Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 10
15 Φλεβάρη 2006

A Plug for the Unplugged $100 Laptop Computer for Developing Nations
New York Times (02/09/06) P. C3; R. Hal

MIT Media Laboratory founder N. Negroponte announced that Quanta Computer will manufacture the $100 laptop using a Linux operating system and an AMD chip during the technology sessions at Davos, Switzerland. The device will have a carrying handle, a spill-resistant keyboard, and a power-generating hand crank, as well as the ability to connect to a wireless network and a screen that is readable in direct sunlight. Negroponte said that network costs would be defrayed by managing the flow of Internet data so as not to compete with commercial data. Microsoft CTO C. Mundie argues that a device similar to a cell phone would make more sense than a laptop, given that the wireless communications industry is growing steadily in developing countries. While Mundie and other critics have focused on the business value of cell phones, Negroponte stresses that laptops yield the strongest educational benefit. Cheap laptops have business value, too, as they could be used as cash registers for merchants, for example, or even as a sort of ATM if it was networked. Laptops could also record and store legal documents such as contracts, a fundamental element of all modern economies. Should the economies of developing nations become dependent on the laptop, it would also have the added benefit of encouraging literacy.

Locking Down Our Digital Future
BBC News (02/08/06), M. Geist

A meeting in Rome last week sponsored jointly by the Italian government and the OECD saw hundreds of representatives from the business, academic, and policy communities converge to discuss the state of the digital economy. Opposing sides voiced the argument for digital rights management (DRM) applications to secure content, while others highlighted the rich body of works that has come from systems that support user-generated content, such as Flickr and Creative Commons. Advocates of the user-generated DRM alternative also focused on the proliferation of blogs, with Technorati CEO D. Sifry noting that 75,000 new blogs are created each day. Of the 27 million blogs that his company follows, Sifry reported that there were more written in Japanese last month than there were in English. DRM supporters noted the difficulty that users now encounter when trying to legally transfer content between devices. The popularity of Napster, for example, has suffered because the system is incompatible with Apple's iPod. Rather than questioning the licensing restrictions, DRM proponents have blamed equipment makers for the incompatibilities, arguing that they should incorporate content neutrality into their next generation of devices. Meanwhile, user-generated content faces an emerging threat from a two-tiered Internet that could restrict access to applications such as BitTorrent, a program frequently used to distribute material such as open source code and independent films. If service providers follow through on their threat to charge Web sites for bringing content to their users, the two-tiered Internet could further undermine the availability of user-generated content, as many smaller sites would be unable to pay the fees.

US Plans Massive Data Sweep
Christian Science Monitor (02/09/06) P. 1; M. Clayton

The U.S. government is working to harvest and link information from such disparate sources as email and blogs to government records and intelligence data in a large computer system built to monitor for terrorist activity. While the government credits the parts of the system that are already operational with having prevented some terrorist attacks, privacy advocates warn against the latest government intrusion into daily life. In describing the care-free attitude with which most people make search and purchase decisions on the Internet, the Electronic Frontier Foundation's L. Tien says, "We have an attitude that no one will connect all those dots. But these programs are about connecting those dots--analyzing and aggregating them--in a way that we haven't thought about." At the center of the initiative is a seldom-discussed three-year-old Homeland Security project known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement). ADVISE relies heavily on data mining, an established practice that the government is applying on an unprecedented scale, mining the digital galaxy for information that is then cross-referenced with government records to be stored in files known as entities. The program demands storage for roughly 1 quadrillion entities as it aims not just to compile information, but to establish patterns that can give insight into terrorists' plans and motivations. The Starlight visualization component of the ADVISE program is already operational, helping analysts see graphical patterns in data that can elude numerical analysis. Privacy advocates are most alarmed by the secrecy of the program, however, as even legislators who oversee the DHS have only vague knowledge about the program, though the department has made assurances that privacy concerns were considered in the program's design.

Broadband Law Rewrite Planned for 2006
CNet (02/08/06), A. Broache

House Energy and Commerce Committee Chairman J. Barton (R-Texas) said his committee hopes to present a "comprehensive" plan for re-tooling U.S. telecommunications statutes later this month during a speech at an annual "state of the Net" conference on Wednesday. Both House and Senate lawmakers have been debating revisions to the 1996 Telecommunications Act, which has been targeted by critics for its failure to accommodate the rapid growth of the Internet and broadband. Sens. J. Ensign (R-Nev.) and J. DeMint (R-S.C.) have each introduced proposals that subscribe to a policy of nonintervention when it comes to broadband, while the Senate Commerce Committee has started a series of hearings that should lead to another reform bill. Barton expressed impatience for the Senate to act, noting that "We don't have that many legislative days this year, so it is time to stop talking, and it is time to start working." Last fall, Barton's committee issued a draft proposal and held a hearing that outlined rules for technology services assigned to the categories of broadband ISPs, VoIP providers, and broadband video providers. The draft was heavily criticized by technology companies such as Amazon and Google for failing to clarify a mandate for network neutrality. Barton made no mention of how that draft would be amended prior to its formal unveiling in the House, but stated his intentions to "very quickly" put out legislation for public review. He added that "it's pretty tough to determine what is right in my mind" as far as network neutrality was concerned.

