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

**Δελτίο 45**
**20 Οκτώβρη 2006**

**Election Integrity Organizations, Leaders Urge States to Plan for Emergency Paper Ballots, Procedures for November Election, US Newswire (10/13/06)**

Letters were sent out on Friday to all 50 governors, secretaries of state, and directors of elections, asking that they provide emergency paper ballots for the upcoming general election and for these to count as regular, not provisional, ballots. Over 50 election integrity groups and individuals including R. Kenney Jr., Sen. J. Kerry, Rep. R. Holt, Leon County, Florida election supervisor I. Sancho, and computer scientist D. Jones signed the letter. The call for paper ballots is a response to the primaries when many electronic voting machines, which will be used by 80% of voters in the upcoming election, malfunctioned and voters were given provisional ballots that may not have been counted or even sent home. B. Friedman, investigative journalist and co-founder of velvetrevolution.us says, "No legally registered voter should ever be sent away from the polls without being able to cast their vote. With these new electronic voting machines failing across the country, it's just common sense to make sure there are back-up plans and procedures in place." Congress recently failed to pass a bill that would have reimbursed states for the cost of emergency paper ballots. Maryland Republican Gov. R. Erlich has called for statewide paper ballots after the problems during the primaries.

**Safe Internet Requires Total Network Security, Prof. Says**
**Wisconsin Technology Network (10/11/06) Plas, J. Vanden**

As Internet security threats change from being recognition-driven to being profit-driven, entire networks must be secured. Those writing malicious code are becoming increasingly motivated and innovative. "It is very clear now that there are people who are making a lot of money by malicious activity, that organized crime is getting involved in malicious activity, and this represents a very, very serious development from the standpoint that it also means that the bad guys are getting much more organized and focused in their activities," says P. Barford, assistant professor in the University of Wisconsin-Madison Department of Computer Sciences and the school's Advance Internet Laboratory. With hacking software becoming increasingly easier to use for less-than-professionals, businesses must change their approach to security. Simply using firewalls and security software is no longer enough, even with such products becoming more automated and easier to use. What is needed to combat the rising threat is a combination of security that is present at all levels, placing barrier after barrier in the way of potential hackers, says security architect M. Hartmann. "It's security in depth. Every device has its own role to play in security, from a laptop, to the network, to your firewall, to your applications," Hartmann says. At the Advanced Internet Laboratory, Barford leads a research team working on various projects that could lead to an improved Internet that can defend itself against attacks. The group's DOMINO project is focused on intrusion detection and monitoring, while the Global Environment for Network Innovations (GENI) project is tracking malicious activity. Barford says that "right now we have a significant lack of deployment of security in networks, and as we move forward with deploying the latest technology in networks, the wholistic approach to security is something that's really going to solve a lot of problems."

**Geek Speak Birdles Information Security**
**Computerworld Australia (10/12/06), R. Gedda**

At this year's Australian Unix Users Group (AUUG) conference in Melbourne on Wednesday, software developers discussed the negative effects that a lack of usability has on cybersecurity. "A lot of the security stuff is designed by crypto geeks [and] because of a lack of usability, people can't apply them correctly," said University of Auckland computer scientist P. Gutmann. Gutmann notes that a good deal of security standards were composed 10 years ago, without usability in mind, and have only been tweaked since then. "They would rather have 100% perfect software that's unusable than 99% perfect software that is usable," said Gutmann. Open BSD developer R. McBride spoke out against intrusion detection systems, saying the technique has no ability of detecting whether a virus is attacking or not. "I do IDS work for a Fortune 50 company and it's a case of 'Oh look, another box has a virus--go turn it off'...It's very hard to automate turning things off in security," McBride says. He believes the problem must be solved within the software, not IDS. An enormous amount of the body of modern software is not safe, and people continue to use it, says Dr. L. Brown, University of NSW School of IT senior lecturer. She adds that most people see computers as relatively new and do not understand the necessity of information security measures.

**Sending Secret Messages Over Public Internet Lines Can Take Place With New Technique, Newswise (10/10/06)**

Messages can be sent so faint over existing public fiber-optic networks such as those operated by Internet service providers that they would be extremely difficult to detect, or even decode. Princeton University researchers E. Narimanov and B. Wu plan to present the technique during this week's Optical Society of America annual meeting in Rochester, NY. The researchers' method buries a secret message in the low levels of noise of real-world fiber-optic networks. The sender translates the message into an intense, ultrashort pulse of light, and then uses a commercially available optical CDMA encoder to spread it into a faint stream of optical data that can hide in the random jitters of the light waves that transmit information through a network. The recipient uses information on how the secret message was spread out to decode it, and uses an optical device to compress it into its original format. The public signal would be too intense for eavesdroppers to detect the message, even if they knew it was being sent. "As the method uses optical CDMA technology, which is still undergoing significant research, I don't think any government or corporation is implementing this technique yet," says Wu. They believe consumers could also use the inexpensive method when sending sensitive information to their bank.

