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

**Δελτίο 171**
**30 Μάρτη 2010**

**Malicious Systems of a Feather Flock Together**
**Government Computer News (03/11/10), W. Jackson**

Indiana University and Oak Ridge National Laboratory researchers have developed a method for finding where malicious systems originate. The researchers performed a statistical analysis of Internet Protocol (IP) addresses from blacklists to identify Internet service providers, hosting services, or other autonomous systems with high levels of blacklisted IP addresses. "We wanted to be able to say if a particular network is doing a good job of cleaning up its machines," says Oak Ridge researcher C. Shue. The researchers found that some autonomous systems have more than 80% of their IP addresses blacklisted. Three US-based hosting providers accounted for more 6% of one of the blacklists, a disproportionately large percentage for the size of the systems. "This indicates that some [autonomous systems] have either too lax a security policy or may be intentionally harbouring cybercrime," the researchers say. The next step is to evaluate the quality of the blacklist data.

**How Privacy Vanishes Online**
**New York Times (03/16/10), S. Lohr**

Personal privacy is being threatened as Internet users increasingly provide information about themselves on social networking sites, which can be collected and analyzed by computers to create a picture of a person's identity. "Personal privacy is no longer an individual thing," says Massachusetts Institute of Technology professor H. Abelson. "In today's online world, what your mother told you is true, only more so; people really can judge you by your friends." Although users can implement privacy controls on most Internet sites, researchers say that is rarely enough to protect privacy. For example, University of Texas professor V. Shmatikov and Stanford University researcher A. Narayanan were able to identify more than 30% of users of both Twitter and Flickr, even thought the accounts had been stripped of identifying information like account names and email addresses. At Carnegie Mellon University, researchers A. Acquisti and R. Gross reported they could accurately predict the Social Security numbers for 8.5% of the people born in the US between 1989-2003--nearly 5 million people. "When you're doing stuff online, you should behave as if you're doing it in public - because increasingly, it is," says Cornell University professor J. Kleinberg.

**Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies**
**Washington Post (03/19/10) P. A1; E. Nakashima; D. Priest; K. DeYoung**

The dissolution of an intelligence-gathering Web site set up by the Saudi government and the US Central Intelligence Agency (CIA), based on suspicions that it was being used by extremists planning attacks on US forces in Iraq, highlights the need for more transparent cyberwar policies. The use of computers to collect intelligence or to disrupt the enemy raises a number of issues, including under what circumstances a cyberattack outside the theater of war is permissible and whether dismantling an extremist Web site represents a covert operation or a traditional military activity. Current and former officials say that lawyers at the US Justice Department's Office of Legal Counsel are engaged in a struggle to define the legal

rules governing cyberwarfare. A key dilemma of cyberwarfare is that an attacker can never be sure that only the intended target will be impacted by an attack. A former official notes than more than 300 servers in Saudi Arabia, Germany, and Texas were unintentionally disrupted when the Saudi-CIA site was dismantled.

**Cyber Warriors**
**The Atlantic (03/10) Vol. 305, No. 2, P. 58; J. Fallows**

Google's recent disclosure of broad surveillance "originating from China" highlighted a threat that many experts are convinced will continue to grow, writes J. Fallows. Purdue University computer scientist E. Spafford says that cybercrime has evolved into a well-financed enterprise perpetrated by mature individuals and groups of professionals who have deep financial and technical pockets, as well as the tolerance, if not support, of local governments or other countries. Cybercrime experts generally agree that the primary damage inflicted by cyberwar so far has been business-versus-business spying rather than the stealing of military secrets or electronic sabotage. Fallows says that China has become even more of a potential cyber-adversary due to its ability to rapidly approach parity with the West in terms of advanced information systems, particularly in its focus on being able to cripple foes' networking infrastructure in times of war.

**Legislators Propose International Cybercrime Cooperation Laws--With Teeth**
**Dark Reading (03/23/10), T. Wilson**

The International Cybercrime Reporting and Cooperation Act, recently introduced by US Sens. K. Gillibrand (D-NY) and O. Hatch (R-Utah), would require the US government to study the cybercrime policies of other nations and either aid or punish those countries according to the findings. The bill requires the president to annually report to Congress on the state of countries' employment of information technology (IT) in critical infrastructure, the scope of cybercrime based in each nation, the sufficiency of each country's cyberlaw enforcement systems, and countries' safeguarding of consumers and commerce online. Furthermore, the legislation would require that programs developed to fight cybercrime be prioritized to countries with low IT penetration in order to deter the creation of future cybercrime sanctuaries in these countries. Moreover, efforts to assist in the development of critical infrastructure would be encouraged to feature anti-cybercrime programs.

