01

01 Lorem ipsum dolor sit amet con sectetuer
02 Aenean eros nulla ullamcorper dapibus lorem
03 Vivamus semper tellus a sem aenean

02

PORTAL COMBAT —*Tallinn*

Preface
Warfare in the 21st century is as likely to be fought on computer screens as it is on battlefields. Monocle goes to Estonia to meet the web wizards preventing hackers and 'cyber-jihadis' from attacking Nato member states via the internet.

WRITER
Adam LeBor

PHOTOGRAPHER
Juho Kuva

03

With their landscaped gardens and verdant lawns, the former Tsarist army barracks in Tallinn seem strangely quiet for a highly classified military base. There are no tanks lumbering across the fields or artillery thundering, merely walls of monitors and rows of work-stations. No gunfire echoes in the background, only the quiet click of keyboards. But the tranquil scene is deceptive, for the Cooperative Cyber Defence Centre of Excellence (CCDCOE) is on the frontline in the coming conflicts: cyber wars. The most potent weapon in the 21st century will not be a gun or a tank, but the simple binary code that drives the computers on which we now all rely for our daily needs.

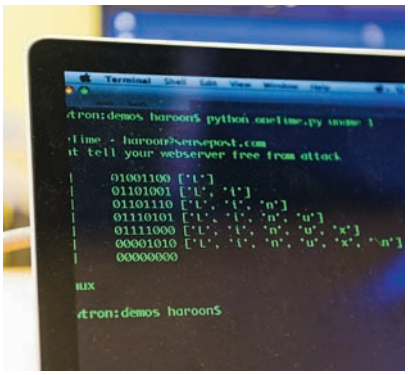
Estonia knows this better than most. It is one of the most wired countries in the world and was a pioneer in e-government. But it learned the hard way that increased connectivity means increased vulnerability. In spring 2007, a sustained series of cyber attacks brought down this Baltic nation's banking services, disrupted its connectivity, and disabled numerous government websites. The attacks lasted several weeks and were highly organised, sophisticated and successful. They were traced back to Russian hackers. No state complicity was ever proven and Russia denied any involvement.

After the attacks, Tallinn was the obvious choice to host the CCDCOE, which is accredited by Nato as an international military organisation. MONOCLE was granted rare access to the centre, where behind the thick, raw-brick walls Nato cyber-warfare specialists are working on new strategies to repel cyber attacks and protect the west's infrastructure systems.

The threat is real, and growing, say experts. As the internet has democratised communication and the spread of information, it has also brought cyber war within the reach of anyone with basic computer skills, says Rain Ottis, an Estonian scientist at CCDCOE. "The barrier for fighting a cyber war is much lower than for regular conflict. If you want to engage with a soldier in Afghanistan you have to travel there, that takes time and money, you have to find a weapon, learn how to shoot and identify the soldiers' routes, and then finally you can engage the enemy. In cyberspace you open your laptop and start engaging right away."

Basic techniques are very simple: for example, pressing the F5 key refreshes the content of a web browser as it views a website. With enough people doing this at


01



03

04


02

the same time, the website will crash: a DOS, or denial-of-service, attack. Easily downloadable programs, available on hacker websites, can automate this process. Botnet software, which covertly controls thousands of computers without their owners' knowledge, and which can be purchased on the internet, can be used to launch a DDOS, or distributed denial-of-service, attack.

"We are entering into a new dimension that has a real impact on our daily lives," says Jaak Aaviksoo, Estonia's minister of defence. The 2007 attacks were a wake-up call for the west. "That was a ringing of the bell, that cyber security is not limited to individuals, or to commerce or industry but is a national-security issue. We learnt that networked offence must have a networked defence, that the world is smaller than we think, and global cooperation in all aspects is important."

No lives were lost, but the psychological effects were serious. Still, there was also an upside, says Aaviksoo, smiling. The cyber attacks put this small Baltic nation of 1.3 million firmly on the map. "We could never have afforded a PR campaign like that which was provided for us by persons still unknown."

Increasingly, cyber war is fought in a political context: the attack on Estonia followed a furore about the relocation of a Soviet war memorial. As Georgian troops battled Abkhazian separatists in 2008 "hacktivists" launched a parallel front in cyberspace. Attacks on Israel soared during the second Lebanon war in 2006 and the assault on Gaza in 2008. The stock market, banks and municipal sites with information about the location of air-raid shelters were all targeted. Pictures of slain Israeli soldiers were posted on a hospital website, damaging morale.

Israel is under constant cyber attack, says Assaf Keren, director of information security for the country's e-government department. The fear is that hackers – dubbed cyber-jihadis – spread around the Middle East, will unite. "They have the numbers and they have some very good people. Attacker kits are available on the internet for beginner cyber-jihadis. You just have to download, install, press a button and it will do everything for you."

