Cyberterror: Public Enemy No. 1?

Ever since the film “War Games” in 1983, techno-doomsayers have added fuel to the fiery idea of a digitally driven Armageddon. The image is simple and seems almost irresistible. A genius in a dark room hacks away relentlessly for years, then one day gains control of nuclear missile launch computers. While it’s a terrifying prospect, is it at all realistic?

The fear of cyberterrorism stems from a belief that the complexity of technologically advanced countries leaves them open to sabotage from disaffected individuals and groups. Fifty years ago it would have been impossible, short of a nuclear attack, to destroy a significant chunk of a national economy in a matter of seconds. Given that modern society is so interconnected nowadays, an attack at one point of the technological or communications infrastructure – the computer systems that run Visa and MasterCard, say – is feared to have a disastrous knock-on effect.

Information itself has become the raw material of attacks via encrypted emails to coordinate terrorist operations and as a vehicle for selecting potential terrorist targets – Google’s street view application for major cities, for instance, provides the lay of the land for budding tourists and terrorists alike.

However, in terms of actual cyberterrorism, while there are certainly genuine security concerns associated with the internet, cyber warfare is still far more of an urban legend than a credible hazard.

According to various government agencies, massive disruptions are unlikely to happen anytime soon. Indeed, the statistical probability of global communications being brought down by a coordinated terrorist attack is on a par with that which would result from a giant asteroid crashing into Earth.

Despite this assessment, there is still an overwhelming sense of vulnerability, particularly in the West. The White House issued a report on cyber-security in May in which President Obama called cyber-security “one of the most serious economic and national security challenges we face as a nation”. Under the purview of the National Security Agency, the US is now looking at plans to build a digital warfare force for the future.

This mirrors a newcomer among Britain’s intelligence agencies, namely, the Cyber Security Operations Centre, which was established in June to beef up defences and coordinate “cyber-forensics” – tech-jargon and innuendo for monitoring and analysing the online activities of suspected terrorists.

But before accepting the demands of government agencies for new and increased powers to fight online threats and prepare for cyber warfare, we should look more closely at well-defined dangers and ask where existing legal norms fall short.

It is alarming that so many people are accepting the assertions about cyber security as a key global problem without demanding further evidence – especially in the light of the WMD debacle in the run-up to the war on Iraq. Just as that ongoing conflict suffered from poor – or at best unheeded – intelligence reports, these claims of rising cyberthreats could lead to policies with long-term and deeply troubling consequences for network openness and personal privacy.

To be sure, there is a case to be made for a formal, organised authority – ideally with a UN mandate – to deal with the ever more critical area of online security. But while there is a barrage of attacks, ranging in scale from trying to gain access to classified corporate memos to the constant cyber-siege of the US Pentagon, there is little to no evidence to suggest that access to the latter is likely or even possible. Moreover, there is already plenty of petty cyber-crime, some of it involving stolen credit card numbers. However, much of it stems from low cyber-security awareness by customers, rather than from large-scale hostile attacks of banks or credit card companies.

In other words, vigilance is vital, but blind acceptance of speculative assertions is not. A battle against cyberterrorism actually poses significant threats to civil liberties.

Imagine, for instance, a country where hackers are classified as terrorists and sentenced to life in prison for their techno-exploits. Immigrants suspected of "terrorist activities" (such as defacing a website or even twittering about a Palestinian state) are detained by law enforcement officials. Even worse: all your communications could lawfully be intercepted by any government. That means – as an Arab-American, say – your private emails from relatives in the Middle East could be read and handed to the police if they seemed suspicious. These are just a few ways civil liberties could get butchered in the long war against terrorism.

The threat of cyberterrorism from disaffected elements in the Third World is hypothetical and owes more to Hollywood fantasies than to reality. With the massive imbalance in power between the West and the Third World, the notion that rogue individuals and groups pose a threat to the technological infrastructure is absurd. However, the willingness of the West to unleash destructive force remains a harsh reality.

***

Arab online activity

The guns may have fallen silent in the uneasy ceasefire between Hamas and Israel, but the battle for hearts and minds is still being waged in cyberspace. In fact, the clear victors in the latest instalment in the Arab-Israeli conflict are neither the terrorists or freedom fighters – depending on your point of view – nor the tanks and phosphorous missiles sent to obliterate them. Whatever the ultimate political outcome of Israel's war on Gaza, the uncontested master of the field has been web 2.0 – the umbrella term encompassing blogs and such interactive websites as Facebook, YouTube and Flickr.

