EMERGING SCIENCE AND TECHNOLOGIES:

Securing the Nation through Discovery and Innovation

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

COUNCIL ON TECHNOLOGY AND INNOVATION

APRIL 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **APR 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Emerging Science And Technologies: Securing The Nation Through Dicovery and Innovation**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Intelligence And National Security Alliance,901 North Stuart Street, Suite 205,Arlington,VA,22203**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

> If we want to make the best products, we also have to invest in the best ideas... Today our scientists are mapping the human brain to unlock the answers to Alzheimer's; developing drugs to regenerate damaged organs; devising new material to make batteries ten times more powerful...
>
>
>
> Now is the time to reach a level of research and development not seen since the height of the Space Race.

PRESIDENT BARACK OBAMA | 2013 STATE OF THE UNION

ACKNOWLEDGEMENTS

INSA CHAIRMAN

Ambassador John Negroponte

INSA SENIOR INTELLIGENCE ADVISOR

Charlie Allen

INSA STAFF

Ambassador Joseph DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Suzanne Wilson-Houck, *Vice President of Business Development*

Jeff Lavine, *Director of Administration & Management*

Joi Grieg, *INSA Senior Fellow*

Matthew French, *INSA Intern*

Kevin Paulson, *INSA Intern*

INSA COUNCIL ON TECHNOLOGY AND INNOVATION CHAIR

Dr. Robert Farrell, *Seneca Technology Group*

LEAD WRITERS

Dr. Allan Sonsteby, *Penn State University*

Maureen McGovern, *Microsoft Corporation*

TECHNICAL REVIEWERS

Lars P. Hanson

Gene Keselman, *Mission Sync, LLC*

Scott Lawler, *Lightspeed Technologies, Inc.*

Brian Morra, *Northrop Grumman Corporation*

EDITORIAL REVIEW

Joe Mazzafro, *CSC*

COPY EDITOR

Elizabeth Finan

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.

"Our national security requires the best possible intelligence, and the best possible intelligence benefits tremendously from the best possible science. It demands it! We must get this message across."

– DR. SIDNEY D. DRELL (2001 INSA WILLIAM OLIVER BAKER AWARD RECIPIENT)[1]

EXECUTIVE SUMMARY

Science, innovation, and discovery have enabled the U.S. to maintain an intelligence advantage over our adversaries. Investment in fundamental science and discovery is integral to economic growth and development as well as to national security.

Other nations, recognizing that investment in science, innovation, and discovery is a required element of economic prosperity (and therefore national security), have increased their commitment to basic research, while U.S. investment in fundamental research, which includes basic and applied research, has declined. While the U.S. continues to maintain a position of leadership in science and technology (S&T), it has experienced a gradual erosion of position with respect to the rest of the world in many areas. This erosion is largely the result of the rapid increase in Asian S&T investment and the results of the European Union's efforts to boost its relative competitiveness in research and development (R&D), innovation, and high technology.

It is clear there are evolving challenges to our nation's leadership in the realm of R&D. The U.S. government has played a pivotal role throughout our history in advancing our nation's technological capabilities, which have also spurred economic growth and development as well as ensured and enhanced our national security. While there may be fiscal challenges in the years ahead, it is also clear that continued advocacy from across government, including from the Intelligence Community (IC), is essential to encourage robust R&D activities, particularly with regard to basic research, which will maintain and enhance our national security. The IC should increase its overall emphasis on S&T and better leverage the funding currently available within the IC and extended federal government research enterprise in order to:

- Develop the generation after next capabilities to collect and assess intelligence data from increasingly sophisticated adversaries and rich new sources of information
- Avoid technological surprise[2] – particularly from those nations that are now investing heavily in the sciences
- Maintain and grow a technology-focused workforce for the IC, industry and academia

As a point of departure, the authors used the five high priority technology needs identified by the ODNI in 2008 – Technical Collection; Communications and Sharing Intelligence; HUMINT – Collection and Operations; Intelligence Analysis; and Protection of the Intelligence Enterprise – as an outline for this study. Based on reviews of appropriate literature, interviews, and surveys of industry, government officials, Federally Funded Research and Development Centers (FFRDCs), and academia, the authors of this paper identified several promising research areas relevant to these ODNI-identified capability gaps that may enable the U.S to better collect and assess intelligence and avoid technological surprise. These include:

- Bio-inspired computing architectures
- Energy harvesting
- Advanced materials for computing
- Human-inspired big-data processing
- Self-protecting data

> While the U.S. continues to maintain a position of leadership in science and technology, it has experienced a gradual erosion of position with respect to the rest of the world in many areas.

A full list of recommended areas for additional research interest and investment is included at the end of this paper. The research areas described in this paper are not meant to be all-inclusive nor prioritized; they should serve as a catalyst for discussion of topical scientific research areas for investment by the IC as well as an increased focus on the long-term value of basic research for the nation.

INTRODUCTION

The mission of the U.S. IC is unique. The IC is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to produce the intelligence necessary to conduct foreign relations and national security activities.

The primary mission of the IC is to collect, analyze, and convey the essential information that the President and members of the policymaking, law enforcement, and military communities require to execute their duties and responsibilities. Members of the IC collect and assess information regarding international terrorist and narcotic activities; hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States. As needed, the President also may direct the IC to carry out special activities in order to protect U.S. security interests against foreign threats.[3]

> Using science and technology to maintain an intelligence advantage over our adversaries has been a core principle of American national defense for much of our history.

The ODNI identified the following five high-priority technology needs:[4]

- Technical Collection
- Communications and Sharing Intelligence
- HUMINT – Collection and Operations
- Intelligence Analysis
- Protection of the Intelligence Enterprise

Using these high priority technology needs as an outline, the authors of this paper sought additional input from industry, academia, and government through interviews and a survey discussed in the Appendix to identify specific research areas that demonstrated great promise to meet some of these high priority IC requirements.

Critical to enabling revolutionary advances in these areas are fundamental science, innovation, and discovery, as was demonstrated during World War II. Basic research led to the rapid development of the atomic bomb, radar and sonar systems, nylon for parachute use, and penicillin that saved battlefield lives. Throughout the Cold War, the United States relied on its technological edge to offset the larger forces of its adversaries. More recently, fundamental research has resulted in the development of transformational technologies enabling supercomputers and large-data processing strategies that allow intelligence analysts to rapidly mine vast amounts of data.

