Cyberwarfare challenge

National cybersecurity plans should go beyond the cold-war mentality of an arms race and focus more on linking traditional computer security with protections for industrial control systems.

If anyone needs proof that a cyber arms race is in the making, they need look no further than last week's news headlines. In the United States, the Pentagon is expected soon to release a report — or at least an unclassified version of a report — describing how the US government might respond to a cyberattack that causes physical damage. One option, according to a report in *The Wall Street Journal*, might be to forgo the subtlety of a cyberresponse, and drop bombs on a suspected attacker.

Similarly, in an editorial in *The Guardian* last week, UK defence minister Nick Harvey revealed the creation of a cyber operations group that would place cyberwarfare on a footing similar to conventional military operations. "Cyber will be part of a continuum of tools with which to achieve military effect, both defensive and otherwise, and will be an integral part of our armoury," Harvey wrote.

It is now nearly a year since the alert was first raised about Stuxnet, the malicious software, or malware, that targeted Iran's nuclear programme. It is hardly surprising, therefore, that governments are now coming forward with plans for cyberwar. Yet the intensive push for cyberweapons only highlights a glaring gap in openly funded research for cyberdefence. Indeed, Stuxnet, possibly the first truly government-backed cyberweapon, was eventually defused not by military cyber warriors, but by private researchers (see page 142).

Stuxnet is clearly a game-changer, demonstrating an ability to target a cyberattack on a grand scale. The subsequent call for the development of cyberweapons sounds very much like the cold-war push to build ever larger nuclear arsenals — and no doubt claims of cyberweaponry gaps will arise. In the United States, the Department of Homeland Security is waging a campaign to engage anybody working with a computer. Governments, it is clear, will have responsibilities to protect infrastructure and installations, but private companies and individuals will be expected to take increasing responsibility for their own and therefore everybody else's protection.

There is a real and profound public vulnerability that should motivate countries to invest in cybersecurity research: the antiquated state of security for industrial control systems, which makes even the most-developed countries as vulnerable as Iran to a Stuxnet-like attack.

It is not just the power plants or the electricity grid that are at risk. In the United States, for example, the water industry is particularly vulnerable, according to experts. Run by small organizations, highly fragmented and with few resources to invest in security, the nation's water supply is an inviting target for attack. The food industry, not traditionally the focus of public concerns about cybersecurity, is another soft spot. Most people don't realize that programmable logic controllers, the devices targeted by Stuxnet, are used to run the heavily automated food-packaging industry. And the Stuxnet history shows that however isolated in cyberspace the target is, there is still a major threat of a spread to any system controlled by software.

On the research side, Stuxnet highlights several challenges worthy of scientific pursuit and government support. Experts point to the need to go beyond the current generation of signature-based anti-virus software. And scientists bemoan the lack of access to good data — in this case viruses — that are needed to help them conduct research. Then there's the need to bridge the gap between traditional computer security and research into industrial-control-system security.

"Stuxnet is proof that governments can bring together different branches of research."

Despite those challenges, the US government has no clear research agenda, or even research community, that focuses on cybersecurity.

This problem could be tackled in many ways, but the first step might be to create a national research plan for cybersecurity, appointing a lead agency that would coordinate research, and perhaps even funding centres of excellence at various universities to encourage interdisciplinary research.

Stuxnet is proof that governments can — when they so choose — bring together different branches of research and bridge the gap between computer-security researchers and the industrial-control-system-security community. If governments can do this to create cyberweapons, they should be equally capable of driving research into cyberdefence. ■

Second chances

Leaders must end a run of unmet pledges when they meet to discuss sustainable development.

Next June, world leaders will gather in Rio de Janeiro, Brazil, for Earth Summit 2012, to discuss (again) how to steer the planet towards a more sustainable future. The gathering marks the 20th anniversary of the 1992 Rio Earth Summit, at which heads of state agreed on a set of principles intended to guide sustainable global economic growth — including the precept that environmental protection should be central to development.

Little progress has been made on this in the two decades since the summit. Rather, countries have continued to pursue relatively unrestricted economic development, with limited attempts to minimize environmental impacts. So, will next year's summit do any better?

Those who attend will be forced to confront a string of failures to meet international green goals, including a pledge to stem the loss of biodiversity by 2010 — as agreed under the Convention on Biological Diversity — and to set new binding targets to reduce greenhouse-gas