Internet Traffic Begins to Bypass the U.S.
New York Times (08/30/08) P. B1; J. Markoff,

During the first three decades of the Internet most Web traffic flowed through the US, but Internet traffic today is increasingly bypassing the US, which could have consequences for the intelligence community and the military. American intelligence officials have warned about this change for several years. "Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge," said CIA director M. Hayden in 2006. "We also need to protect that edge, and we need to protect those who provide it to us." Some Internet technologists and privacy advocates say US government and corporate policies that allowed the US to monitor Internet traffic may be hastening the move away from the US Electronic Privacy Information Center executive director M. Rotenberg says since the passage of the Patriot Act, many companies outside the US have been hesitant to store client information in the US Economics also has led to the shift, with more countries recognizing the importance of having their own networking infrastructure, and how being reliant on other countries for their Internet traffic makes them vulnerable. University of Minnesota professor A. Odlyzko says the US now carries about 25% of the world's Internet traffic, down from 70% 10 years ago. "Whether it's a good or a bad thing depends on where you stand," says computer scientist V. Cerf. "Suppose the Internet was entirely confined to the US, which it once was? That wasn't helpful."

Computer Viruses Make it to Orbit
BBC News (08/27/08)

NASA is investigating how laptops brought to the International Space Station (ISS) in July were infected with the Gammima.AG computer virus. The malicious program does not pose a threat to ISS command or control systems because the infected laptops were only used to run nutritional programs and to let the astronauts send email back to Earth. An astronaut might have taken Gammima.AG into space via a flash or USB drive, and there have been reports that the astronauts did not have any antivirus software on their laptops. The spacecraft does not have a direct connection, and incoming data is scanned before it is transmitted. The computer virus, first detected on Earth in August 2007, is designed to steal passwords and login names so popular online games can be played. Computer viruses have been taken to ISS before, but NASA describes them as only a "nuisance." However, it now plans to install security systems.

Public, Private Sectors at Odds Over Cyber Security
Los Angeles Times (08/26/08), J. Menn

Cybersecurity experts say that three recent, significant computer security breaches highlight how badly the Internet needs a major overhaul, and exposes the rift between corporate America and the US federal government over who is responsible for fixing the Internet. Over the past few months law enforcement officials busted an international ring that accessed customer databases and trafficked tens of millions of credit card numbers, a researcher discovered

a major flaw in the Domain Name System that could allow hackers to redirect Web users to fake versions of popular Web sites, and computer attacks have been used to cripple the country of Georgia's Internet capabilities. However, these incidents have done little to make cybersecurity a more prevalent issue on a national scale. "Nothing is happening," says J. Dixon, former director of the National Cyber Security Division at the Dept. of Homeland Security (DHS). "This has got to be in the top five national security priorities." The US government has primarily argued that the private sector is better positioned to handle the problem, but corporations say the problem is too large for them to manage. Industry professionals say the Internet's technical underpinnings, which are loosely administered by the US Commerce Department, need a major overhaul to eliminate vulnerabilities. The disagreement is largely because cybersecurity issues touch on so many different areas, with DHS overseeing the protection of government networks, the FBI and Secret Service pursuing cybercrimes, and the US State Department following up on cases that lead to other countries. The US government has assembled taskforces that called for increased cooperation and communication between public and private sectors, but experts say their efforts have yet to yield tangible results.

Terror Threat System Crippled by Technical Flaws, Says Congress
Computerworld (08/27/08), P. Thibodeau

A US House subcommittee claims that a $500 million IT project intended to find connections between terrorist suspects and prevent future terrorist attacks is a failure, and is unable to handle even basic Boolean search terms such as "and", "or", and "not." Most of the subcommittee's charges come from a memo prepared by subcommittee staff about a data integration project called Railhead, which is intended to help intelligence and law enforcement agencies discover terrorist plots. Railhead, scheduled to be ready by the end of the year, is supposed to combine and upgrade existing databases, called the Terrorist Identities Datamart Environment, and strengthen terrorism-fighting capabilities. However, the project has suffered from delays and excessive costs, and may be shut down, says subcommittee chairman B. Miller (D-NC). "The end result is a current system used to identify terrorist threats that has been crippled by technical flaws and a new system that, if actually deployed, will leave our country more vulnerable than the existing yet flawed system in operation today," Miller writes in a letter to the Office of the Director of National Intelligence. Railhead uses XML to integrate data from dozens of data sources and a variety of agencies, but the design team behind the project says XML may not be viable. In testing by the Hewlett-Packard Quality Center, Railhead software was able to pass 148 tasks, failed to complete 26 others, and failed 42. Specific problems included a failure to create reports and failing to find non-exact matches for key entries, such as a suspected terrorist's name.

