WHAT IS THE I3P?

The I3P—Institute for Information Infrastructure Protection—is a consortium of leading universities, national laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States. Through its various initiatives, the I3P:

Identifies critical infrastructure vulnerabilities
Fosters collaborative research
Serves as a trusted partner for industry and government
Devises and facilitates the adoption of security tools and other mitigation strategies

In short, the I3P functions as a national forum on cyber security, undertaking research, identifying key R&D disciplinary research topics and seeking solutions through the power of inter-institutional and multi-disciplinary research.

Shari Lawrence Pfleeger, senior information specialist at the RAND Corporation and team leader for the I3P "Insider Threat" project

CLOSING THE SECURITY GAP: FOUR KEY INITIATIVES

In 2007, the I3P launched four new research initiatives:

Process Control Systems Survivability and Recovery

Process control systems (PCS) are essential to the safe, reliable and efficient operation of complex industrial processes, including petrochemical refining and electric power generation.

Recognizing the need to safeguard these critical systems against cyber intrusions, I3P researchers are developing technologies to harden PCS security, including tools that will enable the systems to continue operating if attacked and to quickly recover should a disruption occur.

Insider Threat: An Analysis of Human Behavior

Employees and other individuals with legitimate access to a network's computers have the means, either deliberate or inadvertent, to inflict serious harm on an organization.

Not only do insiders exist at all levels of an organization, but almost anyone can be a potential "insider." Recognizing the seriousness of the situation, an I3P team is undertaking a path–breaking analysis of insider threat, one that encompasses not just technical challenges but also various ethical, legal and economic dimensions. The team's findings will eventually lead to tools for detecting, monitoring and preventing insider attacks.

Business Rationale for Cyber Security

Measuring or quantifying the benefits of cyber security investment is an essential business strategy but also a notoriously challenging one. Many companies underestimate the threat of attack, misunderstand their vulnerabilities and overlook key economic incentives.

To facilitate better decision making, a team of I3P experts has launched a sweeping study of cyber security investment strategies, from risks and vulnerabilities to supply-chain interdependencies and technological fixes.

Safeguarding Digital Identity and Privacy

With ever more information stored and transmitted electronically, the collection, use and disclosure of personal data has emerged as a critical security issue.

Who has legitimate access to which information for what purpose? In answering that question, I3P researchers are devising a comprehensive framework for identity management, including a suite of tools that will significantly restrict unauthorized access to, and distribution of, data. To ensure adoptability, the team is also addressing the legal, economic and social implications of their solutions.

MEETING A CRITICAL NEED

- A leader in identifying infrastructure vulnerabilities, the I3P tackles a wide range of critical cyber security issues from a multi-disciplinary, multi-institutional perspective.
- Promotes technology transfer by developing security tools and other risk-mitigation technologies in partnership with software vendors and end users.
- Serves as an intellectual and technical resource, providing data and expertise to various stakeholders, including industry, policy makers and the general public.
- Responds quickly to new challenges by drawing on the diverse technical and policy knowledge of its members. Fosters effective collaboration among a broad assembly of technical and policy experts.

THE POWER OF A CONSORTIUM

I3P-supported researchers form teams to address specific vulnerabilities and head research initiatives that are externally reviewed on a regular basis for impact and applicability. They regularly host meetings to identify and discuss emerging vulnerabilities and mitigation needs.

They publish in peer-reviewed journals, develop models, make industrial site visits and participate in numerous conferences and professional association meetings.

They share information and collaborate with experts from government as well as the private sector, including banking and finance, the oil and gas industry, and software vendors. Most important, they think strategically about practical problems and devise tools and technologies to help mitigate threats to the nation's information infrastructure.

Barry Horowitz, professor of systems and information engineering at the University of Virginia and team leader for the I3P "Business Rationale" project.

OUTREACH AND EDUCATION

The I3P plays an important role in outreach and education, with a strong track record of hosting workshops and training the next-generation of cyber security experts.

Workshops

The I3P offers hands-on workshops for representatives from industry, government and research institutions. These events focus on emerging cyber threats and on the practical sides of risk management, including security tools and mitigation techniques.

Fellowship Program

The I3P sponsors a fellowship program for post-doctoral researchers, junior faculty and young research scientists, thus contributing to the growth in cyber security research. The fellows, who are selected by a competitive process, must conduct their research at an I3P member institution.

ORGANIZATION

Managed by Dartmouth College, the I3P's administrative offices are located in Hanover, New Hampshire, where the I3P Chair and other professional staff members oversee the consortium's primary operations. An executive committee, comprised of senior representatives from member institutions, provides direction and guidance to the Chair. Membership is limited and applications are subjected to a rigorous selection process.