**Funding for WWII Code-Breaking Centre Bletchley Park**
**Times Online (United Kingdom) (03/26/10), H. Devlin**

The UK government has provided a 250,000-pound grant to repair Bletchley Park, where British mathematicians, including Alan Turing, worked to break Germany's Enigma codes in World War II. The site also is where one of the world's first programmable computers, Colossus, resides. British prime minister Winston Churchill destroyed all evidence of the secret code-breaking program after the war, due to fears the Soviet Union would discover it, but in 1991 the Bletchley Park Trust, formed by historians and ex-codebreakers, saved the site and opened it to the public. The grant will be used to make repairs to the structure and to buy new computer equipment, but Bletchley Park supporters have more ambitious plans to turn the center into a National Museum of Computing.

**Laser Security for the Internet**
**American Friends of Tel Aviv University (03/23/10)**

J. Scheuer at Tel Aviv University's School of Electrical Engineering has developed an information security system that acts as a type of key bearer. The system is designed to transmit the key bearer, a binary code, in the form of 1s and 0s via light and laser rather than numbers. "The trick is for those at either end of the fiber-optic link to send different laser signals they can distinguish between, but which look identical to an eavesdropper," Scheuer says. The system, which runs on existing fiber-optic and computer technology, makes use of a specially designed laser that can reach more than 3,000 miles without losing key parts of the signal. Scheuer says only the sender and receiver would be able to unlock the shared key code, and notes that the strategy is simpler and more reliable than quantum cryptography. Lab demonstrations showed the use of light pulses to transmit binary lock-and-key information could be absolutely secure.

**Academic Paper in China Sets Off Alarms in US**
**New York Times (03/20/10), J. Markoff; D. Barboza**

A paper by Chinese researchers envisioning a cyberattack on the US power grid has ignited concerns in the United States. The researchers outlined an assault on a small US power grid sub-network that triggers a cascading failure of the entire electrical infrastructure. The paper's co-author, Chinese graduate engineering student W. Jianwei, says the research is purely theoretical, and that its intent is to find ways to augment power grids' stability by investigating potential vulnerabilities. Although some analysts see the paper as a sign that China has an interest in interfering with the US power grid, University of Pennsylvania physicist R. Albert disagrees. "Neither the authors of this article, nor any other prior article, has had information on the identity of the power grid components represented as nodes of the network," Albert says. "Thus no practical scenarios of an attack on the real power grid can be derived from such work." Wang says he chose the United States as a potential target because it publishes data on power grids, and it was the only country he could find with accessible, useful information.

**New Spam Targeting Facebook Users Is Invisible to Most Virus Scans, Says UAB Expert, University of Alabama at Birmingham (03/18/10), A. Reiber**

Fake Facebook emails and related viruses are a serious malware threat, according to G. Warner, director of research in computer forensics at the University of Alabama at Birmingham (UAB). Warner says that only one-third of the 42 most common antivirus products are detecting the malware, which is called BredoLab. The team has uncovered at least eight versions of BredoLab since March 16. "What is troubling is the newer versions of the BredoLab used in this latest attack campaign are not being detected by the majority of antivirus services--and that means the majority of users who unwittingly click on the bogus attachments linked to fake emails are going to have their computers infected," Warner says. The spam asks Facebook users to open an attachment to obtain new login information. "Once a computer is infected with BredoLab, the cybercriminals are able to add any other malicious software they desire to the infected computer" he says.

**Cyberattacks Are 'Existential Threat' to US, FBI Says**
**Computerworld (03/24/10), P. Thibodeau**

The threat from cyberattacks is so severe that it actually threatens the very existence of the US, says Steven Chabinsky, the deputy assistant director of the US Federal Bureau of Investigation's cyber division. Chabinsky says the threat comes from two sources - foreign govern-

ments and terrorists. He says foreign governments use cyberattacks in order to steal state secrets and private-sector intellectual property in the hopes of undermining the stability of the US government and weakening the U.S. military and economy. But Chabinsky says a bigger threat comes from terrorists, who are increasingly turning to cyber technologies in order to exploit the US's weaknesses. He says there are several steps that need to be taken in order to deal with this threat, including adopting tier levels of service at federal agencies in order to limit the ability of vital systems to interoperate with weak and vulnerable systems. Chabinsky also says that government organizations need to evaluate their risk postures and ask vendors who provide them with security tools whether they can guarantee the security of their systems. Finally, citizens should help law enforcement officials by reporting cybersecurity breaches, Chabinsky says.