Indian Researcher's Improved Anti-Hacking System for Wireless Networks
Asian News International (09/04/08)

Florida Atlantic University researchers A. Srinivasan, F. Li, and J. Wu have developed the Probabilistic Voting-based Filtering Scheme (PVFS), which they say can protect and help improve the viability of wireless sensor networks (WSNs). WSNs are vulnerable to two types of cybersabotage, according to the International Journal of Security and Networks. The first is the fabricated report with false votes attack that sends phony data to the base stations with a forged validation. The second type of attack adds false validation votes to genuine incoming data, which labels genuine data as being false. Most WSN systems have built-in software to prevent false data from being given valid credentials, but the second type of attack is more difficult to detect. The researchers say the PVFS can counter both of these attacks simulta-

neously. To protect the WSN while maintaining normal filtering, the researchers use a general en-route filtering scheme that breaks WSNs into clusters and locks each cluster to a particular data encryption key. As data reaches the headquarters from the clusters, the main cluster-heads check the report together with the votes, acting as the verification nodes in PVFS. Should a saboteur compromise one or more of the sensors on a WSN, the PVFS will apply probability rules to determine the likelihood that the network was compromised, using data from other sensors in different clusters before reporting incoming data as false.

MIT Lincoln Laboratory Software Aims to Thwart Cyber Hackers
MIT News (08/27/08)

Researchers at the MIT's Lincoln Laboratory are developing the Network Security Planning Architecture (NetSPA), software that will identify the most vulnerable points in a computer network. NetSPA uses information on networks, individual machines, and any programs running to create a graph that displays how hackers could infiltrate the network. System administrators can examine the graph and determine the best course of action. NetSPA relies on vulnerability scanners to identify known weaknesses in network-accessible programs that could allow an unauthorized person to access a machine. NetSPA also analyzes complex firewall and router rules to determine which vulnerabilities can be reached and exploited by attackers, and how attacks can spread within a network by moving from one vulnerable host to another. R. Lippmann, leader of the development effort, says NetSPA enables network administrators to see which vulnerabilities pose the greatest threat to the network, allowing them to fix those problems first instead of patching or fixing vulnerabilities that are not accessible to attackers. NetSPA also can account for unforeseen avenues of attack, such as if a network had to share data with an outside vendor years ago, and now someone is forging that IP address to try to exploit the forgotten permission.

Protecting Your Vote With Invisible Ink
Discover (09/04/08), M. Lafsky

Transparency of the entire voting system has never been more important, and each voter should be able to verify that his or her vote is protected and correctly recorded in the final tally. The challenge is revealing the secret ballot process without sacrificing the privacy that democracy relies on. Computer scientists, lead by cryptographer D. Chaum, say they have found a solution that uses invisible ink to protect voter confidentiality. The Scantegrity II (invisible ink) system was unveiled at the USENIX/ACCURATE Electronic Voting Technology Workshop. The system uses a regular pen and a special decoder pen for use on a ballot that looks like a normal fill-in-the-dot ballot. Voters make their selections by marking the bubble next to their candidate of choice with the decoder pen. A two- or three-letter code will appear in the bubble. The ballots' serial numbers, as well as the invisible codes, have all been created and recorded by voting officials before the election to eliminate the possibility of ballot stuffing. Voters can record their ballots' serial numbers and codes to verify their vote was counted. The ballot is then scanned through an optical scanner. Chaum says that even if only 1-2% of voters go online to check their receipts, it will create a 95% chance that no fraud occurred.