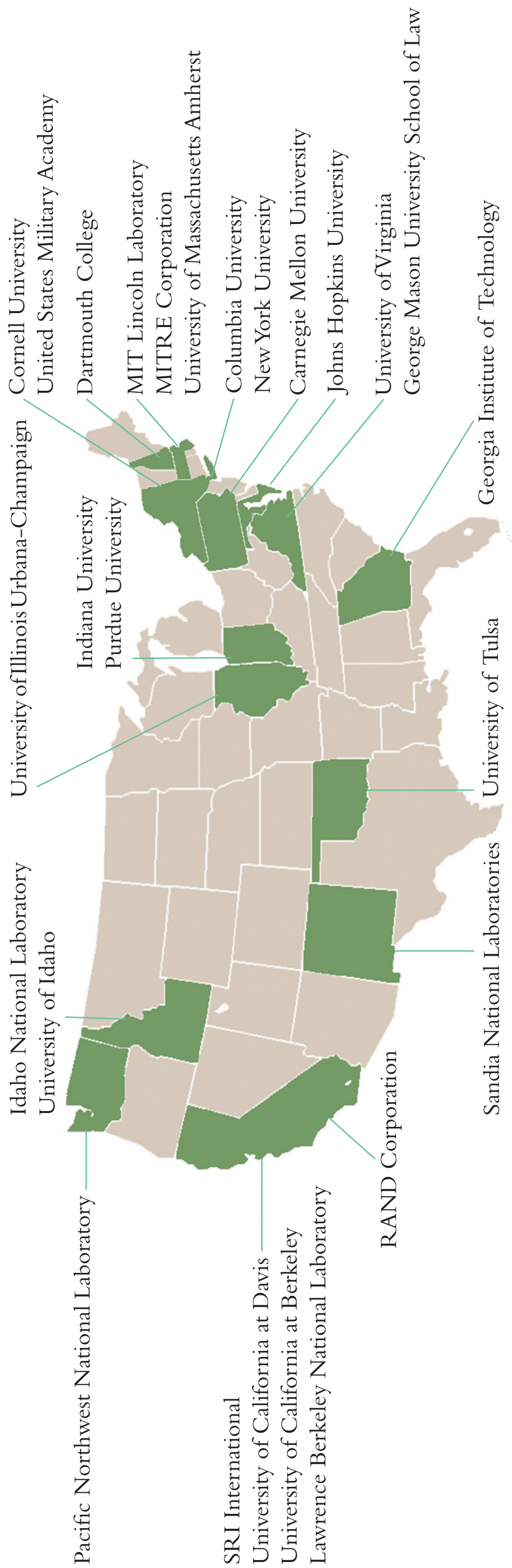
Baker Tower at Dartmouth College

HISTORY

In 1998, the U.S. President's Committee of Advisors on Science and Technology (PCAST) recommended that a non-governmental organization be formed to address national cyber security issues. Subsequent studies by the Institute for Defense Analysis and the National Security Council, as well as a White Paper produced by the Office of Science and Technology Policy, agreed with the PCAST assessment, affirming the need for an organization dedicated to protecting the nation's critical infrastructures. In 2002, the I3P was founded at Dartmouth College with funding from the federal government. Current financial support for the I3P comes from the Department of Homeland Security and the National Institute of Standards and Technology.

A NATIONAL RESOURCE

The multi-disciplinary, multi-institutional I3P represents a unique intellectual resource. In addition to guiding and supporting critical cyber security research, the I3P is committed to finding solutions to infrastructure vulnerabilities, facilitating technology transfer and forging effective alliances with key stakeholders.


Pacific Northwest National Laboratory
SRI International
University of California at Davis
University of California at Berkeley
Lawrence Berkeley National Laboratory
RAND Corporation
Idaho National Laboratory
University of Idaho
Sandia National Laboratories
University of Illinois Urbana-Champaign
Indiana University
Purdue University
University of Tulsa
Cornell University
United States Military Academy
Dartmouth College
MIT Lincoln Laboratory
MITRE Corporation
University of Massachusetts Amherst
Columbia University
New York University
Carnegie Mellon University
Johns Hopkins University
University of Virginia
George Mason University School of Law
Georgia Institute of Technology

The work of the I3P is supported by the U.S. Department of Homeland Security and the National Institute for Standards and Technology. The I3P is managed by Dartmouth College.

A LEADER IN CYBER SECURITY

I3P

Institute for Information Infrastructure Protection

A consortium of leading universities, national laboratories and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States

The I3P is managed by Dartmouth College