

Cyberwar

## War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010



AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would “go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds,” according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, “was the most monumental non-nuclear explosion and fire ever seen from space.”

This was one of the earliest demonstrations of the power of a “logic bomb”. Three decades later, with more and more vital computer systems linked up to the internet, could enemies use logic bombs to, say, turn off the electricity from the other side of the world? Could terrorists or hackers cause financial chaos by tampering with Wall Street’s computerised trading systems? And given that computer chips and software are produced globally, could a foreign power infect high-tech military equipment with computer bugs? “It scares me to death,” says one senior military source. “The destructive potential is so great.”

After land, sea, air and space, warfare has entered the fifth domain: cyberspace. President Barack Obama has declared America’s digital infrastructure to be a “strategic national asset” and appointed Howard Schmidt, the former head of security at Microsoft, as his cyber-security tsar. In May the Pentagon set up its new Cyber Command (Cybercom) headed by General Keith Alexander, director of the National Security Agency (NSA). His mandate is to conduct “full-spectrum” operations—to defend American military networks and attack other countries’ systems. Precisely how, and by what rules, is secret.

Britain, too, has set up a cyber-security policy outfit, and an “operations centre” based in GCHQ, the British equivalent of the NSA. China talks of “winning informationised wars by the mid-21st century”. Many other countries are organising for cyberwar, among them Russia, Israel and North Korea. Iran boasts of having the world’s second-largest cyber-army.

What will cyberwar look like? In a new book Richard Clarke, a former White House staffer in charge of counter-terrorism and cyber-security, envisages a catastrophic breakdown within 15 minutes. Computer bugs bring down military e-mail systems; oil refineries and pipelines explode; air-traffic-control systems collapse; freight and metro trains derail; financial data are scrambled; the electrical grid goes down in the eastern United States; orbiting satellites spin out of control.

Society soon breaks down as food becomes scarce and money runs out. Worst of all, the identity of the attacker may remain a mystery.

In the view of Mike McConnell, a former spy chief, the effects of full-blown cyberwar are much like nuclear attack. Cyberwar has already started, he says, "and we are losing it." Not so, retorts Mr Schmidt. There is no cyberwar. Bruce Schneier, an IT industry security guru, accuses securocrats like Mr Clarke of scaremongering. Cyberspace will certainly be part of any future war, he says, but an apocalyptic attack on America is both difficult to achieve technically ("movie-script stuff") and implausible except in the context of a real war, in which case the perpetrator is likely to be obvious.

For the top brass, computer technology is both a blessing and a curse. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up. Yet growing connectivity over an insecure internet multiplies the avenues for e-attack; and growing dependence on computers increases the harm they can cause.



Enlarge

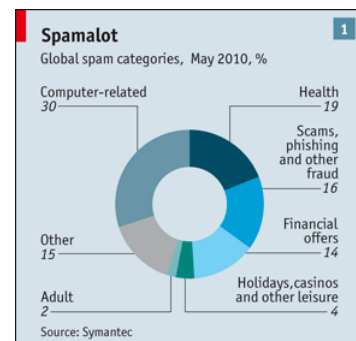
By breaking up data and sending it over multiple routes, the internet can survive the loss of large parts of the network. Yet some of the global digital infrastructure is more fragile. More than nine-tenths of internet traffic travels through undersea fibre-optic cables, and these are dangerously bunched up in a few choke-points, for instance around New York, the Red Sea or the Luzon Strait in the Philippines (see map). Internet traffic is directed by just 13 clusters of potentially vulnerable domain-name servers. Other dangers are coming: weakly governed swathes of Africa are being connected up to fibre-optic cables, potentially creating new havens for cyber-criminals. And the spread of mobile internet will bring new means of attack.

The internet was designed for convenience and reliability, not security. Yet in wiring together the globe, it has merged the garden and the wilderness. No passport is required in cyberspace. And although police are constrained by national borders, criminals roam freely. Enemy states are no longer on the other side of the ocean, but just behind the firewall. The ill-intentioned can mask their identity and location, impersonate others and con their way into the buildings that hold the digitised wealth of the electronic age: money, personal data and intellectual property.

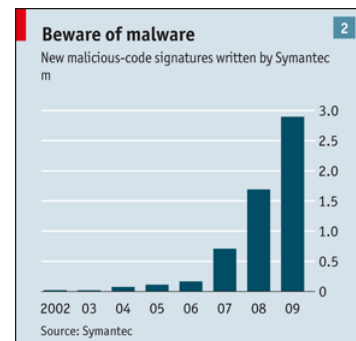
Mr Obama has quoted a figure of \$1 trillion lost last year to cybercrime—a bigger underworld than the drugs trade, though such figures are disputed. Banks and other companies do not like to admit how much data they lose. In 2008 alone Verizon, a telecoms company, recorded the loss of 285m personal-data records, including credit-card and bank-account details, in investigations conducted for clients.

