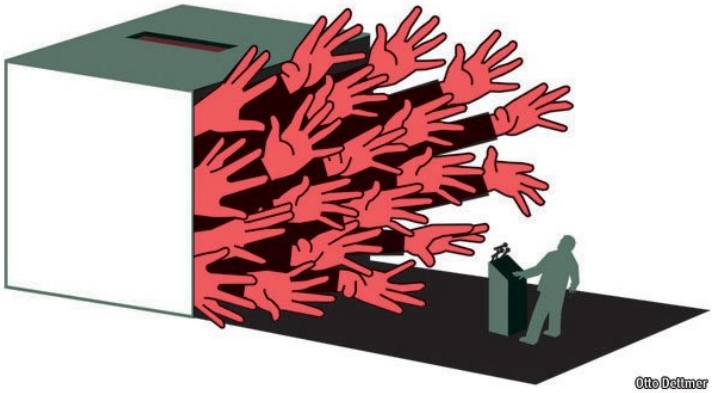
The Economist

High-tech warfare

Something wrong with our **** chips today

Kill switches are changing the conduct and politics of war

Apr 7th 2011 | from the print edition



IN THE 1991 Gulf war Iraq's armed forces used American-made colour photocopiers to produce their battle plans. That was a mistake. The circuitry in some of them contained concealed transmitters that revealed their position to American electronic-warfare aircraft, making bomb and missile strikes more precise. The operation, described by David Lindahl, a specialist at the Swedish Defence Research Agency, a government think-tank, highlights a secret front in high-tech warfare: turning enemy assets into liabilities.

The internet and the growing complexity of electronic circuitry have made it much easier to install what are known as "kill switches" and "back doors", which may disable, betray or blow up the devices in which they are installed. Chips can easily contain 2 billion transistors, leaving plenty of scope to design a few that operate secretly. Testing even a handful of them for anomalies requires weeks of work.

Kill switches and other remote controls are on the minds of Western governments pondering whether to send weapons such as sophisticated anti-tank missiles, normally tightly policed, to rebels in Libya. Keeping tabs on when and where they are fired will allay fears that they could end up in terrorist hands. Such efforts would not even need to be kept secret. A former CIA official says the rebels could be told: "Look, we're going to give you this, but we want to be able to control it."

That lesson was first learned in Afghanistan in the 1980s, when America supplied Stinger missiles to help Afghan fighters against Soviet helicopter gunships, only to have to comb the region's arms bazaars in later years to buy them back (some were then booby-trapped and sold again, to deter anyone tempted to use them).

America worries about becoming the victim of kill switches itself. Six years ago a report by America's Defence Science Board, an official advisory body, said "unauthorised design inclusions" in foreign-made chips could help an outside power gain a measure of control over critical American hardware.

Chips off the home block

In response, America has launched schemes such as the Trusted Foundry Programme, which certifies "secure, domestic" facilities for the manufacture of the most critical microchips. The Defence Advanced Research Projects Agency (DARPA), a Pentagon outfit devoted to expanding the

military's technological abilities, will spend at least $20m this year on ways to identify rogue microchips. The Army Research Office is holding a closed conference on kill switches in mid-April.

Farinaz Koushanfar, a DARPA-funded expert at Texas's Rice University, says microchip designers would like to be able to switch off their products "in the wild", in case the contractors that make the chips produce some extra ones to sell on the sly. She designs "active hardware metering" chips that, in devices connected to the internet, can remotely identify them and if necessary switch them off.

An obvious countermeasure is to keep critical defence equipment off the net. But that is only a partial solution. Chips can be designed to break down at a certain date. An innocent-looking component or even a bit of soldering can be a disguised antenna. When it receives the right radio signal, from, say, a mobile-phone network, aircraft or satellite, the device may blow up, shut down, or work differently.

Old-fashioned spying can reveal technological weaknesses too. Mr Lindahl says Sweden obtained detailed information on circuitry in a heat-seeking missile that at least one potential adversary might, in wartime, shoot at one of its eight C-130 Hercules military-transport planes. A slight but precise change in the ejection tempo of the decoy flares would direct those missiles towards the flame, not the aircraft.

Such tricks may be handy in dealing with unreliable allies as well as foes, but they can also hamper Western efforts to contain risk in unstable countries. Pakistan has blocked American efforts to safeguard its nuclear facilities. The country's former ambassador to the United Nations, Munir Akram, cites fears that such measures will include secret remote controls to shut the nuclear programme down. A European defence official says even video surveillance cameras can intercept or disrupt communications. To avoid such threats, Pakistani engineers laboriously disassemble foreign components and replicate them.

Wesley Clark, a retired general who once headed NATO's forces, says that "rampant" fears of kill switches make American-backed defence co-operation agreements a harder sell. David Kay, a notable United Nations weapons inspector in Iraq, bemoans "scepticism and paranoia". You just can't trust anybody these days, even in the weapons business.

from the print edition | International