

The threat from the internet

## Cyberwar

It is time for countries to start talking about arms control on the internet

Jul 1st 2010



THROUGHOUT history new technologies have revolutionised warfare, sometimes abruptly, sometimes only gradually: think of the chariot, gunpowder, aircraft, radar and nuclear fission. So it has been with information technology. Computers and the internet have transformed economies and given Western armies great advantages, such as the ability to send remotely piloted aircraft across the world to gather intelligence and attack targets. But the spread of digital technology comes at a cost: it exposes armies and societies to digital attack.

The threat is complex, multifaceted and potentially very dangerous. Modern societies are ever more reliant on computer systems linked to the internet, giving enemies more avenues of attack. If power stations, refineries, banks and air-traffic-control systems were brought down, people would lose their lives. Yet there are few, if any, rules in cyberspace of the kind that govern behaviour, even warfare, in other domains. As with nuclear- and conventional-arms control, big countries should start talking about how to reduce the threat from cyberwar, the aim being to restrict attacks before it is too late.

### The army reboots

Cyberspace has become the fifth domain of warfare, after land, sea, air and space (see [article](#)). Some scenarios imagine the almost instantaneous failure of the systems that keep the modern world turning. As computer networks collapse, factories and chemical plants explode, satellites spin out of control and the financial and power grids fail.

That seems alarmist to many experts. Yet most agree that infiltrating networks is pretty easy for those who have the will, means and the time to spare. Governments know this because they are such enthusiastic hackers themselves. Spies frequently break into computer systems to steal information by the warehouse load, whether it is from Google or defence contractors. Penetrating networks to damage them is not much harder. And, if you take enough care, nobody can prove you did it.

The cyber-attacks on Estonia in 2007 and on Georgia in 2008 (the latter strangely happened to coincide with the advance of Russian troops across the Caucasus) are widely assumed to have been directed by the Kremlin, but they could be traced only to Russian cyber-criminals. Many of the computers used in the attack belonged to innocent Americans whose PCs had been hijacked. Companies suspect China of organising mini-raids to ransack Western know-how: but it could just have easily been Western criminals, computer-hackers showing off or disillusioned former employees. One reason why Western governments have until recently been reticent about cyber-espionage is surely because they are dab hands at it, too.

As with nuclear bombs, the existence of cyber-weapons does not in itself mean they are about to be used. Moreover, an attacker cannot be sure what effect an assault will have on another country, making their deployment highly risky. That is a drawback for sophisticated military machines, but not necessarily for terrorists or the armies of rogue states. And it leaves the dangers of online crime and espionage.

All this makes for dangerous instability. Cyber-weapons are being developed secretly, without discussion of how and when they might be used. Nobody knows their true power, so countries must prepare for the worst. Anonymity adds to the risk that mistakes, misattribution and miscalculation will lead to military escalation—with conventional weapons or cyberarms. The speed with which electronic attacks could be launched gives little time for cool-headed reflection and favours early, even pre-emptive, attack. Even as computerised weapons systems and wired infantry have blown away some of the fog of war from the battlefield, they have covered cyberspace in a thick, menacing blanket of uncertainty.

One response to this growing threat has been military. Iran claims to have the world's second-largest cyber-army. Russia, Israel and North Korea boast efforts of their own. America has set up its new Cyber Command both to defend its networks and devise attacks on its enemies. NATO is debating the extent to which it should count cyberwar as a form of "armed attack" that would oblige its members to come to the aid of an ally.

But the world needs cyberarms-control as well as cyber-deterrence. America has until recently resisted weapons treaties for cyberspace for fear that they could lead to rigid global regulation of the internet, undermining the dominance of American internet companies, stifling innovation and restricting the openness that underpins the net. Perhaps America also fears that its own cyberwar effort has the most to lose if its well-regarded cyberspies and cyber-warriors are reined in.

Such thinking at last shows signs of changing, and a good thing too. America, as the country most reliant on computers, is probably most vulnerable to cyber-attack. Its conventional military power means that foes will look for asymmetric lines of attack. And the wholesale loss of secrets through espionage risks eroding its economic and military lead.

### **Hardware and soft war**

If cyberarms-control is to America's advantage, it would be wise to shape such accords while it still has the upper hand in cyberspace. General Keith Alexander, the four-star general who heads Cyber Command, is therefore right to welcome Russia's longstanding calls for a treaty as a "starting point for international debate". That said, a START-style treaty may prove impossible to negotiate. Nuclear warheads can be counted and missiles tracked. Cyber-weapons are more like biological agents; they can be made just about anywhere.

So in the meantime countries should agree on more modest accords, or even just informal "rules of the road" that would raise the political cost of cyber-attacks. Perhaps there could be a deal to

prevent the crude “denial-of-service” assaults that brought down Estonian and Georgian websites with a mass of bogus requests for information; NATO and the European Union could make it clear that attacks in cyberspace, as in the real world, will provoke a response; the UN or signatories of the Geneva Conventions could declare that cyber-attacks on civilian facilities are, like physical attacks with bomb and bullet, out of bounds in war; rich countries could exert economic pressure on states that do not adopt measures to fight online criminals. Countries should be encouraged to spell out their military policies in cyberspace, as America does for nuclear weapons, missile defence and space. And there could be an international centre to monitor cyber-attacks, or an international “duty to assist” countries under cyber-attack, regardless of the nationality or motive of the attacker—akin to the duty of ships to help mariners in distress.

The internet is not a “commons”, but a network of networks that are mostly privately owned. A lot could also be achieved by greater co-operation between governments and the private sector. But in the end more of the burden for ensuring that ordinary people’s computer systems are not co-opted by criminals or cyber-warriors will end up with the latter—especially the internet-service providers that run the network. They could take more responsibility for identifying infected computers and spotting attacks as they happen.

None of this will eradicate crime, espionage or wars in cyberspace. But it could make the world a little bit safer.

Leaders