Foundations for NATIONAL SECURITY

TECHNOLOGIES AT WORK ON THE FRONT LINE

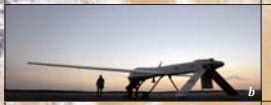
The NITRD Program is the principal source of fundamental advances in the digital technologies powering vital national defense, national security, and homeland security capabilities – from precision command-and-control, communications, and weapons systems, to advanced systems for intelligence gathering and analysis, to technologies and tools for detecting and preventing terrorist attacks on U.S. soil and increasing security for all Americans. The NITRD agencies' expertise is also aiding Administration efforts to coordinate and mobilize Federal technological resources in support of Department of Homeland Security (DHS) applications.

High-priority NITRD research plans for FY 2004 continue to focus on strengthening the overall security, reliability, and robustness of critical U.S. networks, high-end computing systems, and digital infrastructures. This work includes development of "trust" technologies for broadband, optical, wireless, and other ad hoc networks; cost-effective methods for designing highly reliable software; and new science and engineering approaches to achieve unprecedented dependability and security – called "high confidence" – in complex systems and software. Other efforts focus on advanced computational capabilities, such as data mining and language translation, for national security applications. Working with NSTC, the NITRD agencies are also developing a comprehensive plan to guide federal investments in high-end computing to meet critical mission needs ranging from national security and defense to basic science.

Advanced battlefield capabilities

Applications of NITRD research have been and continue to be deployed on many fronts in the war on terrorism. In Iraq, the unprecedented ensemble of networked high-performance communications, reconnaissance, distributed information management, and precision-guided munitions systems supporting U.S. battlefield operations led *Business Week* to term the conflict the world's first "digital war." Among the new capabilities were DARPA's Phraselator language-translation devices and translingual information detection, extraction, and summarization (TIDES) software for intelligence analysis.

The unmanned aerial vehicle (UAV), one of the "advanced concept" capabilities to play a prominent role in Iraq, has achieved a high level of sophistication that reflects NITRD technological advances in hardware and software components, including remote-sensing, telemetry, and secure wireless networking technologies for remote command and control.



These airborne systems, being deployed by several services in a range of sizes and equipped for varying tasks, provide versatile platforms for wide-area, persistent (many hours at a time), and multimodal (many kinds of sensing and scanning devices) reconnaissance and attack without putting soldiers at risk.

Sensor technologies for hazard detection

The NITRD agencies' research in robotics and in the miniaturization, communications capabilities, and integration of digital components with micro-electromechanical systems (MEMS) such as sensors, actuators, and signal processors enables advanced remote-sensing and networked embedded systems not only for military applications but also for space exploration and scientific research. In the war on terrorism, these technologies are also being applied in small, low-cost

a) *U.S. Army Blackhawk helicopter over southern Iraq during Operation Iraqi Freedom. Research on methods and tools for enhancing battlespace visualization for decision making in mobile units and multi-display command-and-control centers is a focus of ODDR&E's Multidisciplinary University Research Initiative.*

b) *U.S. Air Force Predator unmanned aerial vehicle (UAV) receives ground check before mission.*
c) *Precision-guided Tomahawk cruise missile is fired from U.S.S. Winston Churchill in eastern Mediterranean.*
d) *Air Force officers at coalition operations center in Qatar coordinate multinational mission information.*

e) *Navigator on a B-52 "Superfortress" checks flight details with ground control on wireless computer communications system.*
f) *NASA March 25, 2003, satellite image of Iraq shows severe dust storms (orange streaks). Computer weather models developed by Johns Hopkins University and the University of Colorado also helped coalition forces anticipate dust conditions.*

devices for detecting and identifying biological pathogens, chemical and radiation hazards, and explosive materials.

SnifferSTAR, the result of a DOE/SC-Lockheed Martin Corporation partnership, is a half-ounce unit designed to ride on UAVs to detect nerve gases and blister agents. Operating on half a watt of power, it consists of a butter-pat-sized sensor platform on top of a microprocessor board. The airstream is sampled every 20 seconds by the sensors, which register the mass of airborne particles as electronic frequencies and send the signals to the processor; the digital data are transmitted to the UAV or to a ground link, where they are immediately compared against a library of data patterns for many dangerous gases. Other new sensor technologies include inexpensive microarrays of DNA sensors on a chip that can detect multiple pathogens, such as anthrax and smallpox; acoustic sensors that use sound waves to determine the chemical composition of materials in closed containers; and handheld radiation detectors, now commercially produced and deployed in homeland security activities.

Networks of tiny devices

NITRD advances in software and networking now also make it possible to federate microsensor arrays in ad hoc wireless networks, with potential not only for battlefield reconnaissance but for industrial, health, and environmental monitoring. "Smart dust," a DARPA project in sensor miniaturization, incorporates these new capabilities as a result of work funded by DARPA and NSF at the University of California at Berkeley and a partnership with the Intel Corporation. Researchers re-engineered a sensor prototype to turn it into a modular, component-based computing platform with a processor, sensor, radio, and power distribution system. Because the operating system – TinyOS – and database – TinyDB – are open source software, and Intel is sharing wireless networking technology, developers in many domains are now working on commercial applications.

