





-11	DANGER OF THE RES	10 1000 000	manufacture Co.			
	unix 3		STREAM	CONNECTED	2775	
	unix 3		STREAM	CONNECTED	5158	/var/run/db
	bus_socket					
	unix 3		STREAM	CONNECTED	5157	
	unix 3		STREAM	CONNECTED	5152	
	unix 3		STREAM	CONNECTED	5151	
	unix 2		DGRAM	CONNECTED	5149	
	unix 3		STREAM	CONNECTED	5127	/var/run/db
	bus_socket	Calculation 2	COURSE		1222	
	unix 3	[]	STREAM	CONNECTED	2756	
	unix 3		STREAM	CONNECTED	5113	/var/run/db
	bus_socket					
	unix 3		STREAM	CONNECTED	5112	
	unix 3		STREAM	CONNECTED	5083	
	bus_socket					
	unix 3	[]	STREAM	CONNECTED	5162	
	unix 3		STREAM	CONNECTED	5162	
	unix 3		STREAM	CONNECTED	5162	
	unix 3		DGRAM	CONNECTED	5162	
	unix 3		STREAM	CONNECTED	27P5	/var/run/db
	bus socket					
	unix 3	E3	STREAM	CONNECTED	5162	
	unix 3	ΕĪ	STREAM	CONNECTED	5158	/var/run/db
	bus_socket	75000				
	unix 3	ED	STREAM	CONNECTED	5157	
	unix 3	ED	STREAM	CONNECTED	5152	
	unix 3	Œ.J	STREAM	CONNECTED	5151	
	unix 2	[]	DGRAM	CONNECTED	5149	
	unix 3		STREAM	CONNECTED	5127	/var/run/db
	bus socket		SINEAH	COMMECTED	2221	, , , , , , , , , , , , , , , , , , , ,
	unix 3	EJ	STREAM	CONNECTED	5126	
	unix 3		STREAM	CONNECTED	5113	/var/run/db
	u111 7	-1	STREAM	CVIIILCILD	כעעט	, vai , i uii/ ub
	bus_socket					
	unix 3		STREAM	CONNECTED	5112	
	unix 3 bus_socket		STREAM	CONNECTED	5083	
	Pus_sucket					
	THE REAL PROPERTY.	ALCOHOLD IN COLUMN	CONTRACTOR OF STREET		THE REAL PROPERTY.	

TEEN AMERICA DIGITAL PATRIOTS

	- MEETING		ON THE REAL PROPERTY.		
bus_socket					
unix 3		STREAM	CONNECTED	5112	
unix 3	EI	STREAM	CONNECTED	5083	
bus socket					
unix 3		STREAM	CONNECTED	5162	
unix 3	E II	STREAM	CONNECTED	5162	
unix 3	E D	STREAM	CONNECTED	5162	
unix 3	EI	DGRAM	CONNECTED	5162	
unix 3	EI	STREAM	CONNECTED	5162	/var/rur
bus_socket					
unix 3	E J	STREAM	CONNECTED	5112	
bus socket					
unix 3	EI	STREAM	CONNECTED	5162	
unix 3		DGRAM	CONNECTED	5162	
unix 3	[]	STREAM	CONNECTED	5162	/var/rur
unix 3	EJ	STREAM	CONNECTED	5112	
bus socket					
unix 3		STREAM	CONNECTED	5162	
unix 3		STREAM	CONNECTED	5162	
unix 3		DGRAM	CONNECTED	5162	
unix 3		STREAM	CONNECTED	5162	/var/rur

_END OF LINE



In the cyber-war battlefield, they are the US miltary's secret weapon: average age 16.
Meet the West's new front line

