first detected in October last year, is the most prominent recent example of the problem. Not only has the number of network attacks soared since the 1990s, but the attackers are no longer just teenage hackers looking for peer-group glory. Increasingly, they include organized-crime networks that are engaging in spamming, identify theft and industrial and scientific espionage for profit. More ominously still, state and other organizations have begun to target their cyberattacks on crucial infrastructure such as information networks and the electricity grid.

The United States bears a special responsibility for fighting cyberattacks and scams, being the largest single source of them. Recognizing such a need, the administration of former US President George W. Bush began to beef up federal defences with a mostly classified, cross-agency Comprehensive National Cyber Security Initiative that was launched in January 2008. Last week, the administration of current President Barack Obama completed its own review of federal cybersecurity efforts. The study has yet to be made public, but will probably recommend that the White House coordinates cybersecurity efforts between federal agencies and the private sector.

And two bills on the subject have now been introduced in the US Senate. One would give the president the authority to create and enforce cybersecurity standards. The other would put the National Science Foundation (NSF) in charge of related federal research and provide the agency with an additional $1.7 billion for cybersecurity research and education over the next five years.

The United States is not acting alone. The European Commission, for example, introduced a scheme last month to strengthen the European Union's cybersecurity efforts by encouraging standard approaches to prevention, detection and mitigation in its member states.

These are all steps in the right direction, but translating them into action will be a huge task. The fight against cyberattacks can never be 'won'. Cybersecurity is an arms race in which ever-more sophisticated responses will be needed as new threats emerge.

Research is therefore vital, yet many US observers, including the National Research Council, have concluded that federal funding for such research is too low and too erratic. The NSF has made substantial investments in this area, as have the departments of energy and homeland security. But the Defense Advanced Research Projects Agency, formerly a mainstay of such research, dropped out almost entirely during the Bush administration to focus on short-term military projects. Congress and the Obama administration, through whatever mechanism they finally set up, need to provide much more consistency and coordination in the nation's research efforts.

But cybersecurity is much more than a technological problem, and the most pressing needs are for greater awareness and adoption and deployment of the latest best practices and tools. Computer-savvy researchers involved in the electricity grid and other large research networks are at the forefront here, whereas universities have been laggards. If governments need cybersecurity czars and proactive policies, so too does every university. Most researchers at the bench have neither the time nor the skill to be security experts, and nor should they — it is for their institutions to do the heavy lifting in promoting a culture of cybersecurity.

"If governments need cybersecurity czars and proactive policies, so too does every university."

An increasing number of researchers are coming to believe that the Internet itself needs to be redesigned, as it was never created with security in mind. One way to do that would be to build in accountability from the start, by encoding data packets in a way that would make it harder for hackers to hide their true location. This idea is highly controversial in the networking community, not least because it raises serious concerns about privacy. But it would deprive attackers of their anonymity. It should be considered seriously. ■

More than hot air

The United States has finally acknowledged that global warming is a threat. It must now act on that.

Last week, the US Environmental Protection Agency (EPA) opened up yet another front in the climate-policy debate by issuing a document that proposes to acknowledge that greenhouse gases pose a threat to human welfare. To climate scientists, that statement, which is subject to a 60-day comment period, may sound like an utterly bland assertion of the obvious. But sadly — because it should have happened long ago — the announcement is exactly what so many supporters have hailed it to be: a landmark in US environmental history. It is the EPA's first formal claim that it has the power to regulate greenhouse-gas emissions without any further authorization from Congress.

What is not yet clear is how this action is going to play out. In one scenario, for example, the EPA would indeed go it alone. The US Supreme Court endorsed the agency's authority to do so in 2007,