DOE/SC, NOAA, and corporate partners are linking sensor and mass spectrometry technologies, wireless and wired networking, meteorological instruments, remote telemetry, and computer modeling in a prototype SensorNet, a nationwide system for real-time detection and assessment of chemical, biological, radiological, and nuclear threats. The goal of this effort is to provide immediate, scientifically accurate information to first responders about the nature, severity, and likely dispersion of such agents in the environment. This work complements fundamental investigations by NIH and NSF aimed at developing new methods both to prevent biological and chemical agents from causing harm and to mitigate the severity of contamination incidents.

Assuring technology quality

As the primary measurement and standards laboratory for the United States, NIST conducts research in ultra-precision sensors and works closely with other Federal agencies and industry to develop standards that ensure the accuracy of measurements made by new hazard-detection technologies. A NIST initiative with the Federal Aviation Administration, for example, is using mass spectrometry – a powerful laboratory method supported by IT that identifies a substance's unique chemical fingerprint – to assess the effectiveness of walk-through explosive detectors. Developed with EPA and NIH, NIST's digital library of mass spectral prints for 140,000 chemical compounds is included as the standard reference guide with most mass spectrometers sold today.

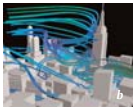
Help for first responders

With funding from the National Institute of Justice, NIST is working with the public safety community to standardize techniques and protocols in wireless telecommunications and IT applications for emergency response networks. NIST is also developing Web-based technologies for integrating sensors, real-time video, "smart tags," and embedded microprocessor devices in a next-generation distributed information-gathering and interactive communications system for field deployment by first responders.

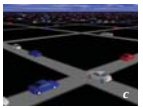
Powerful tools for emergency planning

Today, computational modeling, simulation, and visualization capabilities pioneered in NITRD research are helping emergency planners, first responders, public-health officials, and building engineers better understand and prepare for the complex impacts of catastrophic events. Some examples:

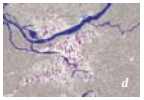
- DOE/SC researchers have developed high-resolution structural dynamics models to simulate the effects of bomb blasts on buildings and other structures. The simulations, which require very high-performance computing capabilities, can be used to evaluate structural vulnerabilities and assist in development of blast-resistant architectural designs and retrofits for existing structures.



- A NIST-developed computational model, the Fire Dynamic Simulator, and related software called SmokeView are enabling investigators of the World Trade Center disaster to study how building geometry, fuel distribution, and wind conditions interacted with the smoke and fires within and outside the towers. In conjunction with its ongoing evaluation of building materials in collaboration with industry, NIST is also preparing a technical assistance package including software tools to help building owners, contractors, designers, and emergency personnel consider how building attributes would factor in a crisis.



- TRANSIMS (Transportation Analysis and Simulation System) – developed for the Department of Transportation by scientists at the National Infrastructure Simulation and Analysis Center (transferred from DOE/SC to DHS) – is a high-end software tool that can integrate tens of millions of interacting variables to represent transportation and traffic flows across an entire urban area over time, from the level of a single pedestrian and traffic light to the aggregate. Designed to provide metropolitan planners with a highly accurate, comprehensive picture of traffic impacts, congestion, and air quality, the tool now is helping emergency planners analyze the effects of disruption on complex urban infrastructures to improve disaster preparedness. IBM Business Consulting Services has licensed TRANSIMS and is working with state and local officials to integrate the tool into their analyses.



- A derivative tool, EpiSIMS (Epidemiological Simulation System), couples models of disease transmission with population-mobility data so that planners can test the efficacy of various public-health response strategies.

NITRD guidance for improving cybersecurity

The NITRD agencies are key contributors to Federal efforts in partnership with the private sector to improve the security of existing networks and computing installations. Work by NIST, NSA, and other DoD agencies underlies the set of "security benchmarks" distributed nationwide in 2002 by the Center for Internet Security, a voluntary consortium of public and private organizations. These instructions and software tools for enhancing security in today's most widely used operating systems and networking technologies are termed "the gold standard" by the IT industry because they reflect public-private consensus on best practices based on thorough evaluation and testing. NIST and NSA jointly support the National Information Assurance Partnership, an international compact among countries that apply validated security standards to assess commercial IT products.

NSF and NIST were authorized by the Cybersecurity R&D Act of 2002 (P.L. 107-305) to take immediate action to address critical national needs in this area. NSF, chartered to take the lead in cybersecurity research and education, has more than doubled its research investment in fundamental security technologies and is supporting training of cybersecurity professionals. NSF plans are underway to expand educational and capacity-building activities in this critical area of workforce development. NIST's responsibilities under the new law include assessing national infrastructure vulnerabilities, fostering public-private partnerships to advance security technologies and standards, establishing postdoctoral cybersecurity fellowships, and coordinating on the IT security research agenda with NSF and other Federal agencies.

NITRD Program representatives participate in NSTC's Critical Information Infrastructure Protection Interagency Working Group, contributing research perspectives and results from long-term NITRD R&D for application in security-related technologies.

a) *"Sniffer Star," a butter-pat-size sensor, samples air for toxic agents and relays findings via wireless system to be checked against digital archive of known toxic gases.*

b) *EPA used computational fluid dynamics simulations after 9/11 to help evaluate the spread of materials from the World Trade Center.*
c) *TRANSIMS enables simulations incorporating millions of data points from disaggregated variables, such as pedestrians, vehicles, mass transport, traffic signals, and road characteristics.*

d) *DOE/SC researchers worked with Portland, Oregon officials to simulate the geographic spread (purple shows cases) of a smallpox epidemic in the city, using the EpiSIMS model. Effects of various interventions versus inaction were examined.*