In 1945 Vannevar Bush (an American engineer, inventor, and science administrator known for his work on analog computers, initiating and administering the Manhattan Project, and founding what was to later become Raytheon) espoused the critical close linkage between research and national security in "Science: The Endless Frontier."[5] In the closing paragraph of his letter of transmittal to President Roosevelt, Bush stated, *"The pioneer spirit is still vigorous within this nation. Science offers a largely unexplored hinterland for the pioneer who has the tools for his task. The rewards of such exploration both for the Nation and the individual are great. Scientific progress is one essential key to our security as a nation, to our better health, to more jobs, to a higher standard of living, and to our cultural progress."*

Half a century later, the Hart-Rudman Commission concluded:

> *In particular, we need to fund more basic research and technology development. As is clear to all, private sector R&D investments in the United States have increased vastly in recent years. That is good, but private R&D tends to be more development-oriented than research-oriented. It is from investment in basic science, however, that the most valuable long-run dividends are realized. The government has a critical role to play in this regard, as the "spinoff" achievements of the space program over the years illustrate. That role remains not least because our basic and applied research efforts in areas of critical national interest will not be pursued by a civil sector that emphasizes short- to mid-term return on investment.*[6]

The return on scientific investment funding and the significant contribution to national security is clear when one considers that whole industries have been created from such research, including:

- Mass production of steel
- Aviation
- Nuclear power
- Global Positioning System (GPS)
- The Internet

Indeed today, fundamental science and discovery are crucial to the national security and economic competitiveness of the United States. In particular, using S&T to maintain an intelligence advantage over our adversaries has been a core principle of American national defense for much of our history. The inclusion of this principle in the National Security Act of 1947 emphasizes its importance.[7]

With the pressures on industry and academia, self-funding for this critical fundamental S&T is endangered. Industry indicates that the competitiveness of rates has potentially reduced Independent Research and Development (IRAD), particularly at the basic research level. Increased competitiveness for CRAD (Contracted Research and Development), a more constrained Bid and Proposal environment, and decreased available funding for basic research are likely constraining the defense and aerospace sectors in the applied areas of the R&D spectrum. Even with these challenges, there are some indications that U.S. industry has increased efforts at the applied and development end of the R&D spectrum.

The purpose of this white paper is to discuss recent global innovation trends as well as identify fundamental areas of scientific research that have the potential to provide revolutionary advances to our nation's intelligence capabilities.

It should be stressed that the research areas described in this paper are not meant to be all-inclusive. Instead, these ideas should serve as a catalyst for discussion of topical scientific research areas for investment by the IC, an increased focus on the long-term national value of basic research, and the development of a skilled work force for the IC, industry and national research enterprise.

GLOBAL INNOVATION TRENDS

As the following discussion will show, other nations undoubtedly realize the significant value of investment in fundamental science and discovery to national security. It is instructive to compare various nations' commitments to investments in innovation on a global scale.

The U.S. has experienced a decline of position with respect to the rest of the world in many areas.

The National Science Board is required to prepare and transmit science and engineering indicators to the President and to the Congress every even-numbered year.[8] Indicators – quantitative representations – seek to capture the scope, quality, and vitality of the global science and engineering enterprise as well as contribute to the understanding of the current science and engineering environment. The 2012 Science and Engineering Indicators report provides insight into global innovation trends. The nine charts on the following pages are extracted and reproduced from this report.[9]

With respect to the impact on national security, it is useful to examine the following:

- Major global S&T trends
- U.S. R&D
- Global and U.S. scientific work force

Governments in many parts of the developing world, viewing S&T as integral to growth, development, and national security, have taken steps to develop their S&T infrastructures, stimulate industrial R&D, expand their higher education systems, and build indigenous R&D capabilities. In the last decade, global S&T capabilities have grown – nowhere more than in Asia.

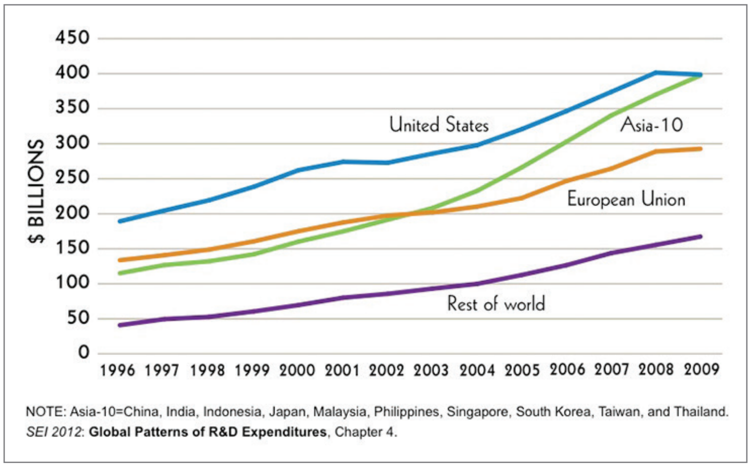
Asia's rapid ascent as a major world S&T center is chiefly driven by developments in China; however, the Asia-8 economies (India, Indonesia, Malaysia, the Philippines, Singapore, South Korea, Taiwan, and Thailand) also have played a role.

The U.S. has experienced a decline of position with respect to the rest of the world in many areas. The National Science Foundation states in their *Science and Engineering Indicators 2012*, "Two contributing developments to this erosion are the rapid increase in a broad range of Asian S&T capabilities outside of Japan and the effects of EU efforts to boost its relative competitiveness in R&D, innovation, and high technology."[10]

U.S. R&D expenditures accounted for about 31% of the worldwide total as shown in Figure 1. The combined R&D expenditures of 10 Asian economies (China, India, Indonesia, Japan, Malaysia, Singapore, South Korea, Taiwan, Thailand, Vietnam) rose steadily to reach U.S. levels in 2009, driven mostly by China, which now has the world's second largest R&D investments.

In the face of adverse economic conditions, the R&D growth of Western and other countries slowed markedly after 2008, as shown in Figure 2. Singapore and Japan experienced especially sharp contractions. After accounting for inflation, R&D growth for both the United States and the European Union was negative. In contrast, China's R&D expenditures increased by 28% in 2009. Rapid Asian growth in R&D investment reflects spending by domestic and private firms and increased public R&D spending that is often focused on sectors deemed to be of strategic importance.