Academics Warn of 'Significant Threat' of Spyware Epidemic
SC Magazine (02/07/06), W. Eazel

University of Washington computer science professor H. Levy calls spyware the top download for unsuspecting Web surfers. Levy is the co-author of a new study that found that more than one in 20 executable files contained piggyback spyware, and that one in 62 Web addresses engaged in drive-by attacks or forced spyware on those who visited a Web site. The UW research team, which also included associate professor S. Gribble and graduate students A. Moshchuk and T. Bragin, examined more than 20 million Internet addresses for the study. "We wanted to look at it from an Internet-wide perspective--what proportion of Web sites out there are trying to infect people?," says Levy. "If our numbers are even close to representative for Web areas frequented by users, then the spyware threat is extensive," says Levy. The researchers found game and celebrity Web sites to be the greatest risk for piggyback spyware, and pirate software sites to represent the foremost threat for a drive-by attack. Although most piggyback spyware was adware, about 14% was malicious, the kind of programs that steal passwords and financial information or even disable computers.

States' Challenge: E-Voting Interoperability
Governing.com (02/09/06), Z. Patton

A lack of federal funding and guidance is hindering many states from setting up voter registration databases, according to D. Markowitz, secretary of state for Vermont. His comments came during a panel discussion hosted by the Brookings Institution and the American Enterprise Institute. The Help America Vote Act (HAVA) of 2002 is a $4 billion mandate that requires states to update voting systems and establish statewide databases of registered voters, but it did not receive funding until a year later and still needs more than another $1 billion to be fully funded. Markowitz added that the states that have implemented new voting systems and voter registration databases have done so without specific direction from the federal government. "In all states, we've had to take some gambles," said Markowitz. Even with a revised January 2006 deadline, about half of the states still have not established voter registration databases. And questions remain over whether the federal government will attempt to fully fund HAVA and provide technical guidance for states. There are also concerns about the need to make the systems interoperable to allow for the sharing of information between states.

Turning the Worm Secures the Computer
New Scientist (02/04/06) Vol. 189, No. 2537, P. 32; C. Biever

Experts predict that computer worms are set to become a powerful force and that beneficial worms will quickly spread through networks and patch machines before a malicious worm can attack. Researchers have wanted to fight bad worms with good ones for a long time and now it appears they are finally getting their chance. "We're talking about fighting fire with fire," says Immunity's D. Aitel. In the past, "patching worms" were used by virus-writing gangs to try to stop the spread of worms deployed by their competitors. Legitimate users have been cautious of releasing patching worms because they are hard to control, raising concerns that the originator would be responsible if one were to crash computers it was not designed to patch. Aitel says he has fixed this problem by programming the beneficial worms to visit only computers on a particular network. He calls the worms "nematodes," which are programmed with a map of the network that tells them the range of IP addresses of all the machines they have permission to invade. The "polite" worms can be programmed to ask a central server to grant them permission to invade. Aitel recommends using the domain name system (DNS) server to guarantee that the infected computer always has access to that central

server. Every computer on the network must have access to the DNS server at all times, because they contact it every time they visit a Web page.

Chinese Sensors of Internet Face 'Hacktivists' in U.S.
Wall Street Journal (02/13/06) P. A1; G. Fowler

While the Internet's growing pervasiveness in China has made it difficult to police the activities of an estimated 111 million users, the Chinese government is nonetheless attempting to reinforce its authority, requiring all bloggers to register with the state and continuing its block on objectionable content, such as Wikipedia and the BBC, as well as dispatching roughly a dozen state agencies to monitor Internet activity. Chinese Web censorship, sometimes referred to as the 'Great Firewall,' has sparked an insurgent community of U.S.-based 'hacktivists' who have developed programs such as Freegate, which links computers within China to U.S. servers, enabling users to access prohibited sites. Other efforts mask the identity of Chinese Web users through multilayered host messages that obscure their trail, and adopt-a-blogger programs furnish Chinese writers with external servers to transmit their message. Practitioners of the Falun Gong--the banned Chinese spiritual group that has been persecuted for alleged subversion--have contributed substantially to the development of anti-censorship applications such as Freegate. Voice of America and Radio Free Asia also contribute to Freegate, and a major boost in funding could come from the renewed congressional consideration of legislation to create an Office of Global Internet Freedom in response to harsh criticism of Google, Microsoft, and others for complying with Chinese censorship laws. Freegate, run by North Carolina-based programmer Bill Xia, cannot be blocked by Chinese censors because it constantly switches the address of its U.S. server. Freegate's effectiveness is limited in China, however, as it is employed mostly by technically proficient users, and many Chinese censor their own Internet use, consciously avoiding keywords and content that could be considered subversive. Meanwhile, the government continually devotes more resources to combating Freegate and other anti-censorship applications.