bus_socket	J-RAFA	Martin State of	- 25	- KIRRY		
unix 3	DDs_sock	e TREAM	CONNECTED	5112		
unix 3	phix 3	STREMM	CONSVERETALLY	SONNECTED	5162	
bus_socket	unix 3		STREAM	CONNECTED	5158	/var/run/dbus/sy
unix 3	DDs_sock	e TREAM	CONNECTED	5162		
unix 3	pmix 3	STREMM	CONSVERETALLY	SOMMECTED	5157	
unix 3	pmix 3	MARTZ	CONSVIERETALLY	SOMMECTED	5152	
unix 3	pmix 3	DGREAM	CONSVERETALL	SOMMECTED	5151	
unix 3	pmix 2	MARTZ	CONNERANED	SONNECTEDan	/5-Julti7/d	bus/sv
	unix 3	EI	STREAM	CONNECTED	5127	/var/run/dbus/sy
bus_socket	bus_sock	et				
unix 3	pmix 3	MAGENTZ	CONNEREDATIO	SOMMECTED	275P	
unix 3	pmix 3	STREMAM	CONNERETALLY	SONNECTEDar	/shluhi/ d	bu/sv/agry/run/dbus/sy
bus_socket						
unix 3	DDs_sock	e TREAM	CONNECTED	5157		
unix 3	pmix 3	MARTE	CONSVERETALLY	SOMMECTED	5112	
unix 3	рвіх З	MAGENTZ	CONSVIERETALID	SOMNECTED	5083	
unix 2	DDs_sock	e DGRAM	CONNECTED	5149		
unix 3	pmix 3	STREDAM	CONSVERETALLY	SONNECTEDAN	/5-14-7/d	bus/sv
bus_socket	unix 3		STREAM	CONNECTED	5162	
unix 3	pmix 3	STREDAM	CONSMERETALLY	SPANECTED	5162	
unix 3	pmix 3	STREDAM	CONNERCAMED	SONNECTEDan	15-34-7 d	bus/sv
	unix 3		STREAM	CONNECTED	5162	/var/run/dbus/sy
bus_socket						
unix 3	DDs_sock	e TREAM	CONNECTED	5112		
unix 3	pmix 3	MARTZ	CONSVEREDAM)	SONDECTED	5162	
bus_socket	unix 3		STREAM	CONNECTED	5158	/var/run/dbus/sy
unix 3	DDs_sock		CONNECTED	5162		
unix 3	pmix 3	MARTZ	CONSVIERETALLY)	€D NMECTED	5157	
unix 3	pmix 3	MAEDATZ	CONSTEREMENT	€1 00 DECTED	5152	
unix 3	pmix 3	DGREAM	CONSMERETALLY	SOMMECTED	5151	
unix 3	pmix 2	MAGENTZ	CONNERANE D	SONNECTED at	/5-Julti7/d	bus/sy
	unix 3	[]	STREAM	CONNECTED	5127	/var/run/dbus/sy
bus_socket	bus_sock					
unix 3	pmix 3	STREDAM	CONSVEREDAM	SOUBECTED	2756	
unix 3	pmix 3	MAGATZ	CONSVEREDED	50BNECTEDar	/Srluhi/d	bus/an/run/dbus/sy

Airman First Class WILLIAM FLEURY,

us_socket unix nix 3 ppix mix 3 mix

Second Lieutenant MARK LUPFER are

unix 3 unix 3 unix 3 bus socket	DDix I	fight	ing for	their	digital lives.
unix 3	phix 3	3	_		
unix 3	phix 3	ZTREJAT	CONWERCHALD	SUBBECTED	5003
bus_socket	bus_soc	ket			
unix 3	рвіх З	MAGENTZ	CONSVEREDALID	SONNECTED	5165
unix 3	pmix 3	MAGERTZ	CONSVEREITALID	SONNECTED	
unix 3	pmix 3	MAGENTZ	CONSMERETALLY	SONNECTED	
unix 3	pmix 3	DGREADM	CONINERCAMED	SONNECTED	
unix 3	pmix 3	MAGDATZ	CONSTEREMENT	EDDBECTED.	ar/filen/dbu/sværy/run/dbus/sy
bus_socket					
unix 3		STREAM	CONNECTED	5112	
unix 3	IL≣ND OF	LIMREAM	CONNECTED	5083	
bus_socket					
unix 3	[]	STREAM	CONNECTED	2775	
unix 3	E3	STREAM	CONNECTED	5162	
unix 3	E3	STREAM	CONNECTED	2765	
unix 3		DGRAM	CONNECTED	2765	
unix 3		STREAM	CONNECTED	5162 /v	ar/run/dbus/sv

_END OF LINE

Wave after wave of attacks batter their network of five military servers running seven operating systems. As they stare at the screens of plain, grey laptops at makeshift tables covered with cables, Fleury, Akers, Lupfer and teammate Josiah Yamada form the online front line of America's war in cyberspace.

