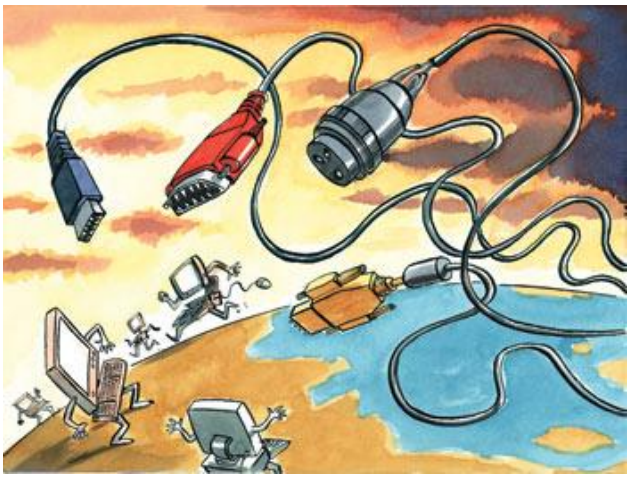
Cyberwarfare

Newly nasty

May 24th 2007
From The Economist print edition



Defences against cyberwarfare are still rudimentary. That's scary

IMAGINE that agents of a hostile power, working in conjunction with organised crime, could cause huge traffic jams in your country's biggest cities—big enough to paralyse business, the media, government and public services, and to cut you off from the world. That would be seen as a grave risk to national security, surely?

Yes—unless the attacks came over the internet. For most governments, defending their national security against cyberwarfare means keeping hackers out of important government computers. Much less thought has been given to the risks posed by large-scale disruption of the public internet. Modern life depends on it, yet it is open to all comers. That is why the world's richest countries and their military planners are now studying intensively the attacks on Estonia that started four weeks ago, amid that country's row with Russia about moving a Soviet-era war memorial.

Even at their crudest, the assaults broke new ground. For the first time, a state faced a frontal, anonymous attack that swamped the websites of banks, ministries, newspapers and broadcasters; that hobbled Estonia's efforts to make its case abroad. Previous bouts of cyberwarfare have been far more limited by comparison: probing another country's internet defences, rather as a reconnaissance plane tests air defences.

At full tilt, the onslaught on Estonia was also of a sophistication not seen before, with tactics shifting as weaknesses emerged. "Particular 'ports' of particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet 'bombs' of hundreds of megabytes in size would be sent first to one address, then another," says Linnar Viik, Estonia's top internet guru. Such efforts exceed the skills of individual activists or even organised crime; they require the co-operation of a state and a large telecoms firm, he says. The effects could have been life-threatening. The emergency number used to call ambulances and the fire service was out of action for more than an hour.

For many countries, the events of the past weeks have been a loud wake-up call. Estonia, one of the most wired nations in Europe, actually survived pretty well. Other countries would have fared worse, NATO specialists reckon.

National security experts used to dealing with high-explosives and body counts find cyberwarfare a baffling new theatre of operations. In Estonia's case, "botnets" (swarms of computers hijacked by surreptitiously placed code, usually spread by spam) swamped sites by deluging them with bogus requests for information. Called a "distributed denial of service" (DDOS) attack, this at its peak involved more than 1m computers, creating traffic equivalent to 5,000 clicks per second on some targets. Some parts were highly co-ordinated—stopping precisely at midnight, for example. Frank Cilluffo, an expert formerly at the White House, says that the attack's signature suggests that more than one group was at work, with small-time hackers following the initial huge sorties.

Most countries have been complacent about guarding information infrastructure. In America, a congressional committee for computer security has given failing grades to many of the federal bodies it scrutinises. The Department of Homeland Security supposedly has a "cybersecurity czar" but the throne has not yet found a steady occupant.

Private firms have had more experience in fighting off internet attacks. Organised crime gangs, often from Eastern Europe, extort money from gambling and pornography sites by using botnets to make them unreachable. Last week a large DDOS attack hit YLE, Finland's public broadcaster. This week Britain's *Daily Telegraph* was hit. No political or financial motive was apparent. A Romania-based hacker led the Finnish attack.