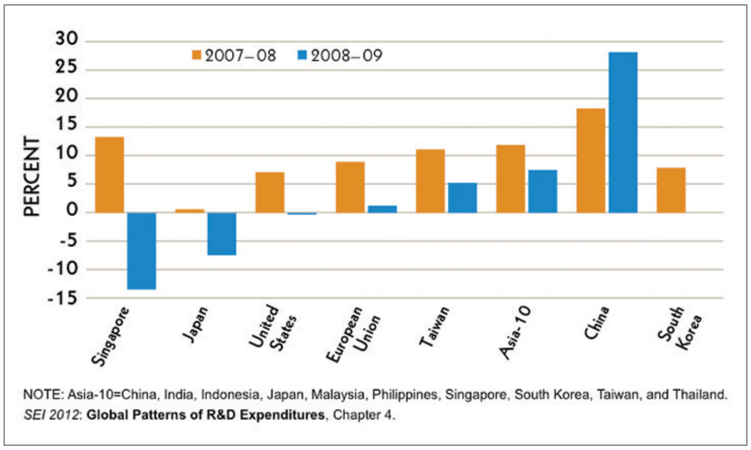
R&D EXPENDITURES FOR THE UNITED STATES, EUROPEAN UNION, AND ASIA-10 ECONOMIES: 1996-2009[11]



NOTE: Asia-10=China, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, and Thailand.
SEI 2012: **Global Patterns of R&D Expenditures**, Chapter 4.

Figure 1

AVERAGE ANNUAL GROWTH OF R&D EXPENDITURES FOR UNITED STATES, EUROPEAN UNION, AND ASIA-10 ECONOMIES: 2007-08 AND 2008-09[12]



NOTE: Asia-10=China, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, and Thailand.
SEI 2012: **Global Patterns of R&D Expenditures**, Chapter 4.

Figure 2

FEDERAL INVESTMENT TRENDS

The U.S. Office of Management and Budget (OMB) defines R&D for all federal agencies as follows:

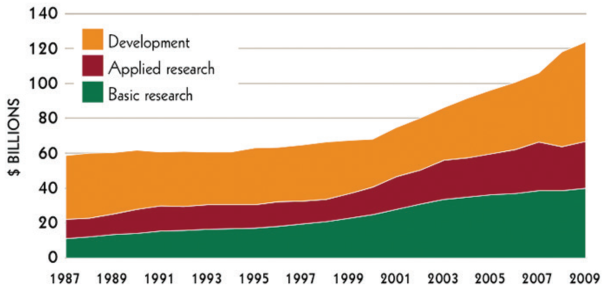
> *Research and development (R&D) activities comprise creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications.*[13]

Furthermore, federal R&D is categorized as basic research, applied research, or development.

> *Basic research is defined as systematic study directed toward fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind. Basic research, however, may include activities with broad applications in mind.*
>
> *Applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.*
>
> *Development is defined as systematic application of knowledge or understanding, directed toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes to meet specific requirements.*[14]

Federal funding for R&D has more than doubled over the last two decades (not adjusted for inflation). For the past decade, basic and applied research funds have accounted for more than half the total. However, federal stimulus funds for R&D have primarily boosted development activities. Federal R&D spending by type of R&D (basic, applied, development) from 1987-2009 is shown in Figure 3. The average annual real growth rate (adjusted for inflation) for federal R&D spending is shown in Figure 4. The trend for national R&D has shifted away from basic research to development.

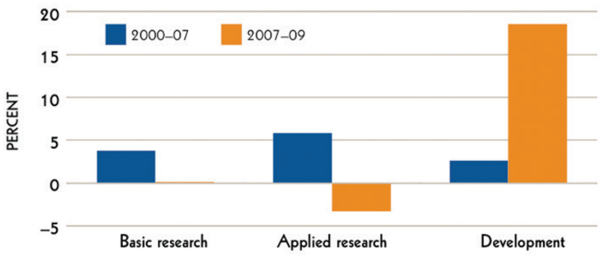
FEDERAL R&D FUNDS, BY CLASSIFICATION OF R&D TYPE: 1987-2009[15]



NOTE: 2009 data are preliminary.
SEI 2012: **R&D by Character of Work**, Chapter 4.

Figure 3

AVERAGE ANNUAL REAL GROWTH OF FEDERAL SUPPORT FOR R&D, BY CLASSIFICATION OF R&D TYPE: 2000-07 AND 2007-09[16]



NOTE: 2009 data are preliminary.
SEI 2012: **R&D by Character of Work**, Chapter 4.

Figure 4

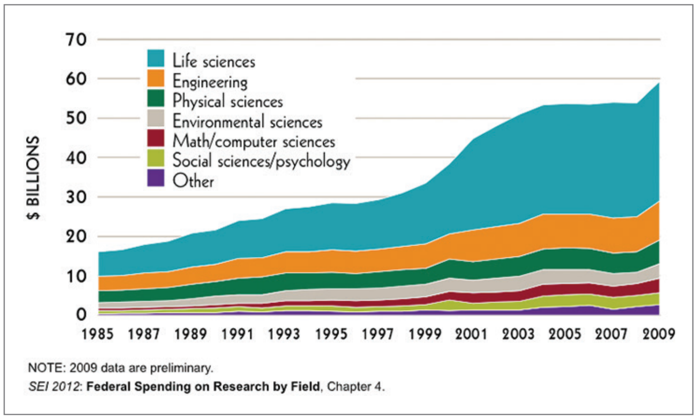
Federal R&D funding is further classified by the science and engineering (S&E) field. Federal basic and applied research funding by the S&E field from 1985-2009 is shown in Figure 5. The life sciences have accounted for half of the federal research portfolio (basic and applied research) since 2001. Over the past decade, federal research funds for the life sciences and math/computer sciences have increased by more than one-third (after inflation); engineering funds rose by one quarter. As shown in Figure 6, inflation-adjusted federal spending over the decade was flat for the physical sciences and shrank for environmental sciences, social sciences, and psychology.

More than half of the federal government's R&D investment is devoted to defense as shown in Figure 7. Considering Department of Defense (DoD) actual R&D funding obligations for 2009 were $68.2B, relatively small amounts were spent on basic research ($1.7B, 3%) and applied research ($5.1B, 7%). The vast majority of obligations ($61.3B, 90%) went to development.[18]

The U.S. IC does not publish the amount of funding allocated to basic research; however, to some extent the IC is able to leverage the basic research funded in support of defense and other national objectives. Unfortunately, as the data in Figures 3 and 4 illustrate, the R&D funding focus has been in the development category, and there has been negligible and negative growth in the categories of basic and applied research, respectively. It is likely that the IC funding trends for basic and applied research follow trends similar to those of the DoD.