For all their crisp Air Force uniforms and regulation haircuts, these cyber warriors are a world away from their compatriots piloting jets and controlling drones in Afghanistan. Here, battles are fought with quick thinking and keystrokes, in a library-quiet hush under the flicker of fluorescent light.

During a rare break, with one eye on his screen, Akers vents his frustration: "It isn't like war when you can see the enemy," he says. "You're just sitting there waiting for them to attack." And attack they do. Unseen enemies swarm through their systems, searching for classified information and launching automated probes, OS exploits, DNS intrusions and packet sniffers that topple servers like dominos.

Finally, after hours of frantic coding, patching and hacking, the Air Force personnel and their fellow techies repel the last of the assaults. As the dust settles, they look like they could really do with a beer – but they'll have to wait a few years. Akers is 17 years old, Lupfer is 16 and Fleury is just 15.

In a conference centre at a golfing resort in Orlando, Florida, an IT room has been crossed with what looks like a reality TV show. In the foreground, bottles of warm Pepsi, boxes of Oreos and racks of humming servers. In the background, an audience of hungry-eyed Air Force brass and plump, prosperous defence contractors. In the middle, eight teams of teens competing to be the nation's foremost

underage digital-security specialists, or in the name of this annual Air Force competition: "CyberPatriots".

This final is the culmination of six months of qualifying exercises and online contests involving hundreds of teams and more than a thousand competitors from all over the United States. At stake are 40 fragile egos, five winners' medals, tens of thousands of dollars' worth of prizes – and just possibly the future of the free West.

The recent attacks on Google in China pale in comparison with the constant cyber warfare waged against the heart of the American state, day in, day out. The headlines speak for themselves: in 2009, the Pentagon spent \$100 million in six months to repair damage from a foreign government's digital intrusion; in 2005, Nasa was hacked and robbed of 20GB of Shuttle data; military networks are attacked "hundreds of millions" of times a day; Barack Obama's Twitter account was compromised. These are just

the facts fit for public consumption.

Alan Paller, director of research at the Sans Institute, a cyber-defence training organisation that sponsors Cyber Patriot, recalls the birth of the competition at a meeting

he attended at the Pentagon with the CIA, the National Security Agency (NSA), and the then cyber-security chief for the National Security Council, Melissa Hathaway. "She had access to all the classified stuff so her knowledge of how badly we were losing in cyberspace was very deep," Paller says. "She said America had to take this on like we did Sputnik, when the country looked up into that October sky and saw a light going: blink, blink, you're losing, you're losing, you're losing."

This so-called "dark war" is being fought by armies of hackers and sysadmins across the globe. "In a missile race, you get the world's brightest physicists to build something where any normal person can push the button," says James Lewis of the Centre for Strategic and International Studies (CSIS), a think-tank in Washington DC. "In cyberspace, you can't build a tool and expect it to work six months from now. It's the human element, the people with the skills who will do the hacking."

Jim Gosler, founder of the CIA's Clandestine Information Technology Office, is thinking along the same lines. "There's a big gap between the state-of-the-art in defence and the state-of-the-art in offence – offence has incredible inherent advantages. You have to have a world-class technical cadre to understand how the game is played."

So, last summer, the White House's Commission on Cybersecurity announced the US Cyber Challenge, a national talent search to find 10,000 young Americans capable of becoming "the top guns in cyber security".

But could America's newest secret weapon really be a gaggle of teenagers? All of the teams in CyberPatriot come from either Civil Air Patrol (CAP) or Junior Reserve Officers' Training Corps (JROTC) units attached to local high schools: think well-dressed, paramilitary Scouts with occasional access to heavy weaponry. "They may be only 16 years old, but they're ready now to operate in cyberspace," Paller says. "They might not be fully skilled, but they're ready."