It was probably inevitable that cyberspace would become the fifth domain of war – after land, sea, air and space. The internet has its roots in Arpanet, the Advanced Research Project Agency Network, a digital communications network created by a team at MIT and the US Department of Defense in the 1960s. And cyber war predates today's internet: in June 1982 a Soviet gas pipeline exploded in Siberia after its computer control centre malfunctioned. Soviet spies had

Geek speak

Air-gapped network: Computer network isolated from external influences and not connected to the internet, eg military.

Botnet: Remotely controlled network of computers that have been taken over to attack other computers, without owners' knowledge.

DDOS: Distributed denial-of-service attack – overloads a computer, causing it to crash by directing a flood of information requests from multiple computers, usually a botnet.

Drive-by-downloads: Malicious programme that installs covertly when owner clicks a link, opens email or visits infected website.

Exploit: Using a known vulnerability in software or operating system that has not yet been patched.

Malware: Malicious software that infects a computer without owner's consent, such as a virus.

Remote access tool: Allows access to and control of computer or network from outside location.

Sandbox: A secure computer space for running suspect programs or suspicious code.

Trojan horse: Software that seems legitimate, eg a web-browser update, but which provides back-door access to user's computer and operating system.

Virus: Computer code that uses host system to self-replicate and pass on to other systems.

Zero day: Software vulnerability that is unknown to developer and which has no available patch.

05

06

01 Lorem ipsum dolor sit amet con
02 Aenean eros nulla ullamcorper dapibus
03 Vivamus semper tellus a sem aenean
04 Lorem ipsum dolor sit amet con sectetuer
05 Aenean eros nulla ullamcorper dapibus
06 Vivamus semper tellus a sem aene
07 Aenean eros nulla ullamcorper dapibus
08 Vivamus semper tellus a sem aenean

07

08

stolen the technology from a company in Canada. What they didn't know was that the CIA knew of their plans, and tampered with the settings to cause the explosion. Nowadays the ever-deeper digitalisation of our daily lives – from air traffic control to banking – makes policy-makers quake at the potential for enemy states or terrorists to cause chaos and even a complete break-down in society. In May, the Pentagon set up Cyber Command with a "full spectrum" mandate to defend the US's critical infrastructure.

Unlike conventional warfare, where two enemies face each other across the battlefield, cyber war is asymmetric. Hackers can hijack a network halfway around the world to launch an attack and it may not be possible to discover who and where they are. "The vulnerabilities of the internet and its core infrastructure can be exploited by anybody who has the appropriate resources and know-how," Melissa Hathaway, who served on President Obama's National Security Council and is now president of Hathaway Global Strategies, told MONOCLE. Nato has now highlighted cyber warfare in its strategic review, but awareness of cyber security is still at a nascent stage. "We need to be addressing this. Nato is completely dependent on connectivity of our nations for both information flow and deployment of our military forces, so the security of that information system has to become a higher priority," adds Hathaway.

Other Nato nations agree. "Cyber issues tend to be regarded by people over 50, maybe even over 40, as something a bit beyond them," says a senior British official. "They know it's important and we should do something but when you start to get into it, they get nervous." The asymmetric nature of cyber conflict and the near instantaneous speed of data transfer demand a rapid and devolved decision-making process, something neither governments nor bureaucracies are good at. "The things that could happen in an all-out cyber war and the speed at which it would work are terrifying. You have to take instant decisions and you have to allow these decisions to be taken at quite a low level. If you are under attack you cannot call a cabinet meeting to decide what to do because by that time you are finished. Somebody has to say we are under attack and we have to shut down, and that could be the equivalent of a corporal."

But not everyone is convinced of the threat. "It's bad public policy to create a bunch of scare scenarios and say this is what we should base our policy decisions on," says Bruce Schneier, chief security technology officer at telecoms firm BT. The real question is who is benefiting. "Cyber war is a big industry and there is a lot of money available in the US for contracts. Playing on people's fears is very effective."

Expert hackers disagree. They say it would be fairly straight-forward to launch a serious cyber attack. Speaking at the CCDCOE's Conference on Cyber-Conflict, Charlie Miller, a former analyst at the National Security Agency, outlined how, if he were hired by Kim Jong-il, he would build a cyber-force to attack the US. He estimates it could be done in two years, with a staff of 600 computer specialists. It would cost about $50m (€39m) – a bargain, considering US defence spending totalled $696.3bn in 2008. "From the technical side there is nothing that would stop me hiring people and training them to get into sensitive systems. We could get in anywhere we wanted. I don't need tanks or bombs, just people," said Miller.

It would be hard for his cyber-army to target US military networks, which are "air-gapped" and not connected to the internet. But in comparison, Wall Street is wide open. A successful attack on banks would cause a financial collapse and trigger a run on the dollar. There would be a backlash against the government. Shops would run out of food. There would be riots on the streets. Something similar has already happened in Tallinn. New York, London or any western capital could well be next. — (M)