The declining investment in basic and applied research by the IC, DoD, and the nation as a whole will have a detrimental effect on the development of future capabilities. In addition, the lack of investment in basic research will affect the number of graduate students focusing in areas relevant to national security, and consequently, the pool of qualified scientists and engineers available for hiring by IC, DoD, and industry will be reduced.

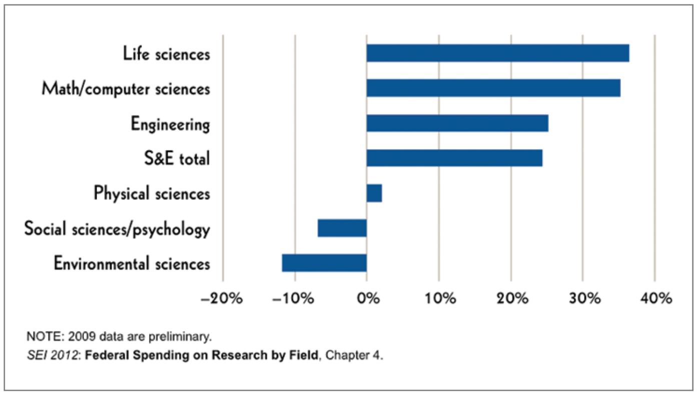
FEDERAL BASIC AND APPLIED R&D FUNDS, BY S&E FIELD: 1985-2009[17]



NOTE: 2009 data are preliminary.
SEI 2012: **Federal Spending on Research by Field**, Chapter 4.

Figure 5

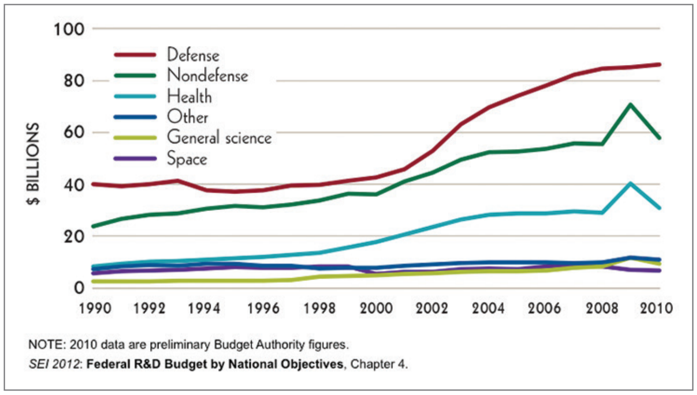
INFLATION-ADJUSTED INCREASE IN FEDERAL RESEARCH FUNDS, BY S&E FIELD: 2000-2009[19]



NOTE: 2009 data are preliminary.
SEI 2012: **Federal Spending on Research by Field**, Chapter 4.

Figure 6

FEDERAL R&D BUDGET, BY NATIONAL OBJECTIVES: 1990-2010[20]



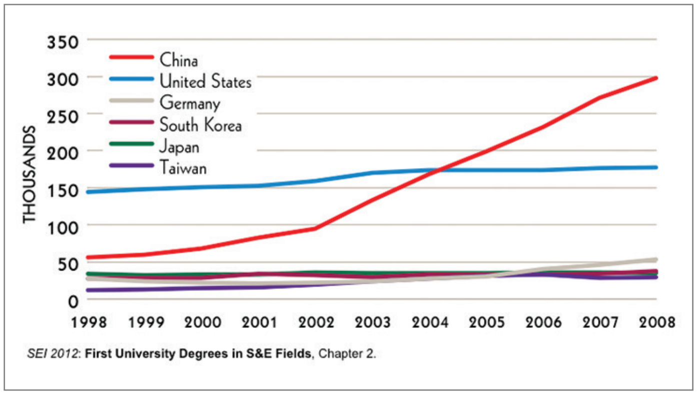
NOTE: 2010 data are preliminary Budget Authority figures.
SEI 2012: **Federal R&D Budget by National Objectives**, Chapter 4.

Figure 7

Education at all levels in science, technology, engineering and mathematics (STEM) develops, preserves and disseminates knowledge and skills which convey personal, economic and social benefits as well as work force development for the IC, DoD, and supporting industry. One measure of national commitment to developing and maintaining a vibrant R&D enterprise is the number of university degrees awarded in science and engineering. Figure 8 shows the number of first university degrees (baccalaureate) awarded in engineering fields in selected countries/ economies. An indirect measure of national commitment to funding basic research is the number of doctoral degrees awarded in science and engineering. Figure 9 shows the number of doctoral degrees awarded in natural sciences and engineering by selected country/ economy.

The declining investment in basic and applied research by the IC, DoD and the nation as a whole will have a detrimental effect on the development of future capabilities.

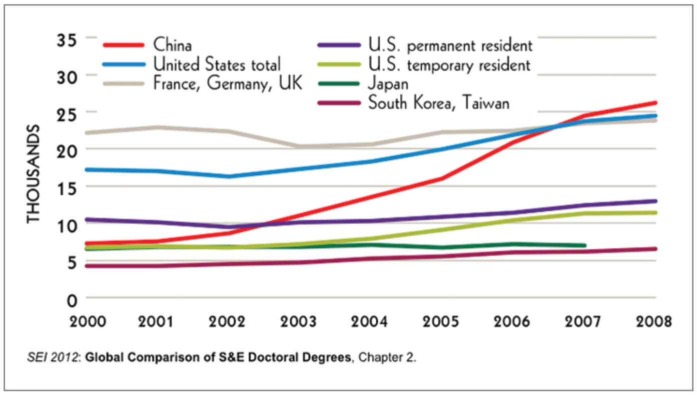
FIRST UNIVERSITY DEGREES IN ENGINEERING, SELECTED COUNTRIES/ECONOMIES: 2000-2008[21]



SEI 2012: **First University Degrees in S&E Fields**, Chapter 2.

Figure 8

DOCTORAL DEGREES IN NATURAL SCIENCES AND ENGINEERING, SELECTED COUNTRY/ECONOMY: 2000-2008[22]



SEI 2012: **Global Comparison of S&E Doctoral Degrees**, Chapter 2.

Figure 9

SCIENCE TO ENABLE OR ACCELERATE IC CAPABILITIES

As discussed earlier, the ODNI published a summary of high priority technology needs – areas where fundamental science, innovation, and discovery could enable development of revolutionary capabilities for the IC. This section describes the five published technology needs and identifies fundamental research areas that are likely to significantly advance our capabilities as identified by the collective group developing this paper and the INSA survey conducted.

> These new means may reduce the need for the range of expensive collection tools that U.S. agencies once had as their specialty and comparative advantage.