At first glance, cadets Fleury, Akers, Lupfer and Yamada make unlikely top guns. By turns awkward and enthusiastic, the four teenagers from Torrance, California, seem



more like an enthusiastic chess club than fearsome cyber ninjas. But sit them in front a PC, Mac or Linux box and their skills shine through – complete with fighter-pilot nicknames for excursions into the digital danger zone.

Leadfoot (Lupfer) is the group's natural leader, radiating an intense, unshakeable confidence: "Cyber security is about protecting an entire country's defences in the digital world," he says. "Not only state-based attacks from other countries but kids in the garage having fun, seeing how far they can go and not even realising they have access to the country's biggest, deepest secrets."

He could almost be talking about Windows Smasher (Fleury), a ramrod-straight Air Force enthusiast with a background in coding on the darker side. "Hackers start as script kiddies," he says. "Then they learn code

and that changes everything - I speak from experience."

If there's a cool-headed member of this fast-talking team, it's Penguin Wrangler (Akers), a Linux expert who can pilot his way through open-source code as smoothly as Iceman from *Top Gun* handles an F-14. Despite this, there's little jet-jockey cockiness on show. "In the last round, we had three computers but they

weren't really talking to each other," says Akers. "This is different. We're on a network and we'll have active attacks. It's a whole new scale."

None of the three had any computer-security training before CyberPatriot, but the members of Civil Air Patrol Beach Cities Cadet Squadron 107 still came through three rounds of qualification with the highest score out of nearly 200 teams. Next year's competition will be open to all high schools, with potentially 600 entries. Today, though, at the Rosen Shingle Creek resort in Orlando, Team Torrance is seen as the one to beat.

Previous spread, left column: Fleury, Akers, Lupfer and Yamada. Above: the competition venue in Orlando

It won't be easy. A confident JROTC team from Clearwater. Utah, was just a handful of points behind Torrance in qualification. The Rome, New York, squad is being coached by a cyber-security expert from the Air Force's very own high-tech research laboratory. Overachievers abound: a local group from Spring Hill, Florida, has a member who has been building his own PCs since the age of seven, and the Portsmouth, New Hampshire, team reached the finals with just two contestants, compared to the other teams' usual five.

The CyberPatriot competition gives each team a network of five computers, running seven operating systems, to protect. Over an eight-hour period, they face increasingly aggressive attacks from automated systems and the Red Team. The Red Team is a group of official hackers who exploit weak points in the teams' defences and launch wider botnet intrusions. Every time a server goes down or the Red Team succeeds in disrupting services, the teams lose points. "They put in a lot of little things that you don't even realise until they sneak up on you," Lupfer says. "For instance, filling up your hard drive to the point your virtual machine just crashes. It's not something you look for. For us, it's going to be about applying our skills, keeping cool and staying motivated. If we do all those things, we'll pull ahead."

The same could be said of America itself. The country has some of the world's most innovative computer companies, an entrepreneurial spirit that churns out start-ups by the thousand, and a population that spends a large chunk of its time online. But when it comes to financing the fight against cyber warfare,

critics say the US has some catching up to do. "America is like the fattest kid in school challenging everyone to a race," says James Lewis of CSIS. "Why are we doing this? We depend more on the internet than any other country but people who think about security haven't thought very much about cyberspace."

Most experts put the total number of top-level, governmentemployed cyberwarriors in the US at around 1,000. Ex-CIA tech Jim Gosler told WIRED: "The US government and industry is inadequate to deal with the cyber-security threat. To give a back-ofthe-envelope number, we have probably only 1,000 people who are deep under the hood, who understand the subtleties and nuances of software at the 1 and 0 level. Within that first team, if the crisis is really hot, you have an even smaller number of people who are the go-to people, and it's never enough." America is not just short



contests, but there is one nation that probably has more child cyber warriors than the rest of the world combined. China began running its own cyber challenges over a decade ago, and now has up to 200





Opposite: the two-man Portsmouth team. This page: the eight teams' score cards; Team Torrance receive their trophies

contests testing as many 15,000 participants annually. The challenges usually pitch two teams against each other, defending and attacking simultaneously. Defensive exercises such as CyberPatriot are virtually unknown.

iDefense Labs in Virginia provides security intelligence to governments and businesses around the world. A senior researcher in its International Cyber Intelligence team agreed to speak about Chinese-state cyber warfare on condition of anonymity. iDefense believes the Chinese government was behind January's concerted attack on Google and 30 other US companies which was widely assumed to be not just an act of sophisticated industrial espionage but also an attempt to find the email and other details of state dissidents. The company estimates there are around 15,000 people working on information security tasks for the Chinese People's Liberation Army (PLA) or Ministry for State Security (MSS) at any one time – and that many are teenagers.