Firms of varying competence and credibility peddle technical solutions. The typical protection against DDOS attacks is to buy lots of extra computers and bandwidth to handle an unexpected spike in traffic. "Mirroring" content across several servers means the cyber-attackers must hit many more targets simultaneously before disrupting anything. A system's architecture helps too: Estonia's open approach, with its built-in flexibility and resilience, and co-operation between the state, business and academics, worked well. Mr Viik hopes this will deter those trying to build cyberdefences on a military or state monopoly model.

Counterattacks are possible, but tricky. Security firms' staff can pose as hackers to infiltrate cybergangsterdom. This used to be a mere battle of wits. Now there are real fears of violence. "It's changed now that big money is involved. It is not beyond the realm of imagination that someone might be targeted," says Mikko Hyppönen of F-Secure, an internet security firm.

But technology and sleuthing offer only a partial fix. The real question facing industrialised countries is how to create a legal environment that counts cyberaggression not as a kind of practical joke, but a grave breach of the legal order, akin to terrorism, international organised crime, or aggression against another state.

NATO is rethinking its position. It is designed to protect members against physical attack. When Estonia appealed for help it could only send an observer to Tallinn to monitor the attacks. For now, informal alliances are more useful. Internet companies in friendly countries such as Sweden headed off many of the attacks before they even reached Estonia. Ken Silva, the security chief at VeriSign, which runs big chunks of the internet's domain-name system, advocates defences at the core of the network to tackle malicious data-

packets before they reach their target. But finding agreement among the world's privately run internet networks is hard.

The urgent need is for an international legal code that defines cybercrimes more precisely, and offers the basis for some remedies. The Council of Europe, a continent-wide talking-shop that is the guardian of many international legal conventions, has a treaty on cybercrime dating from 2001. Acceptance has been partial. From overseas, America and Japan have signed up; Russia so far hasn't.

The International Telecommunication Union, which unites all 191 countries that use the world telephone system, hopes to take the lead in pushing for a global convention against cybercrime. Alexander Mtoko, its expert on cyberwarfare, says the key issue is anonymity: "We are in an industry where there is no control, no rules, no identities—it's the wild west. But for critical applications you have to know who you are dealing with." NATO experts agree. At a minimum, any international cybercrime convention is likely to oblige internet service providers to co-operate in blocking DDOS attacks coming from their subscribers' computers.

Yet the underlying problem is the internet itself. Wreaking havoc with anonymous telephone calls is hard. The internet's inherent openness allows hackers to hide. Yet that also helps make it cheap and innovative. Some countries may be more willing than others to trade freedom for security.

Mr Viik thinks a new global cybersecurity treaty may be reached by 2012. But victory will never be complete, thanks to the asymmetry between cat and mouse, notes Bruce Schneier, a security expert. "It is easier to come up with a new attack than with a new defence," he says. The strongest defence, says Mr Cilluffo, may be resilience: "the ability to reconstitute quickly, recover and absorb."

Greatest hits

May 24th 2007
From The Economist print edition

Milestones in the history of information warfare

1986—The Cuckoo's Egg: A Soviet-backed hacker in Hanover, Germany, is caught breaking into computers at America's Lawrence Berkeley Labs to steal missile-defence secrets.

1998-99—Moonlight Maze: America traces a series of computer break-ins at the Pentagon, NASA and elsewhere to a computer in Russia (which denies involvement). Many files containing classified information are compromised.

1999—Kosovo: Chinese hackers break in and vandalise American government websites in retaliation for the bombing of the Chinese embassy in Belgrade by American aircraft. The White House website closes for three days.

2000-01—Middle East: Israeli and Arab hackers vandalise and crash each others' websites over a four-month period. Attacks also occur against telecoms firms supplying internet connections.

2001–America v China: After an American spyplane and Chinese fighter collide, hackers from both countries deface or crash the other's public and private-sector websites. The White House and *New York Times* sites are briefly brought down.

2006—Sneaky Word Doc: An American State Department employee opens an e-mailed file that secretly opens a backdoor in the computer system, allowing the theft of data. As the problem escalates, the agency cuts internet access, leaving some officials offline for weeks.

2007—Netwarcom: Officials at America's Naval Network Warfare Command (Netwarcom) accuse China of sponsoring hundreds of suspicious hacking incidents each day against military and private-sector computer systems to steal technology, gather intelligence, probe defences and install "sleeper" software.