Wars may be tragic, but they can be the making of media channels, both old and new. For instance, in 2001, al-Jazeera's coverage of the war in Afghanistan elevated it to the status of a major league network television station that had to be taken serious. As the bombs fell on Afghanistan, al-Jazeera was the only channel with a live link to Taliban-controlled Kabul. Overnight, a sizeable proportion of the world's population was glued to an Arabic-language satellite channel that most people outside the Middle East had never heard of, transmitting from Doha – a place that even fewer had heard of. The station's logo is now a recognized feature on TV screens across the world.

The war on Gaza has been a similar boon for online activity in the Arab region. Given that Israel barred all journalists from entering Gaza, the media and public were compelled to rely on non-traditional sources for information about the crisis. For instance, the number of individual hits to the online Palestinian magazine Electronic Intifada – whose contributions come from a wide range of unofficial reporters, humanitarian workers and activists – soared by some 300 per cent over the course of the three-week conflict.

The spike in Arab online activity comes against the backdrop of already significant growth in internet and computer use. According to Internet World Stats, there were almost 42 million internet users in the Middle East by the end of 2008, translating into an impressive growth rate of 1,177 per cent over the period 2000-2008. By contrast, over the same period the number of internet users in the United States and Europe grew by 131 and 210 per cent, respectively, albeit starting from significantly higher penetration rates. Currently, the highest penetration rate in the Arab region is in the United Arab Emirates, where almost half the population of 4.6 million regularly use the internet.

Much of this growth in the region stems from blogging and social networking sites – the emerging hallmark of web 2.0 – which is helping to unite and give voice to a fragmented silent majority. With the advent of web 2.0, the new paradigm of media is not to define the zeitgeist, rather to flow from it through self-created content. While the old internet was all about access and creating flashy web applications, web 2.0 is about letting users run wild with personal blogs, podcasts and amateur videos.

For instance, during the 22-day carnage in Gaza, support groups sprouted up on Facebook, including “Stop Genocide in Palestine”, which drew in more than 118,000 members. Meanwhile, in Second Life (SL) – the internet-based cyberworld – online avatars showed up in SL Israel with their virtual banners to voice their support for Hamas and the Palestinians. People used Twitter updates to tell the world what they were witnessing on the ground and how they felt about the war. And several videos of the bloodshed in Gaza notched up more than 250,000 views.

Of course, it’s not only about war and politics. Several home-grown social networking sites have sprung up in the past few years to cater to a variety of niches, ranging from the general interest, Arabfriendz, to the Middle East’s answer to LinkedIn: Snap (Social Network for Arab Professionals). Even the enduring popularity of Second Life has spawned Muxlim Pal – the latest virtual world offering with a Muslim twist (see box).

But this newfound freedom of expression comes at a price, particularly in more conservative countries. Some governments in the Arab region are doing their best to hobble web 2.0 precisely because it allows people to vent their anger and frustrations, which is as likely to focus on repressive Arab rulers as it is on Israeli occupiers. For example, Syrian authorities temporarily blocked Facebook in 2008 when the website played host to a debate on the president, Bashar al-Assad; and in a separate incident, some 20 dissidents were arrested for creating an online opposition front to the ruling Baath Party.

Censorship remains endemic across the Middle East, as highlighted by the international advocacy group, Reporters Without Borders, in its 2008 survey. Among Arab states, only Kuwait and Lebanon were not in the category of “under surveillance”, which lists countries that occasionally ban websites and block content. More damningly, five of the world’s top 13

Internet-censoring regimes were in the Arab region, with Syria and Saudi Arabia at joint pole position as the most “hostile” in terms of routinely stifling internet freedom.

To be sure, as users increasingly make themselves heard, the ensuing bedlam will not be to everyone’s liking. However, blocking the internet is not only anathema to the very raison d'être of the web, but also unachievable in practice. Web 2.0 cannot be nailed down easily because of the host of channels that are now at the disposal of users and that can be employed to circumvent the censors. A single media story – say a politically-sensitive blog or video footage – can be emailed to friends, added to a YouTube favourite, posted on Facebook, dugg through a Digg account or commented on in Twitter. Whether online or off – as in the blockade of Gaza – borders will always be too porous to restrict the flow of information.