"The absolute minimum age would be 15 but that would be uncommon. You're usually looking at between 17 and 19," says the iDefense researcher. "They try to catch kids right at the end of high school and early university, before they start developing plans and ambitions that might make them less amenable to work with the PLA. The bigger challenges are at least as advanced as any at the major security conferences throughout the world and sometimes more so, especially for the winners."

The most famous graduate of China's cyber challenges is Wicked Rose, a secondary-school student who came first in a PLA hacking competition in 2005. The army per winners around the country and

arranged for him to compete with other winners around the country and undergo further training. A year later, with a small team and unofficial state funding at his disposal, Wicked Rose built rootkits to exploit weaknesses in Microsoft Office software and unleashed them on government targets in the US and Japan. His team was able to transfer tens of thousands – possibly even millions – of official documents back to China.

Wicked Rose is by no means the only successful Chinese hacker. Governments from India and Germany to Australia and New Zealand have reported attacks of a Chinese origin. Two years ago, MI5 warned over 300 British firms doing business with China that they were being actively targeted.

Chinese hackers enjoy both popular and official acclaim. "The young Chinese hacker is framed as very crafty and patriotic, constantly defending China's interests and using his mind in very innovative ways," says the iDefense staffer. "This image is very much supported and amplified in the state propaganda. For young people, it's fashionable to have intense negative sentiment against China's rivals or neighbours, and that is deeply tied to the hacking culture."

Hacking has even spilled out of the military into everyday life. The *China Daily* reports that independent, online hacking schools have become a £20 million industry, churning out tens of thousands of wannabe (although often only semi-skilled) hackers. Do cyber warriors Akers and Lupfer find themselves as popular at school as, say, the captain of the football team? They laugh. "My friends have no idea what I'm talking about," Akers says, "but they think it's cool that I get a free trip to Orlando to compete in a national competition. I bet there are a lot of teenagers who would like to do this but don't know about it."

They soon will. This is the second year of CyberPatriot and it is already twice as big as last year's. Next year, it will be three times as big again. A British version, called Cyber Security Challenge UK, is also scheduled to debut in 2011.

CyberPatriot uses CyberNEXS software developed by military simulation and engineering company SAIC. CyberNEXS offers realistic, live security threats in controlled Windows and Unix environments, with an automatic scoring process that rates each team on its ability to remove vulnerabilities, deal with incoming attacks and communicate with human judges. In the qualifying stages, the nationwide teams competed simultaneously online using virtual targets downloaded to school laptops. Here in Florida, the eight teams are using the very same hardware and software as SAIC's most sophisticated military and intelligence customers.

Rick Smith, principal cyber-security engineer at SAIC, is presiding over the Red Team as they ramp up their attacks. He points happily at a screen showing the status of each team's servers. Only a handful are running smoothly: most show warning exclamation-mark icons and many have the blinking red crosses that indicate



complete failure. "The attacks we use are ones you'd typically find on the internet. For instance, we planted back doors using open-source tools," he says. "Some teams have caught a lot of the back doors but some haven't. No one has done the patching yet. That's quite obvious because we pretty much got into all the teams."

At their table, Fleury and Akers are conferring intensely in front of a Dell notebook. Lupfer is trying to stay upbeat: "Some attacks have been pretty obvious – they're leaving messages on the server like 'Red Team was here'. We're having fun finding ways to work around them."

Around the room, not everyone is enjoying themselves. Several students are staring blankly at their screens with their heads in their hands, and there's an increasing air of urgency as servers stay down. First lieutenant Erika Boone (Twidget) of the Spring Hill, Florida, team admits, "It's difficult and it got really dif-

ficult, really fast." Over at the Air Force-coached New York team, 17-year-old Colonel Sean Bird is itching to let his cyber warriors loose on the Red Team. "We're not allowed to counterhack," he complains. "It would be a lot easier if we were."