Wireless to Organize--and Maybe Save--Lives
Reuters (02/11/06), S. Carew

The popularity of wireless technology has some laboratories rushing to insert electronic chips into a variety of different products. Sensor chips may one day even be embedded into underwear to send laundry-related text or voice alerts to cell phones, according to Institute for Global Futures President James Canton. "It will tell you when it needs to get cleaned," Canton says. Others predict that wireless sensors may be helpful for saving lives. MIT electrical engineering and computer science professor John Guttag is currently studying how wirelessly connected medical devices may automatically send warnings of a problem to the patient's mobile phone and then on to a relative or a physician. Guttag cautions that such devices would only work if they are sophisticated enough to avoid false alarms. The use of cell phones, software, computers, and sensors can also make our jobs easier and get rid of daily chores, according to researchers at Motorola. Motorola human interaction researcher Tom MacTavish says voice-recognition technology on cell phones could improve with the use of pattern-recognition technology. Image-recognition technology is also in the process of being developed, which could assist law enforcement with the use of wireless devices that can read license plate numbers. Many analysts predict location-aware phones will have an important impact in the future, despite critics who are skeptical about focusing on sophisticated applications, which they say will take years to develop.

Security Gurus Report on the State of Cybersecurity at Demo 2006
ZDNet (02/08/06), D. Farber

John Patrick led a discussion on the state of security with Arizona State University cryptography professor P. Dasgupta, Shinkuro CTO H. Orman, and C. Palmer of IBM Research at the recent Demo 2006. The panelists all say that security problems are here to stay. Not all computer users today know enough about computers and security. "Some products and techniques are bringing security down to the mainstream to protect people who can't protect themselves, said Dasgupta. "It's a cat and mouse game, but we need to bring it to level we can live with it." Palmer said part of the problem is that computers were not designed with security in mind, and today's hackers are more motivated by financial gain than ever before. Dasgupta suggested the use of PKI and smart cards as a way to improve security, despite the reluctance from financial institutions to use smart cards. The experts all agreed that smart cards are not invulnerable, and that they can be used to extract data, which is a problem for high value transactions. Dasgupta also said teaching programming students how to write safe code is not done anymore, which causes problems. Orman added that computer security started with a trusted operating system and that is where it will return to. The panelists were also asked if they thought the NSA could crack 128-bit encryption, and Dasgupta said the answer is unknown. Other forms of security, such as biometrics, were another popular topic of discussion.

Chips That Really Get Under Your Skin
CNet (02/08/06), T. Krazit

At the recent International Solid State Circuits Conference, scientists at the Korea Advanced Institute of Science and Technology presented a chip that is implanted in a user's forearm to function as an audio signal transmission wire that links to an iPod. Many of the presentations featured devices that conserved power, though this chip goes a step further, harnessing the human body's natural conductive properties to create personal-area networks. It is not practical to wire together the numerous devices that people carry with them, and Bluetooth connections fall prey to interference, leading scientists to explore the application of the human body as a networking cable. The Korean scientists augmented an iPod nano with their wideband signaling chip. When a user kept his finger pressed to the device, it transmitted data at 2 Mbps, at a consumption rate lower than 10 microwatts. Researchers from the University of Utah also presented a chip that scans brainwave activity by wirelessly streaming data through monitors in the hopes of creating prosthetics that quadriplegics could operate with their brain waves, though both projects are still in the preliminary research stages.

They Saved the Internet's Soul
Wired News (02/08/06), R. Singel

When the U.S. Supreme Court struck down the 1996 Communications Decency Act (CDA) it preserved the Internet as the free-for-all space it is today. This now has become a landmark case in recognizing the essential free speech nature of the Internet, and it prevented the government from imposing "decency" standards on the Internet that would have had a wider-than-expected muzzling effect. The 1996 CDA made Web sites and ISPs legally responsible for all content on their sites and services, and this would have forced companies to severely limit message board postings, blogs, and all sorts of content. The ACLU challenged the CDA in court and won, though at the time no one knew whether the Supreme Court would see the

Internet as a zone of speech, or in terms of the licensing restrictions imposed on television broadcasters. Center for Democracy and Technology staff counsel J. Morris remembers how back in 1996 the legal team attacking the CDA had to bring computers into courts to educate judges about the Internet. These days 75% of the U.S. population uses the Internet to keep in touch, peruse news, download music, blog, and for other purposes. However, a free and open Internet still faces threats. The U.S. Justice Department plans to appeal an injunction preventing enforcement of the 1998 Child Online Protection Act, and censorship by governments such as China not only affect the Internet, but have influenced Google and Microsoft to cooperate with their censorship relating to search-engine users and bloggers, respectively.