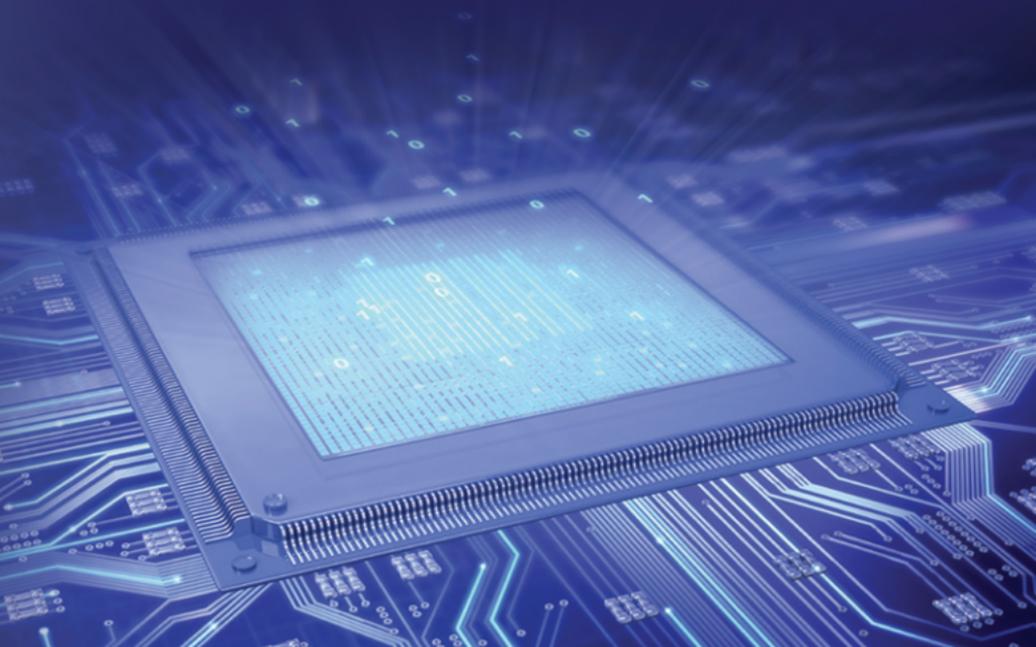


Director of Science and Technology
Office of the Director of National Intelligence

Intelligence Community

High Priority Technology Needs

June 2008



May 19, 2008

The Intelligence Community is composed of 16 different intelligence agencies and elements, plus the Office of the DNI, and almost all have Science and Technology activities dedicated to their specific mission-sets. One of the remarkable developments of the past few years is the increased communication across agency boundaries that has allowed the S&T Enterprise to create a community-wide collection of technology needs.

This booklet is a summary of areas we feel are in need of a new and different effort. We typically discuss our needs in classified forums with traditional partners, but we are providing this at an unclassified level to create opportunities for new ideas and new partnerships with industry, academia, and other innovators who can contribute to US national security.

Our hope is that the simple and broad discussion here brings inspiration from new viewpoints. We look forward to hearing from you.

Steve Nixon
Office of the Director of National Intelligence
Director of Science and Technology

“Capability to detect, locate and identify Weapons of Mass Destruction”

Representative Technology Needs

Capability to detect, locate and identify Weapons of Mass Destruction-related production and weapons or devices at stand-off distances.

A new generation of scalable-size sensors that can access intelligence targets in any environment.

Capability to exploit all data types associated with emerging and future broadband, mobile-communications systems.

New sensors, techniques, and tools to detect, deter and defeat denial and deception efforts.

Capability to exploit computer networks in the face of sophisticated protection schemes.

“Provide users easy access to data and information”

Representative Technology Needs

New solutions for collaborative analysis and information sharing that:

Interconnect between/among networks of varying security levels

Provide users easy access to data and information

Allow for multiple collaborative approaches, and protect privacy rights

A new generation of capabilities that will allow Intelligence Community personnel and assets to communicate securely and reliably.

“communicate securely and reliably”

“validation of human sources”

Representative Technology Needs

New techniques and tools that provide for the validation of human sources and the verification of their information.

New capabilities that will exploit both the offensive and defensive potential of biometrics.

“offensive and defensive potential of biometrics”

“employing improved search and machine reasoning techniques”

Representative Technology Needs

Tools and capabilities that ensure the information privacy and other legal rights of Americans within the context of the evolving Information Sharing Environment.

“Right to privacy.” Compliant capabilities that employ improved search and machine-reasoning techniques. Capabilities that can discover information in unstructured data by detecting hidden patterns or deviations, extracting key components and potential linkages, and transforming the data for further analysis, while preserving individual privacy.

Automated tools and techniques that support the collection and processing of open source intelligence information.

New Human-Language Technologies that can rapidly and automatically organize, catalog, translate and extract knowledge from foreign language information found in a variety of formats and media.

Technological solutions that would mark intelligence data with “life long” metadata tags that:

Propagate to any newly created or aggregated data that uses the marked data

Allows for updates, recall or correction of the original data and any derived products

Enables transition to new data marking processes and procedures, as appropriate.

“information that actively participates in ensuring its own security”

Representative Technology Needs

Advanced cryptographic algorithms that can resist attack by algorithms developed for quantum computers, and fast computing hardware that can rapidly encrypt, decrypt and transmit data utilizing these new algorithms.

“**Smart**” or **self-protecting** data (i.e. information that actively participates in ensuring its own security) that should know where it has been, who has seen and used it, and recognize when it is somewhere where it shouldn't be; it should be able to strip or otherwise protect sources and methods while retaining as much content—facts and conclusions—as possible.

“Automatically configure computer systems and networks”

Capabilities that:

Automatically configure computer systems and networks to balance functionality and security

Discover unexplained patterns of activity or anomalous events on networks and differentiate suspected, malicious activity from normal or unusual but acceptable behavior of authorized users

Provide accountability for malicious events (e.g. accessing and exfiltrating sensitive information)

Multi-level security capabilities that will process information with different classifications and categories while simultaneously permitting access by users with different security clearances and denying access to users who lack authorization.

Network access management solutions that absolutely identify and authenticate users.

“Exploration and evaluation of quantum computing”

Representative Technology Needs

Research focused on the development of innovative solutions to signals intelligence collection and information assurance problems posed by emerging technology.

Secure, high performance computing hardware, architectures, operating systems, programming languages, compilers, and measurement tools to enable current and future IC cryptanalysis and information assurance.

Exploration and evaluation of quantum computing.

Nanotechnology research focusing on the discovery and understanding of nanoscale and nanostructure materials and the fashioning of nanoscale devices and systems that will achieve improved performance or new functionality.

Improved chemical and biological forensic investigation capabilities.

“Reliable power solutions”

Discovery and improved understanding of phenomenology and related “signatures” associated with the most difficult targets and threats. .

Social and Human Sciences research that improves our understanding of the motivation and thought processes of potential adversaries.

Reliable power solutions for use in a range of challenging intelligence collection environments.



Director of Science and Technology
Office of the Director of National Intelligence
(703) 275-3311 or 3315