***

Cellular Evolution

Wireless phone standards have a life of their own. You can tell, because they’re spoken of reverently in terms of generations. There’s great-granddad whose pioneering story pre-dates cellular and who brought into being grandma and grandpa GSM, the 2G technology. Then there’s mum and dad digital cellular, 3G wireless, who are beginning to make a place for themselves in the world. And finally, in the current wireless scrapbook, there’s new baby on the horizon, 4G.

According to the market research firm, Juniper Research, the wireless subscriber base in the Gulf region is set to grow at an average annual rate of 10.5 per cent between 2008 and 2013. Moreover, Saudi Arabia ranked tenth in the world in terms of 3G subscription base, at 3.1 million in 2007, and 3G penetration rates are projected to exceed 50 per cent by 2011. The United Arab Emirates is expected to reach that milestone a year sooner, in 2010. This growth is driven primarily by “greater network capacity and download speeds allied to consumer interest in mobile rich-media services and mobile Internet,” says Windsor Holden, principal analyst with Juniper Research and the author of the report.

It’s all part of a continuing lurch towards ever more developed cellular wonders – bristling with cameras, games and Internet access – that are not just for talking anymore. According to another survey by ABI Research, the market for smart phones, such as the iPhone and BlackBerry, which offer e-mail and Web access, will grow from the current rate of 10 per cent of the cell market to 31 per cent by 2013.

Indeed, the iPhone, the cell phone/media player from Apple, has been largely credited with making consumers more eager for third-generation cell phone networks. The 3G model was released in 24 countries on 11 July 2008, with launches planned in 49 others, including a regional debut in Qatar in the last quarter of 2008. With enough bells and whistles to outfit a marching band, the iPhone encourages people to think of using their devices for data and is – almost single-handedly – winning over mainstream consciousness to perceive 3G as the ultimate experience.

To be sure, as wireless phone companies in the Gulf accelerate their rollout of 3G phones and services, consumers are confronted with a dizzying array of promotional effluvium. Choosing a cell phone used to be easy. You simply had to calculate which was the better value. But these

days, you're not shopping for a phone; you're shopping for a company that advertises the spiffiest phones, with ample screens to fill with high-resolution movie clips and graphics.

Now that the quest to replace a business traveller's laptop with a cell phone or hand-held device is quickly becoming a reality, wireless carriers are knocking themselves out to lure customers with ever more exclusive features. Indeed, for a business traveller, the most exciting aspect of 3G phones is already available, namely, networks that are fast enough for them to do demos or access corporate applications and databases.

To some analysts, the marketing cart is finally in step with the technological horse to spell the end of 2G. Buy into 3G now, they say, or get left behind. But others are less sanguine, pointing to the fact that, despite the hundreds of billions of dollars invested in 3G since the turn of the century, it is only now beginning to attract widespread use. Essentially, it has taken a long time for 3G handsets to get to the point of competing with 2G-type phones, which can be attributed to issues of scale and volume. It takes time to deploy new consumer technologies, and someone ultimately has to pay the higher price for devices. The reality is, even after a standard has been accepted for a wireless network, it's at least five or six years before anyone starts using it on a commercial basis.

But it's 4G, the next generation, that's already in the sights of many in the industry. 4G holds the promise of routinely delivering the higher end of 3G transmission rates, and much faster in some cases, up to 100 Mbps for downloading and 50 Mbps for uploading. At this nascent stage, the main 4G issues relate to the wireless standards that should be used and the cost to network operators and, ultimately, to customers.

In addition to these teething problems, the downturn in the global economy could equally prove a deterrent in the push to create 4G phones. This is why some of the leading companies such as Ericsson, Motorola, Lucent, Nortel and Qualcomm are working on "3G-plus" concepts that push performance using 3G standards – replicating, in essence, the interim 2.5G that extends 2G systems.

However, once 4G lifts off – and analysts tend to disagree only on the timing – the main application that will propel fourth-generation wireless in terms of consumer usage is expected to be social networking. With faster upload speeds, shooting a video with your camcorder phone and uploading to a social networking site will become a breeze.

More to the point, your cell phone will be your wallet, and your ticket broker, your bank, your shopping buddy and much more besides. For example, new technology will allow you to snap a picture of someone wearing an outfit you want and will automatically search the Web to find the designer and the nearest shops in your city that carry that outfit. You can then see what that outfit looks like on your personal avatar – a 3-D representation of you – right on your phone, and ask your friends in different locations to check it out online and give their opinion. Your 4G phone will also guide you when visiting a city, automatically providing you with local entertainment options, activities and dining options that match your preferences, and then make reservations and purchase tickets for you – like a private secretary.