TECHNICAL COLLECTION

Technical Collection refers to the need for a new generation of sensors to support the broad intelligence collection requirements of the IC.

Sensors

- To detect, locate, and identify weapons of mass destruction (WMD) and related production capabilities at a variety of stand-off distances.
- To sense a variety of human, animal, and plant biological signatures – both from within the host as well as from a distance.
- Immune to denial and deception tactics and techniques that our adversaries frequently employ.
- To perform reliably and survive in the harshest environments – from the depths of the ocean to the farthest reach of the universe and everything in between.

Also of great interest are sensors that have no physical dimension – sensors which exist only in cyberspace – virtual worlds and to other digital domains.

Energy Harvesting

Fundamental to the development of any sensor is energy – how will the sensor be powered? While research in the battery chemistry area continues to evolve, energy harvesting techniques show promise to power the sensors of tomorrow.

Energy harvesting is the process for collecting energy from the surrounding environment and converting it to electricity or other useful form. Energy harvesting methods convert ambient energy in the form of light, vibration, heat, and radio waves into electricity – potentially negating the need for batteries. The ability to efficiently harvest energy from its environment – whether deep in the ocean, within the human body, or orbiting in space – is required for the development of revolutionary sensing capabilities.

Bio-mimicry

Bio-mimicry is a relatively new discipline, which studies nature's best ideas and then imitates these designs and processes. The core idea is that nature, imaginative by necessity, has already solved many of the complex sensing issues confronting the IC. Animals, plants, and microbes are the consummate engineers – they have found what works, what is appropriate, and, most importantly, what best performs the desired function to ensure survival. After 3.8 billion years of R&D, failures are fossils, and what remains has adapted to survive.

Many examples exist of replicating biological systems to perform a specific function by harnessing nature's evolutionary designs, for example: the artificial canine nose for detection of single molecules, adaptable wings on airplanes, and scale-like coatings on undersea vehicles. It is likely that one of the next great fields of transformative research to revolutionize sensing capabilities lies at the boundaries of life sciences, physical sciences, and engineering.

The Internet of Nature

Experiments have shown that plants have a form of awareness and ability to communicate with other plants. For example, in a forest, if one tree is cut or chopped down, there is evidence that the tree experiences a type of "stress" which is communicated to other nearby trees. Similarly, animals can sense changes in weather or environmental conditions. It may be possible to consider the use of plants and animals as a sort of "sensing network" for understanding an environment and detection of environmental changes. One could envision a kind of "internet of nature" (analogous to the "internet of things" in which inanimate objects have embedded sensors, processors, and communication devices connected to the internet), for monitoring areas of interest to develop a situational awareness and detection of anomalies.

> It is likely that one of the next great fields of transformative research to revolutionize sensing capabilities lies at the boundaries of life sciences, physical sciences and engineering.

COMMUNICATIONS AND SHARING INTELLIGENCE

Communications and Sharing Intelligence refers to capabilities that will allow IC personnel and assets to communicate securely and reliably and to provide users easy access to data and information. This includes providing environments for collaborative analysis and information sharing between networks and users at varying security levels.

Swarm Technologies and Communications

Swarm technologies could enable large numbers of simple assets or devices to collaborate in various tasks such as intelligence gathering, analysis protection, and offensive actions. Communications between individual active elements need to be simple and secure. The entire swarm needs to be controllable and failsafe. Research in this area could open up significant discriminating capabilities in a variety of practical applications. For example, a swarm of small sensors could provide high fidelity information about a specific area. Different types of sensors could support various frequency bands such as visual, infrared, audio, radio-frequency, physical-vibration, etc. Working collectively, a swarm of miniature collaborative devices could accomplish tasks such as infiltrating a facility or identifying and disabling specific types of equipment.

Holographic Telepresence

Present collaborative technology solutions include standard video-teleconference systems (e.g., Tandberg) as well as immersive visualization systems using avatars. The ultimate telepresence system will likely be capable of rendering life-size, full-color, high-definition, holographic three-dimensional images and will be able to interact with all of our senses – sight, sound, touch, smell, and taste. Research in photorefractive polymer film fabrication with rapid refresh rates is one area necessary for revolutionary advancement before a holographic telepresence system can be realized

Advanced Materials for Computing

Since the 1950s, silicon has been the preferred medium of computing circuitry. While transistor density has continued to increase according to Moore's law, the technology is beginning to reveal its limitations, resulting in increased heat and energy consumption to achieve more computing power. When silicon reaches its ultimate limits in miniaturization and speed, which some believe could occur within the next decade, something must be ready to take its place. Carbon-based electronics, such as graphene or carbon nanotubes, may be a promising successor.

Graphene is a single layer of carbon atoms tightly packed into a two-dimensional honeycomb lattice. Graphene is part of the family of atomic "nano-carbons" that includes carbon nanotubes and buckyballs, and is a single or a few atomic layers of the three-dimensional material graphite. Graphene is being most widely studied for its remarkable electronic transport properties at room temperature for ballistic transistors and other high-speed electronic components. Silicon's mobility (the speed at which an electron can travel through the material) limits current computers to gigahertz speeds. Graphene's speed limit has the potential to enable terahertz computing, 100 to 1000 times faster than silicon. Graphene has also been suggested as a potential material for use in quantum computing and spintronics.

> R & D in the area of advanced carbon-based materials has the potential to revolutionize the capabilities of the intelligence community by enabling terahertz computing and re-setting Moore's law with a new class of electronic devices.

R&D in the area of advanced carbon-based materials has the potential to revolutionize the IC's capabilities by enabling terahertz computing and re-setting Moore's law with a new class of electronic devices.

Bio-inspired Computing

Biochemical "nano computers" already exist in nature; they are manifest in all living things. DNA simulates software and enzymes simulate hardware. When they are put together in a test tube, the way in which these molecules undergo chemical reactions with each other allows simple operations to be performed as a byproduct of the reactions. Researchers tell the devices what to do by controlling the composition of the DNA software molecules – a completely different approach than electrons moving through silicon as in a conventional computer. There is no mechanical device. A trillion bio-molecular devices could fit into a single drop of water. Instead of showing up on a computer screen, results are analyzed using a technique that allows scientists to see the length of the DNA output molecule. Bio-inspired computing will also enable development of new classes of programming and analysis techniques. Silicon-based computing relies on a binary system of zeros and ones, whereas a DNA-based computer relies on four nucleic acid bases (adenosine and thymine, guanine and cytosine – A, T, G, and C) which provide the potential to deal with "fuzzy" data – going beyond digital data.

