Cellphone Encryption Code Is Divulged
New York Times (12/29/09) P. B3; K. O'Brien

German encryption expert K. Nohl says he has deciphered and published the secret code used to encrypt most of the world's cell phone calls in an effort to call attention to vulnerabilities in global wireless system security. The privacy of 80% of mobile calls worldwide is shielded by the 21-year-old global system for mobile communication (GSM) algorithm, whose security Nohl said was inadequate at the Chaos Communication Congress, a four-day conference of computer hackers that runs through Wednesday in Berlin. In August, Nohl challenged other hackers to assist him to crack the GSM code, and through the collaborative initiative the algorithm's code book was eventually reproduced through random combinations. Nohl says the code book was accessible on the Internet via services such as BitTorrent. Although the GSM Association devised a 128-bit successor to the 64-bit algorithm originally adopted in 1988, the majority of network operators have not upgraded to the new code. At the hacker conference, Nohl warned that the hardware and software required for digital surveillance of cell phone calls were freely available as an open source product in which the coding is available for individuals to customize. Nohl's decryption efforts were deemed illegal by the GSM Association, but ABI Research executive S. Schatt says the disclosure, while not threatening in itself, makes the case that companies and governmental organizations should take the same measures to guarantee the security of their wireless conversations as they do with antivirus software for computer files.

Moving Video to "CAPTCHA" Robot Hackers
American Friends of Tel Aviv University (12/29/09)

Tel Aviv University (TAU) researchers have developed a new Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) security mechanism designed to stop computer algorithms programmed to beat current CAPTCHA technology. TAU's D. Cohen-Or led a research team that created video CAPTCHA code that uses an emergence image - an object on a computer screen that only becomes recognizable when it is moving. Humans are very good at identifying these types of images while computers are not. "Computer vision algorithms are completely incapable of effectively processing emergence images," says TAU professor L. Wolf. The researchers also are developing ways of generating hidden images in a natural background, such as an eagle or a lion in a pastoral mountain setting. "A good CAPTCHA has to be something that's easy for people but hard for a computer," says Cohen-Or.

Q&A: Researcher Karsten Nohl on Mobile Eavesdropping
CNet (01/01/10), E. Mills

German security expert Karsten Nohl made headlines at the recent Chaos Communications Congress hacker conference in Berlin by demonstrating that the encryption function for Global System for Mobile Communications (GSM) technology is insecure. Nohl showed how easy it was to eavesdrop on GSM-based cell phones, which account for about 80% of the mo-

bile phone market. As part of an open source, distributed computing project launched in August, Nohl released a code book for cracking GSM encryption to the public. The problem with GSM's A5/1 encryption function is that its 64-bit key is not long enough to handle the computing power of today, he says. "When the algorithm was designed 20 years ago when CPU cycles and storage were much more expensive, it must have seemed a lot more secure," he says. "However, the A5/1 function should have been replaced years ago when researchers first discussed practical attacks." Nohl notes that the tables developed to crack the A5/1 function could not crack A5/3, the newer encryption used in third-generation networks, which also is considered a security patch for GSM networks.

K-State Computer Scientists Developing Techniques to Strengthen the Security of Information Systems for Health Care, Military Data
Kansas State University News (01/05/10), J. Hatcliff

Kansas State University (KSU) researchers, in collaboration with Princeton University (PU) computer scientists, are developing tools to secure information systems spanning large distances. The research team, led by KSU's J. Hatcliff and PU's Andrew Appel, received a five-year, $3 million grant from the Air Force Office of Scientific Research. The new tools involve creating mathematical and logical models that can be used by special auditing programs to make sure that information systems are secure. "We're doing foundational research on novel forms of mathematical models and logics that enable designers and analysts to precisely state what information is allowed to flow from one point to another and under what conditions," Hatcliff says. The researchers also are working with Rockwell Collins, a company that creates communications and aviation electronics. Rockwell Collins wants to apply the KSU research to several systems currently in development at the US Dept. of Defense. The new tools also have the potential to be integrated into the health care system for use with patients' medical records, Hatcliff says. The researchers say the tools already have been used by several academic research groups and various industries from around the world.

Pentagon Computer-Network Defense Command Delayed by Congressional Concerns
Washington Post (01/03/10), E. Nakashima

US Congressional concerns about privacy and legality are slowing plans to move forward with the Pentagon's cyberdefense system. The Pentagon's system, known as cyber command, aims to consolidate the existing offensive unit, Joint Functional Command Component-Network Warfare, and the defensive unit, Joint Task Force-Global Network Operations. The plan also calls for intensified blocking of malicious software and codes entering military networks. Technology currently exists that can detect and block malware at the gateways to the Pentagon's networks, but the ability to use that technology has led to policy questions. Privacy advocates are sensitive to government monitoring of private communications networks. The Pentagon is working with the US Justice Department, the US Dept. of Homeland Security, the White House, and other agencies to make sure the actions are legal and part of a national cybersecurity framework. Almost all of the cyber command's focus will be on defensive measures, according to C. Inglis, deputy director of the US National Security Agency (NSA). "Our goal is to better protect our forces," says deputy assistant Secretary of Defense R. Butler. Although concerns remain about the government's monitoring of communication lines, defense officials say that cyber command will be used solely as a protective measure. "No information will be shared other than to support what we need to defend the networks--the defense military information networks," says NSA Lt. Gen. K. Alexander.

Airline Security: The Technical Task of Connecting Dots
InformationWeek (01/07/10), J. Foley

Maintaining the security of airlines entails a formidable effort to assimilate intelligence data produced by numerous sources, if intelligence breakdowns, such as the one that led to the near-bombing of an airliner on Christmas Day, are to be averted. Among the myriad elements that must be linked together from multiple intelligence agencies is data on known terrorists and suspects, information taken from passports and visa applications, ticket purchases, airport screening systems and procedures, airline passenger lists, video surveillance, information generated by associates of terrorists and suspects, phone records, and even hints on social media sites. Intelligent Enterprise's D. Henschen says the challenge the US government is facing is the classic information management problem of mining mammoth volumes of structured data as well as unstructured data for meaning that could make the difference between life and death. Technologies and practices that play a role in data assimilation include business intelligence tools, enterprise content management, data integration middleware, master data management, complex event processing, text mining, identity resolution, data mining, data cleansing, relational databases, and data warehouses. Emerging technologies such as social media analysis software and open source search capabilities also could contribute to the intelligence enhancement effort. However, technology alone will not cure the intelligence community's communication difficulties. People, processes, and communications also need to be emphasized.