About nine-tenths of the 140 billion e-mails sent daily are spam; of these about 16% contain moneymaking scams (see chart 1), including "phishing" attacks that seek to dupe recipients into giving out passwords or bank details, according to Symantec, a security-software vendor. The amount of information now available online about individuals makes it ever easier to attack a computer by crafting a personalised e-mail that is more likely to be trusted and opened. This is known as "spear-phishing".

The ostentatious hackers and virus-writers who once wrecked computers for fun are all but gone, replaced by criminal gangs seeking to harvest data. "Hacking used to be about making noise. Now it's about staying silent," says Greg Day of McAfee, a vendor of IT security products. Hackers have become wholesale providers of malware—viruses, worms and Trojans that infect computers—for others to use. Websites are now the favoured means of spreading malware, partly because the unwary are directed to them through spam or links posted on social-networking sites. And poorly designed websites often provide a window into valuable databases.



Malware is exploding (see chart 2). It is typically used to steal passwords and other data, or to open a “back door” to a computer so that it can be taken over by outsiders. Such “zombie” machines can be linked up to thousands, if not millions, of others around the world to create a “botnet”. Estimates for the number of infected machines range up to 100m (see map for global distribution of infections). Botnets are used to send spam, spread malware or launch distributed denial-of-service (DDoS) attacks, which seek to bring down a targeted computer by overloading it with countless bogus requests.



### The spy who spammed me

Criminals usually look for easy prey. But states can combine the criminal hacker’s tricks, such as spear-phishing, with the intelligence apparatus to reconnoitre a target, the computing power to break codes and passwords, and the patience to probe a system until it finds a weakness—usually a fallible human being. Steven Chabinsky, a senior FBI official responsible for cyber- security, recently said that “given enough time, motivation and funding, a determined adversary will always—always—be able to penetrate a targeted system.”

Traditional human spies risk arrest or execution by trying to smuggle out copies of documents. But those in the cyberworld face no such risks. “A spy might once have been able to take out a few books’ worth of material,” says one senior American military source, “Now they take the whole library. And if you restock the shelves, they will steal it again.”

China, in particular, is accused of wholesale espionage, attacking the computers of major Western defence contractors and reputedly taking classified details of the F-35 fighter, the mainstay of future American air power. At the end of 2009 it appears to have targeted Google and more than a score of other IT companies. Experts at a cyber-test-range built in Maryland by Lockheed Martin, a defence contractor (which denies losing the F-35 data), say “advanced persistent threats” are hard to fend off amid the countless minor probing of its networks. Sometimes attackers try to slip information out slowly, hidden in ordinary internet traffic. At other times they have tried to break in by leaving infected memory-sticks in the car park, hoping somebody would plug them into the network. Even unclassified e-mails can contain a wealth of useful information about projects under development.

“Cyber-espionage is the biggest intelligence disaster since the loss of the nuclear secrets [in the late 1940s],” says Jim Lewis of the Centre for Strategic and International Studies, a think-tank in Washington, DC. Spying probably presents the most immediate danger to the West: the loss of high-tech know-how that could erode its economic lead or, if it ever came to a shooting war, blunt its military edge.



Western spooks think China deploys the most assiduous, and most shameless, cyberspies, but Russian ones are probably more skilled and subtle. Top of the league, say the spooks, are still America’s NSA and Britain’s GCHQ, which may explain why Western countries have until recently been reluctant to complain too loudly about computer snooping.

The next step after penetrating networks to steal data is to disrupt or manipulate them. If military targeting information could be attacked, for example, ballistic missiles would be useless. Those who play war games speak of being able to “change the red and blue dots”: make friendly (blue) forces appear to be the enemy (red), and vice versa.

General Alexander says the Pentagon and NSA started co-operating on cyberwarfare in late 2008 after “a serious intrusion into our classified networks”. Mr Lewis says this refers to the penetration of Central Command, which oversees the wars in Iraq and Afghanistan, through an infected thumb-drive. It took a week to winkle out the intruder. Nobody knows what, if any,

damage was caused. But the thought of an enemy lurking in battle-fighting systems alarms the top brass.

That said, an attacker might prefer to go after unclassified military logistics supply systems, or even the civilian infrastructure. A loss of confidence in financial data and electronic transfers could cause economic upheaval. An even bigger worry is an attack on the power grid. Power companies tend not to keep many spares of expensive generator parts, which can take months to replace. Emergency diesel generators cannot make up for the loss of the grid, and cannot operate indefinitely. Without electricity and other critical services, communications systems and cash-dispensers cease to work. A loss of power lasting just a few days, reckon some, starts to cause a cascade of economic damage.