**Tackling Highjacking With Technology**
**CNN.com (10/06/06), D. Rosenblatt**

A revolutionary in-flight security system called the Security of Aircraft in the Future European Environment (SAFEE) is being developed that could not only detect the presence of a terrorist threat, but safely land the plane in the case of an attempted hijacking. SAFEE uses sensors, cameras, microphones, and biometric devices to detect the presence of biological and chemical agents and monitor the behavior of passengers. The system even has an autopilot function that could lock the controls and take over flying the plane. Psychologists have found evidence that certain biometric "red flags" exist, including body language, visible stress, and even odors released, which can allow someone about to commit a terrorist act to be identifyied. "You cannot make a security system based only on technology, you have to focus on [the

behavior of] people," says Omer Laviv of Athena GS3 Security Implementations. With regard to the recent hijacking of a Turkish airline by an unarmed man, which ended peacefully, "the SAFEE system would have alerted the crew to the issue before the hijacker was able to enter the cockpit," Laviv says. Although SAFEE is scheduled for completion between 2008 and 2010, developers must still win over passengers who are not happy with the prospect of being observed to such a degree. Currently, the system would include a memory bank, similar to a black box, that would erase all passenger information after the flight landed.

**Computerized Voter Registration Databases Need a Major Overhaul**
**Technology Review (10/16/06), K. Bourzac**

University of Utah political scientist T.ad Hall says the most pressing concern facing voters in this November's general election is not voting machines being hacked into, but their names being deleted from the voter registry. Hall is co-author of the recent book "Point, Click, and Vote: The Future of Internet Voting." The problem, Hall explains, is that there is no standard format for creating voter registries, and thus comparison of databases is very unreliable. "You want states to have common databases so that at least within a state you should be able to know if a person has moved, and you can keep records with a state accurate." Kentucky was sued by its own attorney general earlier this year for attempting to delete 8,000 voters from the rolls, with no notice given to these voters. The attempted removal was the result of a comparison of its database with that of Tennessee and South Carolina, which tried to identify voters registered in multiple states. The process of matching names to identify voters registered in two states needs to be a dynamic one, explains Hall, so that registry in one state would lead to immediate removal of the voters name from the rolls of his previous state of residence. Currently, the process is done in a one-time bulk comparison of databases. The Organization for the Advancement of Structured Information Standards (OASIS) and IEEE are currently working on election standards that provide uniformity for difficult issues such as how addresses are to be broken down. Another way the voting process lacks standardization it that hardware from one manufacturer and software from another cannot be used together, severely limiting the choice officials have in creating the most reliable election infrastructure. The Help America Vote Act, the first intervention of the federal government into elections, does not give the four-year-old Election Assistance Committee power to enforce federal standards, to do so would require an act of congress, but Hall foresees increasing pressure for this power to be granted.

**Brazil's Electronic Voting Has Safeguards Lacking in the US**
**Associated Press (10/14/06), S. Lehman**

Brazil began using electronic voting 10 years ago with great trust in the system, but many computer experts think this faith has gone too far. The voting machines operate using Windows CE, but Microsoft, which cites trade secrecy, will not allow independent investigations to assure that malicious programmers have not tampered with the software, and for this reason many advocate switching to an open-source system. A. Brunazo, a computer and data safety engineer who is also the Democratic labor Party's permanent technical representative, founded the Safe Vote Forum to lobby for greater transparency of the electronic voting process. "I agree the electronic ballot box makes it more difficult to defraud the election process, but the system is still not transparent enough, and the best way to address this is by allowing an independent inspection of the operating system used in the machine." A verification system was tried in 2002, where a slip of paper appeared behind glass to assure the voter that their vote was counted correctly, but the manufacturer, Diebold Procomp (Diebold's Brazili-

an division), was opposed to this and favored a single printout from each machine recording every vote registered. However, this "ballot box bulletins" system cannot assure that the votes were not "flipped" by a malicious program. The problem, according to A. Rubin, director of the Information Security Institute at Johns Hopkins University, is not that elections have necessarily been rigged, but that no way to confirm whether or not they were rigged exists. Brazil does conduct random tests of machines hours before its elections, and an independent non-partisan tribunal oversees every step of the election process. "A. Dourado de Rezende, a computer science professor at the University of Brasilia says, "The main flaws are not in the software, hardware, or data transmission systems, but in the human links that control the connections between the three--connections held together by the myth of infallibility and incorruptibility of those who run the system."

**Electronic Voting Machines May Not Eliminate Election Problems**
**Ottumwa Courier (10/09/06), M. Milner**

Despite the uproar over a need for electronic voting machines after the 2000 Florida "hanging chad" controversy, many are doubting the reliability of these new machines. Some of them do not supply a print out of each vote, meaning should the machines fail, or fraud is suspected, there would be no paper trail to consult. With so much riding on these machines, the risk of a hacker or virus tampering with the election is a danger that must be taken seriously. E-voting expert D. Jones, associate professor in the University of Iowa's computer science department, says a tension exists between transparency represented by the paper ballots and the secret ballot process represented by the machines. When using machines, he says, only computer experts can tell if anything has gone wrong, but anyone can understand a paper ballot. Jones also points out that "far more frequent than fraud in elections are mistakes." Jones cites that fraud drops off significantly if only 10% of voters look over again their ballot after making their mark. Poll workers are not professionals, are generally inexperienced, and pose as a large a threat to a smooth election as any element. Jones's problem with voting machines is in the standards to which they are tested after fabrication and before distribution, which are no stricter than any other consumer good coming off an assembly line. Each state has different laws on printouts from voting machines or if paper ballots can be used at all. Iowa's laws, which provide paper ballots in the case that the machines malfunction "come as close to perfect as you can get," says Jones. What Jones really thinks is needed is for election officials to increase emphasis on research and development of voting machines.