Hardly surprisingly, engineering gurus are already hard at work on the newborn's eventual offspring: 5G, 6G and beyond, when technology is set to become even more space age. The next generation – human generation, that is – could well witness micro-sized, voice-activated

cell phones that can even be implanted into people's bodies. By then, even cell phone batteries could become a thing of the past as power will be drawn instead from the human body itself.

***

Spying on the Kids

For every parent who ever told their children that they had eyes in the back of their heads, modern technology can now do one better. In a move that is more reminiscent of location-tracking devices in such sci-fi films as The Matrix or Total Recall, wireless companies in the West have begun to roll out a service that uses GPS tracking into something children carry voluntarily: cell phones. Using a phone's inbuilt GPS, parents can now tell every time their children skipped school or visited someone they shouldn't have.

After securing a foothold in the teenage market, wireless companies are now setting their sights on the so-called tween market, eight to 12-year-olds, to drive consumer growth. With competition in the wireless market as cut-throat as ever, many industry analysts see this younger segment as the next big sales opportunity. This comes as the adult market nears saturation levels, with the global subscription base by the end of 2007 estimated at 1.68 billion by Fitch Ratings, which represents a year on year growth of 17.6 per cent. In the Gulf region, in particular, the estimated penetration rate of 130 per cent – amounting to more cell phones than people – can be largely attributed to increases in disposable income; improvements in infrastructure, bandwidth and cost; and convenience of use stemming from next-generation phones. Within that context, the UAE's Etisalat and Kuwait's Zain registered the highest numbers of subscribers at 63 million and 42.4 million, respectively.

In the US, which was the first country to see the lucrative potential of first the teen and now the tween segments, the growth of young subscribers is set to overtake that of the overall American population in the next two or three years. According to a survey by the technology consulting firm, Jupiter Research, this growth has been fuelled by parental concerns over safety, particularly in the wake of terrorist attacks and shootings in the country's high schools.

Specifically, the ability for children to reach their parents in an emergency is driving both young teen and tween sales. Jupiter Research estimates that some 9.2 million out of the 20 million American children in the 8-12-year-old bracket had cell phones by the end of 2007. By 2010, there could be as many as 12 million preteen cell phone users. Moreover, the number of eight-year-olds with phones more than doubled to 600,000 from 2003, while the number of mobile-touting nine-year-olds jumped to 1.5 million from 500,000.

Indeed, the latest tracking services such as Verizon Wireless's Chaperone and Sprint's Family Locator are all part of the marketing mix aimed at convincing parents to buy into the tween vision. And from the perspective of the average preteen, demand is being expanded with special, tailor-made phones for children. For example, the bright blue Firefly Mobile, which was introduced in 2005, features only five keys, with child-friendly icons for speed-dialling a parent.

In the Arab region, the teen and tween subscription base is also on the rise. However, the increase owes more to demographics rather than concerns over child safety in schools and on the streets. Given that 55 per cent to 65 per cent of the total population is aged under 30 years,

wireless companies in the Gulf region have been quick to roll out plans for younger customers, particularly university students. And while there isn't the same focus on tailor-made phones for children – which makes it difficult to pick out figures for younger subscribers from the adult base – here too the incursion of cell phones into tween society has ratcheted up the electronics race, with mobile phones joining laptops, digital cameras and iPods on children's wish lists.

Children want cell phones for reasons obvious to them: they look cool and make them feel grown-up. They convey a certain status and allow them to stay in near-constant touch with friends (and parents).

Of course, there are very different considerations for parents. The decision of when or indeed whether to buy children cell phones is often emotionally charged and value-laden, which raises thorny questions about safety, maturity and materialism.

While for some parents, cell phones can be an electronic security blanket for both parent and child, for others the practical use of cell phones for young children who are rarely without adult supervision is at best marginal; and the cell phones for the tots can soon be forgotten and lost among the tangle of toys.

To be sure, the novelty and razzle-dazzle of cell phones wear off, and they are often put out of young minds in the way of other, once-coveted electronic games and toys. And besides, young children, who can barely be convinced to say a few words to granddad over the phone, have few peers with phones to call.

Moreover, while mobile communications for youngsters is gaining wider acceptance, safety and security has a different meaning for a parent, depending on the age of the child. For older teenagers, the catalyst can be leaving home for the first time to go to university; for younger children, it's the convenience of a parent being able to keep tabs on the child.