Unfortunately for them, the Red Team can go about its nefarious business without fear of retaliation. CyberPatriot rules strictly forbid teams from hacking into the system, attempting social engineering or attacking their rivals. Dwayne Williams from the Center for Infrastructure Assurance and Security runs a similar defensive cyber challenge for American universities and sums up the attitude of organisers: "If you're Wal-Mart, you don't hire somebody to go attack Kmart. You hire somebody to protect Wal-Mart."

This sporting attitude helps to identify the ethically minded team players whom recruiters say they're looking for. However, not everyone believes that that approach reflects the rough and tumble of real-life cyber warfare. "People cannot do good defence unless they understand how the attacks work," says Alan Paller of Sans. "And they can't attack at all unless they know what they're attacking and how the defence works."

Although CyberPatriot has received the most publicity, the White House's Cyber Challenge also includes two other competitions. The

Department of Defense's DC3 contest is aimed at budding CSI techs, focusing on encryption, passwords, hidden data and other digital forensics issues. But the real hacker-on-hacker action is to be found in NetWars.

NetWars doesn't have corporate sponsors or a highprofile final in the sun; it's fought in a series of online "capture the flag" contests designed to be as realistic as possible. Unlike the clean-cut CyberPatriot cadets, Net-Warriors are positively encouraged to think dirty.

In an early round, a lone 17-year-old student from Connecticut, Michael Coppola, beat university-level teams by compromising the competition's own Twitter feed and awarding himself 10,000 points. Another contestant figured out how to put firewalls around high-value targets so that other contestants couldn't access them. In both cases, the judges allowed them to keep the points. "That's kind of what it's like in cyberspace," Lewis says. "There are no rules."

It's this lack of rules that promises to appeal to a wider audience of hacker fanboys, script kiddies – and even some CyberPatriot contestants. "NetWars, where you get to go offensive, sounds interesting," admits Fleury with a

smile, as he continues to fight off the Red Team. "It's something I might, just might, have experience of." Luckily, a few youthful indiscretions didn't disqualify him from entering CyberPatriot. In its rush to recruit and train thousands of cyber warriors, the US military establishment is flirting with a new type of "don't ask, don't tell" policy, this time relating to teenagers' black-hat backgrounds.

Barbara Endicott-Popovsky runs the Center for Information Assurance and Cybersecurity at the University of Washington, and helps to organise collegelevel cyber competitions. "The kids that are coming in these days are digital natives. They grew up with computers coming out of their fingernails," she says.

"Sometimes I don't want to know what they did when they were 12 years old. I don't ask. Some of them may have had their turn at playful activities, so to speak."

Paller uses the same euphemisms. "There are a million kids doing this stuff already, they've played around," he says. "We're trying to capture some and bring them over, offering advancement down our path rather than that path. Am I worried that we're training people who will then use those skills in ways that are not positive? Yes. We'll probably have some leakage backwards and some great skills getting used by the bad guys. But they've got lots of ways of learning those skills. It's the good guys that don't have the programmes."

For NetWars champ Michael Coppola, the competition was a way to focus his interests: "There are a few homemade war games and hacker-challenge websites, but they don't provide opportunities or open doors," he says. "Otherwise most would just target random servers and hack illegally. It was great that I came across NetWars."

NetWars might also represent the best job interview Coppola will ever have. At a recent Gov 2.0 summit, Jeffrey Sorenson, three-

DUS SONTE AMED LINE SONTE AMED STREAM CONNECTED 5158 /var/run/dbus/sv CONNECTEREAMED SECONNECTED STREAM CONNECTED CONNECTERAM SISTEMENTS CONNECTERAM SISTEMENTED CONNECTERAM SISTEMENTED CONNECTED CONNECTED SI49 5152 /var/run/dbus/sv bus_so是使是性 CONNECTED 5149 bus_so是使是性 CONNECTED 5149 connected 5149 unix 3 STREAN STREAN LAJAJZoz_zud Should America be unix 3 unix 3 searching for cyber warriors among cadets who polish buttons? unix 3 TREATE UNNECTED UNIX 3TREATE CONNECTED 5150 NNECTED UNIX 3TREATE CONNECTED 5150 NNECTED 51 5151 /var/run/dbus/sy BY LEAME TO CONNECTE BE A METS CONNECTED IN THE STATE OF THE STATE OF