Fundamental research in the areas of bio-inspired computing has the potential to significantly improve the computation and analysis capabilities of the IC through the development of DNA-based computing systems or hybrid systems consisting of silicon or carbon based technologies combined with bio-inspired co-processors developed for specific tasks.

HUMINT COLLECTIONS AND OPERATIONS

HUMINT Collections and Operations refers to the overall process of gathering intelligence by means of interpersonal contact, as opposed to more technical intelligence gathering disciplines such as signals intelligence (SIGINT) or imagery intelligence (IMINT).[23] Successful HUMINT collection and operations face challenges on many levels, including identification and validation of candidate assets for recruitment, continual vetting of existing assets and data, successful evasion of counterintelligence activities (tradecraft), and the establishment and operation of covert communication channels. In addition, the potential offensive and defensive uses of biometrics are of interest.

Though fundamental science and discovery are not typically associated with supporting HUMINT collection and operations, advances in the research areas described below could greatly facilitate this field.

Big Data Knowledge Discovery for Asset Identification

The big data phenomenon refers to the practice of collecting and processing very large data sets (structured and unstructured) and to the associated systems and algorithms used to analyze these massive datasets. "IBM estimates that every day, 2.5 quintillion bytes (exabytes) of data are created – so much that 90% of the data in the world today has been created in the last two years."[24] The operational challenges of Big Data include data capture, storage, search, sharing, analysis, and visualization.

Though big data currently is receiving significant investment from both the private and government sectors, opportunities exist to leverage this investment and supplement it with research focused on the HUMINT mission such as asset identification – research into strategies for mining large data sets to identify candidate assets for recruitment.

Countering Asymmetric ISR for HUMINT Signature Reduction

The proliferation of smart mobile devices, access to commercial satellite imagery, publicly available persistent surveillance information (e.g., via video surveillance cameras) as well as cyber open-source analysis leads to the opportunity for asymmetric intelligence, surveillance, and reconnaissance (ISR). Virtually any small team or adversarial counter intelligence activity can obtain ISR using these readily available resources that likely rival our own ISR capabilities. The development of behavioral models, and associated anomaly detection methodologies, from the perspective of asymmetric ISR, could significantly reduce the signature of HUMINT activities and enhance their effectiveness.

Behavioral Biometrics

Broadly speaking, there are two types of biometrics: physical and behavioral. Physical biometrics comprises unique biological and physiological characteristics, including the voice, face, fingerprint, iris, and retina. Physical biometric systems that recognize the voice, face, iris, retina, or fingerprint are well known and widely used. In contrast, behavioral biometrics focuses on unique behavioral and psychological characteristics, including the way one uses a keyboard or records one's signature.

Behavioral biometrics combines physical biometrics with behavior models and can be used to aid in identification or detection of deceptive intent. Examples of some early research in this area examined the walking gait of an individual to detect deception. Other research has examined subtle facial changes such as temperature gradients in response to overt and subliminal messaging. The area of behavioral biometrics has the potential to provide significant support to HUMINT operations in areas such as asset validation and estimation of intent.

Bacterial Steganography

Steganography is writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Countless techniques have been developed and are presently employed to support covert delivery of messages between assets. A relatively new area of science (sometimes referred to as InfoBiology) includes the encoding, transmission, and release of information using living organisms as carriers of data. Living systems also offer the possibility for timed release of information as features can take hours or days to develop. By choosing the bacterial strains, people could send messages that appear after specific periods of time, or slowly degenerate.

Research in the areas of bacterial steganography, or InfoBiology, could likely result in communication through compromised channels, asset vetting, and other key areas relevant to successful HUMINT operations.

INTELLIGENCE ANALYSIS

Intelligence Analysis is the process of taking available (yet possibly deceptive) information about situations and entities of strategic, operational, or tactical importance, then characterizing the known and (with appropriate statements of probability) the future actions in those situations and by those entities. It is generally accepted that today, the intelligence analysis process must cope with "too much" data. Intelligence sources include electronic signals, satellite imagery, moving-target data, full-motion video, HUMINT, as well as a plethora of open-source data. Some intelligence data are structured (e.g., ELINT, FISINT), some data are unstructured (e.g., full-motion video), some data are subjective (e.g., HUMINT) and some data are just misleading (incorrect data or deceptive data). The overarching objective for the analyst (or analysis system) is to characterize a scenario based on all of the available intelligence.

Consider the following from Dr. Richards J. Heuer:

> *How can intelligence analysis be improved? That is the challenge. A variety of traditional approaches are used in pursuing this goal: collecting more and better information for analysts to work with, changing the management of the analytical process, increasing the number of analysts, providing language and area studies to improve analysts' substantive expertise, revising employee selection and retention criteria, improving report-writing skills, fine-tuning the relationship between intelligence analysts and intelligence consumers, and modifying the types of analytical products.*
>
> *Any of these measures may play an important role, but analysis is, above all, a mental process. Traditionally, analysts at all levels devote little attention to improving how they think.* ***To penetrate the heart and soul of the problem of improving analysis, it is necessary to better understand, influence, and guide the mental processes of analysts themselves.***[25]

Research efforts to develop cognitive sciences are required to provide revolutionary advances in the discipline of intelligence analysis.

Research in the areas of bacterial steganography, or InfoBiology, could likely result in communication through compromised channels, asset vetting, and other key areas relevant to successful HUMINT operations.

Derivation of Knowledge from Data

Most data collection and sensing methods use physical sensors to collect signals, images, scalar, or vector data which "represent" some observed situation. While an enormous amount of research has been conducted in image and signal processing (e.g., transformation of signal and image data into feature vectors, state vectors or even entity labels), with subsequent data association and fusion, little attempt has been made to address the entire transformation of physical data into knowledge – such as the transformation of data into textual, context-grounded knowledge. Research to address the entire information inference chain from data to knowledge (e.g., via signal and image processing, feature extraction, natural language processing, semantic meta-data generation, context-based reasoning, and "storification" to present data more easily understood by a human analyst) would provide significant improvement to the human analyst.