For that reason, the tracking services that are widely available in the US, Europe and the Far East are proving ever more popular with parents. Of course, not all trackers phone home. For instance, OurKids, which was launched by Blue Tree Service in the UK last year, is a basic GPS locator with an alarm button that slips in neatly in a child's backpack.

But the purpose is the same whether they're fully-fledged cell phones or simple black boxes. To pinpoint the device, you call up a dedicated website, enter a password, click "locate" and an icon appears on a map – either a street map or actual satellite photo. In the US, you can zoom in enough on photo view to see individual buildings. These are existing satellite photos – a truant child won't actually be standing there – but this feature is cutting edge if altogether creepy.

Many experts believe such tracking devices will soon become as mainstream as cell phones themselves. However, it's important to raise the moral implications of this technological advance. In essence, these companies are selling the parents a spying tool. And playing Big Brother for a bit of peace of mind – or rather, Big Mum or Dad – could ultimately prove more damaging than useful.

Keeping too close an eye on kids undermines the trust and, more often, backfires. After all, remember what always happens in the sci-fi films when the hero discovers the tracking device. Whether it's Arnold Schwarzenegger extracting the tracker from his nose in Total Recall, or the

arachnid bot being sucked out of Keanu Reeves's navel in The Matrix, it's the people who are responsible for planting the trackers who always get their comeuppance.

***

The Slow Road to Speedy Access

The key to happiness in the Internet age is bandwidth. Bandwidth, bandwidth, bandwidth. Fat pipes, capable of sucking down Web pages, music files, video clips, e-mail and other forms of digital information and entertainment from the Internet in the blink of an eye. A data spigot that is always open, without busy signals and without the kinds of delays and service interruptions that drive most computer users mad.

Bandwidth - a measure of the flow of information, in bits, that moves over a given distance in a period of time - is the most important factor in the development of new types of services on the Internet, more so than increases in personal computer processing power or new types of Internet communications devices.

Until recently, high-bandwidth connections to the Internet were available mainly to businesses and certain lucky people willing and able to pay hundreds or even thousands of dollars a month for so-called broadband Internet access. But with the development of cable modems, digital subscriber line (DSL) modems and satellite data services, the trend is set for access to high-speed, broadband data services.

In the West, the merger of America Online and Time Warner has raised hopes that cheap, high-speed Internet access may soon be available everywhere - at least in the United States. In the Middle East, the future of so-called broadband access is looking more complicated.

Almost 3 million people in the United States already have high-speed Internet access via cable systems or DSL, and American companies of all stripes are jumping into this market. But analysts in the Middle East say the spread of broadband has lagged in most Arab countries because of slow deregulation of the old state telecommunications systems, competing technologies and regional differences in infrastructure.

"You have to bear in mind that it is a fragmented picture here," says Michel Kilsey, IT consultant and general manager of Internet Facilities. "But it is fair to say that the Middle East is up to two years behind."

One big reason for the gap, according to analysts, is limited competition in the telecommunications markets of many countries.

DSL, which is catching on quickly as a means of high-speed access in the United States, runs over the same copper telephone wire that carries voice calls from a central office into each house or apartment. But in most Arab countries, this local phone infrastructure, known as the "local loop," is owned and controlled entirely by the giant phone companies that still have a monopoly on national phone service, like Lebanon's Ministry of Post and Telecommunications (MPT) and the UAE's Etissalat.

Legislation which "unbundled" this control and gave competing telecom providers access to the local loop in the United States, has not spread across the Middle East, but regulators say they are looking closely at this issue.

"The next phase is to look at the unbundling of the local loop," says Degaulle Azar, deputy general manager and Internet analyst with Bond Communications. "We need to produce a set of recommendations designed to increase competition and reduce prices. But each country will have to apply those recommendations on its own."

Jehan Abuzeinah, Channel Sales Executive for the networking giant, 3com, believes that without access to local phone lines, "new service providers and next-generation telephone companies haven't had the opportunity to roll out DSL services themselves."

As a result, telecommunications companies across the Middle East are taking their time rolling out serious DSL services, or setting high prices for them. The companies are not interested in undermining profits from metered local calls for dialup access, leased lines for businesses and ISDN service, an older technology that is similar to DSL but not as fast.

"Many telephone companies in the region are quite carefully protecting their revenue stream of very profitable ISDN or leased line services," says Kilsey. "Why should they kill the golden goose?"