Experts disagree about the vulnerability of systems that run industrial plants, known as supervisory control and data acquisition (SCADA). But more and more of these are being connected to the internet, raising the risk of remote attack. "Smart" grids", which relay information about energy use to the utilities, are promoted as ways of reducing energy waste. But they also increase security worries about both crime (eg, allowing bills to be falsified) and exposing SCADA networks to attack.

General Alexander has spoken of "hints that some penetrations are targeting systems for remote sabotage". But precisely what is happening is unclear: are outsiders probing SCADA systems only for reconnaissance, or to open "back doors" for future use? One senior American military source said that if any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis.

### **Estonia, Georgia and WWI**

Important thinking about the tactical and legal concepts of cyber-warfare is taking place in a former Soviet barracks in Estonia, now home to NATO's "centre of excellence" for cyber-defence. It was established in response to what has become known as "Web War 1", a concerted denial-of-service attack on Estonian government, media and bank web servers that was precipitated by the decision to move a Soviet-era war memorial in central Tallinn in 2007. This was more a cyber-riot than a war, but it forced Estonia more or less to cut itself off from the internet.

Similar attacks during Russia's war with Georgia the next year looked more ominous, because they seemed to be co-ordinated with the advance of Russian military columns. Government and media websites went down and telephone lines were jammed, crippling Georgia's ability to present its case abroad. President Mikheil Saakashvili's website had to be moved to an American server better able to fight off the attack. Estonian experts were dispatched to Georgia to help out.

Many assume that both these attacks were instigated by the Kremlin. But investigations traced them only to Russian "hacktivists" and criminal botnets; many of the attacking computers were in Western countries. There are wider issues: did the cyber-attack on Estonia, a member of NATO, count as an armed attack, and should the alliance have defended it? And did Estonia's assistance to Georgia, which is not in NATO, risk drawing Estonia into the war, and NATO along with it?

Such questions permeate discussions of NATO's new "strategic concept", to be adopted later this year. A panel of experts headed by Madeleine Albright, a former American secretary of state, reported in May that cyber-attacks are among the three most likely threats to the alliance. The next significant attack, it said, "may well come down a fibre-optic cable" and may be serious enough to merit a response under the mutual-defence provisions of Article 5.

During his confirmation hearing, senators sent General Alexander several questions. Would he have "significant" offensive cyber-weapons? Might these encourage others to follow suit? How sure would he need to be about the identity of an attacker to "fire back"? Answers to these were restricted to a classified supplement. In public the general said that the president would be the judge of what constituted cyberwar; if America responded with force in cyberspace it would be in keeping with the rules of war and the "principles of military necessity, discrimination, and

proportionality”.

General Alexander’s seven-month confirmation process is a sign of the qualms senators felt at the merging of military and espionage functions, the militarisation of cyberspace and the fear that it may undermine Americans’ right to privacy. Cybercommand will protect only the military “.mil” domain. The government domain, “.gov”, and the corporate infrastructure, “.com” will be the responsibility respectively of the Department of Homeland Security and private companies, with support from Cybercom.

One senior military official says General Alexander’s priority will be to improve the defences of military networks. Another bigwig casts some doubt on cyber-offence. “It’s hard to do it at a specific time,” he says. “If a cyber-attack is used as a military weapon, you want a predictable time and effect. If you are using it for espionage it does not matter; you can wait.” He implies that cyber-weapons would be used mainly as an adjunct to conventional operations in a narrow theatre.

The Chinese may be thinking the same way. A report on China’s cyber-warfare doctrine, written for the congressionally mandated US-China Economic and Security Review Commission, envisages China using cyber-weapons not to defeat America, but to disrupt and slow down its forces long enough for China to seize Taiwan without having to fight a shooting war.

### **Apocalypse or asymmetry?**

Deterrence in cyber-warfare is more uncertain than, say, in nuclear strategy: there is no mutually assured destruction, the dividing line between criminality and war is blurred and identifying attacking computers, let alone the fingers on the keyboards, is difficult. Retaliation need not be confined to cyberspace; the one system that is certainly not linked to the public internet is America’s nuclear firing chain. Still, the more likely use of cyber-weapons is probably not to bring about electronic apocalypse, but as tools of limited warfare.

Cyber-weapons are most effective in the hands of big states. But because they are cheap, they may be most useful to the comparatively weak. They may well suit terrorists. Fortunately, perhaps, the likes of al-Qaeda have mostly used the internet for propaganda and communication. It may be that jihadists lack the ability to, say, induce a refinery to blow itself up. Or it may be that they prefer the gory theatre of suicide-bombings to the anonymity of computer sabotage—for now.

Briefing