Human-inspired Big Data Access Strategies

The increasingly huge volumes of intelligence data collected through persistent surveillance and other means provide a plethora of data which cannot be adequately processed quickly enough by a limited number of analysts. Humans face an analogous situation with their multiple senses. How does a human address the potential moment by moment sensory overload? Cognitive studies have provided some clues that seem to involve a dual-approach strategy. First, the vast majority of our sensory input information does not reach the level of consciousness. Rather, information achieves conscious recognition via an "alert" process (e.g., a bee sting would result in information being provided to the conscious brain, while ordinary sensations from the skin are not perceived). Second, the focus of attention by volition (e.g., the desire to pick up a pen) directs conscious feeling of one's fingertips, etc. This combination of "data-push alerting" and "attention-directed sensing" provides the means for humans to survive in the world without being overwhelmed by their senses. A fundamental investigation of this human cognitive/perceptual strategy could lead to new methods for addressing data overload in the IC. Similarly, studies related to cognitive issues such as synesthesia and attention deficit disorder could inform development of automated computing methods for improved focus of attention and anomaly detection.

Activity Based Intelligence and Predictive Analytics

Emerging Activity Based Intelligence (ABI) approaches are combing multi-INT sources into a fused view. However, due to its infancy, the analytic discipline lacks ability to pull knowledge from the vast volume of activity data available to analysts. Significant research is required into data fusion of dissimilar data types. Research is required for context-aware ABI to identify fusion and presentation approaches that are outside of traditional intelligence tradecraft.

A fundamental investigation of this human cognitive/perceptual strategy could lead to new methods for addressing data overload in the intelligence community.

PROTECTION OF THE INTELLIGENCE ENTERPRISE

The Protection of the Intelligence Enterprise area refers to capabilities that protect aspects of the IC infrastructure including capabilities which:

- Automatically configure computer systems and networks to balance the requirements for 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 extracting sensitive information)
- Multi-level security (MLS) capabilities which 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 to identify and authenticate users absolutely

Relevant technology areas that support Protection of the Intelligence Enterprise include:

Quantum Computing and Associated Technologies

This includes advanced cryptographic algorithms, which 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. Specifically, efforts should be focused on quantum key distribution (QKD). QKD uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. An important and unique property of quantum distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e., the eavesdropper has no information about), otherwise no secure key is possible and communication is aborted.

The security of quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional key distribution protocol that relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel.

Self-Protecting Data

Although computer networks have grown considerably more complex over the decades, current cyber security policies remain largely reactive. Approaches to protecting and controlling digital information effectively ignore its digital nature in order to reduce the problem to physical access, rather than exploiting that digital nature to create self-protective mechanisms. A key concept to be considered is data that can protect itself, or self-protecting data. That is, the data inherently contains the protection mechanisms needed to prevent or at least to detect compromise. One example of a self-protecting data application is to provide data sets with active, lifelike properties. These properties are analogous to DNA in biological systems and would serve to identify data sets to allow them to maintain information relating to identity, provenance and integrity. When these sets are combined, they would inherit the genetics of their parent data sets, enabling users to determine the ultimate origins of the information.

Data Authentication

A method to reduce the dependence on passive defense (e.g., firewalls) is to strengthen authentication technologies. For example, on-going research includes putting code inside data objects that would prevent two pieces of data from being combined into a third piece. Much classified information consists of data pieces that are not individually sensitive unless they are combined. Because of the government's worries about this information, the current state of data defense is preventing it from being combined by unauthorized parties. Methods such as applying biological techniques to data sets would prevent "mosaic" situations where unclassified data is combined to produce classified results. Because the data's origins are traceable through workflow or use, with the utilization of distributed data storage, it may be possible to re-create a data set from a single sample of its DNA. Such a capability would produce a living data set that would be self-organizing and able to recognize a user's right to access information in specific combinations.

Much classified information consists of data pieces that are not individually sensitive unless they are combined. Because of the government's worries about this information, the current state of data defense is preventing it from being combined by unauthorized parties.

SUMMARY AND RECOMMENDATIONS

Science, innovation, and discovery have enabled the U.S. to maintain an intelligence advantage over our adversaries. Investment in fundamental science and discovery is integral to economic growth and development as well as to national security. The U.S. government has had a pivotal role in advancing our nation's capabilities which have supported economic growth and development as well as ensured our national security. While the U.S. continues to maintain a position of leadership in terms of broad R&D activities, our position is eroding as other nations (particularly China, now the second largest investor in R&D) take steps to develop their S&T infrastructure and invest in fundamental research.

Decreased emphasis in the U.S. on fundamental research, particularly in fields likely to enable national security capabilities, will have long-term negative effects on our nation including:

- Degradation of our ability to develop revolutionary capabilities to collect and assess intelligence data from increasingly sophisticated adversaries
- Susceptibility to technological surprise – particularly from those nations that are now investing heavily in the sciences
- Difficulty maintaining a technology focused workforce for the IC, industry, and academia

As part of a national strategy, greater emphasis should be placed on investment in fundamental science and discovery. For its role, the IC should make certain that its research portfolio is properly balanced across basic, applied, and development categories.

In the present fiscally restrained environment, basic research areas should be carefully coordinated within the IC and chosen to maximize the likelihood that they would ultimately result in capabilities that would adequately prepare the U.S. to face the long-term threat of adversary states and non-state actors. Positive outcomes of a robust basic research program with emphasis on long-term IC needs include:

- Developing of new science for transition into applied research programs
- Maintaining a national research enterprise that includes government, industry, and academia with a focus on the long-term needs of the IC
- Growing of a skilled work force with advanced science and engineering degrees in support of the IC and industry

Key stakeholders, including the IC, the government research enterprise, industry and academia, must coordinate efforts in support of diverse IC objectives.[26] The IC should increase emphasis in science, innovation and discovery activities through:

- Continued funding for basic research activities with the objective of developing science that will revolutionize the capabilities of the IC
- Increased coordination within the IC and across the national security enterprise to ensure that research efforts are coordinated and that programs are leveraged where possible
- Development of incentive strategies to encourage industry to invest in long-term basic research programs in areas relevant to the IC
- Support for processes that increase industry comfort with Intellectual Property (IP) protection for research programs
- Increased outreach and engagement with universities
- Increased educational outreach including:
    - Strengthening the workforce of the IC and supporting industrial base
    - Attracting and retaining students in science, technology, engineering and mathematics (STEM) disciplines with a focus on IC objectives

Continued government advocacy of these recommendations can sustain and enhance our nation's security.

Despite fiscal challenges in the years ahead, continued advocacy across government for R&D, including from the IC, is essential, particularly with regard to basic research, in order to maintain and enhance our national security and ensure our technological leadership.