ISDN may also be slowing the adoption of high-speed services. While it proved unpopular in the United States, ISDN has been very popular in Europe and, to a lesser degree, in the Middle East. In Lebanon, for example, Data Management has just launched an ISDN service to corporate users touting it as the latest in broadband. While in the UAE, 25 percent of households have ISDN lines. "ISDN is a pretty good intermediate technology providing increased capacity," says Azar, and may be discouraging residential users from adopting higher-bandwidth technology like DSL.

Analysts say the phone companies' lack of interest in shaking up the access business leaves an opening for cable. Cable does have the early lead across the Middle East, although it is not expected to last. According to some estimates, as much as 80 percent of broadband access connect to the Internet using cable modems. But strong regional differences across the region mean that competition from cable companies will thrive in some places and languish in others.

"People tend to see the Arab world as a whole, when you really have large differences within the countries and regions," says Azar.

Perhaps 65 percent of Lebanese households are passed by cable, meaning they could sign up for cable services if they chose to. But that number masks a more complicated picture. In the UAE and Bahrain, for example, more than 95 percent of households are passed by cable, while in Syria almost none are.

For now, the phone companies' hold on the telephone infrastructure is good for cable, believes Kilsey. "The grip that they have on the consumer plays to the advantage of cable operators," he says. There are some 500 cable operators in Lebanon - mostly illegal - charging an average of $45 a month for unlimited access, compared with $20 plus phone bills running at $1.4/hour of typical dialup. Unlike other Internet service providers, cable providers are not dependent on phone companies for access to consumers. And until the phone companies start getting serious

about offering broadband service to residential customers, cable access providers will have one leg up.

But in the Middle East, no one is putting all of their bets on cable. Where and when it is appropriate, companies will provide broadband service using any available technology. "Our content model is platform-agnostic and can be delivered over DSL and other platforms as they emerge," says 3com's Abuzeinah.

In the coming years, Arab businesses may be offered the luxury of using not just one broadband connection but three: a cable modem, a DSL modem and a satellite modem. "It'll be a test period," believes Kilsey. "Companies will be testing the connections to see which one to keep, a decision that sooner or later a lot of Net surfers are going to make."

Despite cable's theoretical speed advantage, the actual performances of cable and DSL are comparable. Therefore, the determinants come down to price and, to a lesser extent, to security, the choice of ISP and reliability.

Satellite rates are typically of the order of $600 that go towards installation and the cost of a dish, and a monthly fee that is a function of the amount of information to be downloaded - $110 for 230MB, $2,600 for 10GB. Connection speeds via satellite top out at about 512 Kbps. "There is a strong client base of customers who are more interested in quality and speed than in the price of a service," says Azar.

Sam Lutfallah, general manager of Inconet, agrees. Since the launch of its satellite service last year, the ISP has attracted 30 customers ranging from small businesses to hospitals and universities. "Speed is the new buzzword in the Middle East - the fastest bird catches the information worm."

Satellite systems have a drawback, though, that's down to the speed of light. For geostationary earth orbit satellites - those in orbits that keep them stationary relative to the Earth's surface - one of the major issues is the latency inherent in a signal transport path that's 22,300 miles long in each direction. That translates into a time lag of one-quarter of a second for the round trip itself, plus framing, queuing, and switching delays that can increase the latency to half a second or more - far too long a delay to allow effective use of interactive real-time applications. And there isn't much that can be done about the propagation speed of electromagnetic transmissions.

In Lebanon, though, the most important disadvantage to satellite systems is that they are asymmetric - that is, given the monopoly of the Ministry of Post and Telecommunications on outgoing traffic, you can download directly off cyberspace, but you have to go through a Lebanese ISP to upload. This turns into a key selling point for cable or a future DSL as these technologies lets users stay constantly connected to the Internet without tying up a phone line.

In the final analysis, high-speed Internet, in all its varieties, is almost upon us. When broadband access finally spreads across the Middle East, files will be downloaded in a snap, Web pages will pop onto screens, and no-one will think twice about downloading video clips or MP3 music files. Multiplayer network games and home videoconferences will suddenly become practical. But the thing that's set to change everything is the fact that the Internet will always be on, whenever users want it. At that stage, the biggest nightmare will be to wake up someday and have to connect to the Internet using - the horror of horrors - an old-fashioned dialup 56K modem on a dialup telephone line.

***