BATTLE STATIONS

DIGITAL WARFARE'S KEY COMBATANTS

> UK

Cyber Security
Operations Centre
Location: GCHQ
Task: The operational
arm of the Cyber
Security Office was
set up in 2009 to
"actively monitor the
health of cyberspace".

> US

US Cyber Command Location: Fort Meade, Maryland Task: CYBERCOM, formed in 2009, collects the various cyber divisions of the military into one unit.

> Israel

Military Intelligence/ Computer Services Directorate, Israeli Defence Force Location: Mt Avital Task: It was confirmed in March that Israel was working to create a specialised "internet warfare" team.

> China

Third Department, General Staff Department Location: Beijing Task: A Pentagon report estimates that the Third Department has in excess of 130,000 staff. star general and deputy CIO of the US Army, kept an audience of politicians, soldiers and business leaders waiting while he attempted personally to recruit the young hacker into the army.

As all three of the CyberPatriot competitions end, the Red Team's status screen tells a mixed story: Spring Hill's network is a blizzard of red crosses whereas others – including those of Torrance, Clearwater and Rochester – look relatively healthy. Then time runs out, the Red Team relaxes and Akers, Lupfer, Fleury and Yamada get up from their chairs to stretch after eight hours hunched over their screens. Lupfer looks a little shaken. "It was pretty intense at the end," he says simply. "There were lots of surprising things."

While CyberPatriot's referee Jim Jaeger tallies up the eight teams' final scores, he reveals that the results are about far more than just the \$25,000 of college scholarships on offer. The winners of Cyber-Patriot will be packed off to intensive "cyber camps"

at universities in the summer to hone their skills, prepare for future study and (so the CyberPatriot organisers hope) smooth their recruitment into the United States' military, the NSA and FBI.

That's assuming the private sector doesn't get them first. Jaeger is also director of Cyber Systems at General Dynamics Advanced Information Systems and sees CyberPatriot as prime recruiting territory for defence contractors. "We view these competitors as future staff members," he says. "One of the things that CyberPatriot is doing is building a database so that we can track these kids from high school to college and into their careers, to ensure we're doing the right things to position them for the future."

America has always needed teenage troops. In battles from Normandy to Vietnam to Afghanistan, teenage soldiers have been given guns and told to follow orders. But times change. Cyber warfare is ubiquitous and continually evolving – just the kind of battles that today's digital natives are equipped to fight. In tomorrow's Dark Wars, teenagers will be given laptops and told to safeguard military secrets, critical infrastructure and billions in economic assets.

The question is whether America should be searching for its next generation of cyber warriors among cadet corps who enjoy polishing buttons and fantasising about F-16s, or in the wider hacking community. There are

some promising signs, particularly the aforementioned "don't ask, don't tell" policy regarding some teenagers' previous hacking experience and the NetWars competition, which builds on Def Con's "capture the flag" games. Huge scholarships, high-tech boot camps and proactive career guidance promise a bright future for students prepared to don a white hat. Ironically, America could do a lot worse than learn from its arch rival in cyberspace. China's cyber warfare may be black hat all the way down, but the state has undeniably succeeded in channelling and coopting its hacker community at a grass-roots level.

As for CyberPatriot, all of the eight teams managed to maintain at least 95 per cent availability of their networks in the face of persistent Red Team attacks. The Torrance team came third, just pipped to the post by the high-flying JROTC team from Clearwater and a dark-horse team of CAP cadets from North Carolina.

Windows Smasher, Penguin Wrangler and Leadfoot are disappointed but not devastated. "Before, I was like, Air Force pilot – yeah!" Akers says. "Now I'm actually starting to look at the cyber side."

One cyber-security top gun down - 9,999 to go.

Mark Harris is a technology writer based in Seattle