In summary, listed below are the five ODNI identified high priority technological areas of need and associated research areas recommended by the authors to help satisfy those needs:

- Technological Area: Technical Collection Research Recommendations:
    - New Generation Sensors
    - Energy Harvesting
    - Bio-mimicry
    - The Internet of Nature
- Technological Area: Communications and Sharing Intelligence Research Recommendations:
    - Swarm Technologies and Communications
    - Holographic Telepresence
    - Advanced Materials for Computing
    - Bio-inspired Computing
- Technological Area: HUMINT Collections and Operations Research Recommendations:
    - Big Data Knowledge Discovery for Asset Identification
    - Countering Asymmetric ISR for HUMINT Signature Reduction
    - Behavioral Biometrics
    - Bacterial Steganography
- Technological Area: Intelligence Analysis Research Recommendations:
    - Derivation of Knowledge from Data
    - Human-inspired Big Data Access Strategies
    - Activity Based Intelligence and Predictive Analytics
- Technological Area: Protection of the Intelligence Enterprise Research Recommendations:
    - Quantum Computing and Associated Technologies
    - Self-Protecting Data
    - Data Authentication

We believe that additional interest and emphasis in these recommended research areas has the potential to revolutionize the intelligence capabilities of our nation and enhance U.S. leadership in S&T.

APPENDIX

In addition to the sources cited, a survey was conducted to identify S&T areas that may enable or accelerate developments that support increased capability and effectiveness and which might benefit from additional focus in the IC. It was distributed to INSA members, academia, and Federal Funded Research and Development Centers (FFRDCs). This survey was made available in October 2012, and input was collected through the end of November 2012. Specifically, the survey sought to identify S&T research activities that are critical enablers to the Intelligence Community.

With more than fifty respondents, the results corroborated the data obtained through other sources. Recipients indicated needs in big data, detection of weapons of mass destruction (WMD), increased investments in cyber technology, and the application of open source and social media intelligence.

Respondents indicated a need to develop knowledge that can lead to discovery and verification from big data. Specific areas noted that need additional research were human- and bio-inspired big data strategies and how to mine the data into useful information by using advanced algorithms, pattern detection, and predictive analytics. Additionally, respondents noted the need for research in advanced sensors and detecting WMD. The advancements in biometric security limit the access of human intelligence sources to restricted areas, particularly in identifying the location and scope of WMD facilities. Respondents indicated that research into sensors that can detect WMD from greater distances, differentiate between WMD facilities and facilities with similar characteristics, and be incorporated into an integrated collection system could address the needs in this area.

The survey also indicated a need for further research in areas of tactical intelligence and intelligence application. Social media and mobile networks offer insight into individual behavior and networks in real-time, which provides a valuable tactical advantage. While not an area of basic research, respondents indicated a need to better apply intelligence from open source and social media. The ability to analyze this information and particularly to infer intent and gather information into the nature of relationships was an area that had the potential for large intelligence benefits relative to the investment. Cyber security, including offensive and defensive capabilities, was identified as a vulnerability that, while already a significant R&D focus, warranted additional research as well.

[1] *A quote from Dr. Sidney D. Drell, 2013 winner of the National Medal of Science and Sr. Fellow Hoover Institution and Professor of Theoretical Physics (Emeritus) at Stanford's SLAC National Accelerator Laboratory, in Nuclear Weapons, Scientists, and the Post-Cold War Challenge, 2007, p. 37*

[2] *Technological surprise is sometime referred to as U3 (unwarned, unconventional and unexpected) capabilities.*

[3] *http://www.intelligence.gov*

[4] *Intelligence Community High Priority Technology Needs, Director of Science and Technology, Office of the Director of National Intelligence, June 2008.*

[5] *V. Bush. Science: The Endless Frontier. Washington, DC. U.S. Government Printing Office, 1945.*

[6] *U.S. Commission on National Security, "Road Map for National Security: Imperative for Change," Washington, DC. 2001. Page 32*

[7] *National Security Act of 1947, Public Law 253, 80th Congress, 1st Session, 1947*

[8] *National Science Foundation (NSF) Act, 42 U.S.C. § 1863 (j) (1)*

[9] *National Science Board. "Science and Engineering Indicators 2012." Arlington, VA: National Science Foundation (NSB 12-01).*

[10] *http://www.nsf.gov/statistics/seind12/c0/c0s1.htm; Paragraph 3*

[11] *http://www.nsf.gov/statistics/digest12/global.cfm#2*

[12] *http://www.nsf.gov/statistics/digest12/global.cfm#3*

[13] *"Preparation, Submission, and Execution of the Budget," OMB Circular A-11, August 2012. Page 11 of Section 84.*

[14] *OMB Circular No. A-11 (2010), Section 84, pg. 3*

[15] *http://www.nsf.gov/statistics/digest12/portfolio.cfm#1*

[16] *http://www.nsf.gov/statistics/digest12/portfolio.cfm#1*

[17] *http://www.nsf.gov/statistics/digest12/portfolio.cfm#2*

[18] *National Science Board. "Science and Engineering Indicators 2012." Arlington, VA: National Science Foundation (NSB 12-01). Table 4-16, Pages 4-31, 4-32.*

[19] *http://www.nsf.gov/statistics/digest12/portfolio.cfm#2*

[20] *http://www.nsf.gov/statistics/digest12/portfolio.cfm#3*

[21] *http://www.nsf.gov/statistics/digest12/stem.cfm#2*

[22] *http://www.nsf.gov/statistics/digest12/stem.cfm#4*

[23] *The FBI definition: "Human Intelligence (HUMINT) is the collection of information from human sources."*

[24] *Christopher Frank, "Improving Decision Making in the World of Big Data," Forbes, 25 March 2012. http://www.forbes.com/sites/christopherfrank/2012/03/25/improving- decision-making-in-the-world-of-big-data/*

[25] *Psychology of Intelligence Analysis, Richards J. Heuer, Jr., Center for the Study of Intelligence, Central Intelligence Agency, 1999.*

[26] *National Science Foundation, Defense Advanced Research Projects Agency, Intelligence Advanced Research Projects Activity, Office of Naval Research, Air Force Office of Scientific Research, Army Research Laboratory, U.S. National Laboratories, Federally Funded Research and Development Centers, and University Affiliated Research Centers.*

INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

ABOUT THE INSA COUNCIL ON TECHNOLOGY AND INNOVATION:

INSA's Council on Technology and Innovation is comprised of dedicated business and government professionals who are passionate about harnessing the power of emerging technologies and innovative ideas to solve U.S. national security problems. Through partnerships forged between the public, private, and academic sectors, the Council works to mobilize the nation's entrepreneurial resources for national security ends.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org