**DARPA and New Theory of Intelligence** [**http://bit.ly/pdTYP**](http://bit.ly/pdTYP)

Darpa’s latest venture, called “**Physical Intelligence” (PI)** is to prove, **mathematically**, that **the human mind** is nothing more than **parts and energy**. In other words, all brain activities — reasoning, emoting, processing sights and smells — derive from physical mechanisms at work, acting according to the principles of **“thermodynamics in open systems.”** Thermodynamics is founded on the conversion of energy into work and heat within a system (which could be anything from a test-tube solution to a planet). The processes can be summed up in formalized equations and laws, which are then used to describe how systems react to changes in their surroundings.

The ***military wanted a new equation: one that explains the human mind as a thermodynamic system.*** Once that’s done, they’re asking for **“abiotic, self-organizing electronic and chemical systems**” that **display the PI principles**. More than just computers that think**, Darpa wants to re-envision how thought works** — and then design computers whose thought processes are governed by the same laws as our own.

The **Physical Intelligence program** aspires to understand intelligence as a physical phenomenon and to make the first demonstration of the principle in electronic and chemical systems. **A central tenet is that intelligence spontaneously evolves as a consequence of thermodynamics in open systems**. The **program plan is organized around three interrelated task areas**:

(1**) creating a theory (a *mathematical* formalism) and validating it in natural and engineered systems;**

**(2) building the first human-engineered systems that display physical intelligence in the form of abiotic, self-organizing electronic and chemical systems; and**

**(3) developing analytical tools to support the design and understanding of physically intelligent systems.** If successful, the program would launch a revolution of understanding across many fields of human endeavor, demonstrate **the first intelligence engineered** from first principles, create new classes of electronic, computational, and chemical systems, and **create tools to *engineer* intelligent systems that match the problem/environment in which they will exist.** Concepts **relevant** to **the objectives** of the **Physical Intelligence program** can be found in numerous disciplines and areas of research including ***statistical physics, non-equilibrium thermodynamics, dissipative systems, group theory, collective behavior, complexity theory, consciousness theory, non-linear dynamical systems, complex adaptive systems, systems analysis, multi-scale modeling, control systems, information theory, computation theory, topology, electronics, evolutionary computation, cellular automata, artificial life, origin of life, microbiology, evolutionary biology, evolutionary chemistry, neuropsychology, neurophysiology, brain modeling, organizational behavior, operations research*** and others.

**The DARPA Quantum Network - World's First Quantum Cryptographic Network**

[**http://bit.ly/jwzXZI**](http://bit.ly/jwzXZI)

Under DARPA sponsorship, and together with our academic colleagues Harvard University and Boston University, BBN Technologies has recently built and begun to operate the world's first Quantum Key Distribution (QKD) network. **The DARPA Quantum Network employs 24x7 quantum cryptography to provide unprecedented levels of security for standard Internet traffic flows such as web-browsing, e-commerce, and streaming video.**

The DARPA Quantum Network became fully operational on October 23, 2003 in BBN's laboratories, and has run continuously since. It currently consists of two BBN-built, interoperable weak-coherent QKD systems running at a 5 MHz pulse rate (0.1 mean photons per pulse) through telecommunications fiber, and inter-connected via a photonic switch, together with a full suite of production-quality QKD protocols. In the near future, **we plan to roll out this network into dark fiber between our campuses through the Cambridge, Massachusetts metropolitan area, introduce a series of new quantum cryptographic links based on a variety of physical phenomena, and start testing the resulting network against sophisticated attacks.**

The principles underlying a quantum cryptographic network have already been proven on a limited scale. **Using lasers and photo detectors, light is sent, in a manner in which eavesdropping is always detectable, through either fiber optic cable or the atmosphere to distribute cryptographic keys that are used to scramble (encrypt) and de-scramble (decrypt) a message.** **The DARPA Quantum Network has improved upon these techniques to create an extremely secure, highly robust network protected by quantum cryptography, This secure network technology is 100% compatible with conventional Internet technology.**

**Quantum cryptography, invented by Charles Bennet and Giles Brassard in 1984, begins with a radically different premise -- one can base security on known physical laws rather than mathematical complexity. Physical devices, with specialized cryptographic protocols, can conjure up an ever-flowing stream of random bits whose values are unknown to any third party. When these bits are used as key material for Vernam ciphers, Shannon's ideal of perfect secrecy can be achieved cheaply and easily. By contrast with the unproven foundations of public key techniques, quantum cryptography promises information-theoretic secrecy firmly based on the laws of physics.**

**BBN's Technology / RAYTHEON Role** [**http://bit.ly/jwzXZI**](http://bit.ly/jwzXZI)

**Since developing the ARPANET (DARPA) over thirty years ago, BBN Technologies has been a pioneer in networking technologies. In creating the DARPA Quantum Network, we are applying this deep expertise to integrate new quantum optical sources and detectors with novel networking protocols. Our work is focused on three crucial areas:**

**Building a network based on the fundamental principles of quantum physics that is fully compatible with the current and future arena of most message traffic, the Internet. This has required the design and development of new hardware, software, and network protocols, and careful thought about the foundations of quantum cryptography.**

**Dramatically increasing both the speed and security of quantum cryptography by creating high-speed detectors and cryptographic systems based on entangled photons.**

**Identifying the potential problems and vulnerabilities posed by the most sophisticated "quantum hacking" techniques and integrating safeguards into the Quantum Network design.**

**Raytheon BBN Technologies** [**http://bit.ly/jmxnou**](http://bit.ly/jmxnou) **develops security protocol standards for use in both the public and Department of Defense (DoD) Internet communities. We are the editors of the core IP security (IPsec) standards developed in the Internet Engineering Task Force, and major contributors to DoD standards for the next-generation of programmable cryptographic devices that will be used to protect classified data. Raytheon BBN Technologies staff have led the development of public key infrastructure (PKI) standards and designed and implemented protocols to secure Internet routing.**

**The COSMOS program,** [**http://bit.ly/mgi82D**](http://bit.ly/mgi82D) **funded by the Defense Advanced Research Projects Agency’s (DARPA) Microsystems Technology Office, is changing the paradigm of how mixed signal circuits (combined analog and digital circuits such as analog-to-digital converts) are designed and built. The COSMOS program is enabling close integration of different semiconductor materials within the same circuit to allow the designer to pick the “best junction for the function,” thereby improving circuit dynamic range,**

**For more than 30 years, the wide bandgap semiconductor GaN has been theoretically identified as ideal for producing high-powered, high-frequency transistors. However, until the late 1990s, research on GaN was largely limited to a few university research groups and small companies, because the quality of the material was insufficient to support high-performance devices. The article presents an overview of the history of GaN electronics along with current work that is preparing to insert GaN MMICs into U.S. Department of Defense (DoD) systems. This research effort began at Raytheon in 2000 and has benefited from funding from multiple agencies — including the Office of Naval Research, the Missile Defense Agency (formerly the Ballistic Missile Defense Organization) and DARPA — as well as significant IRAD investments from Raytheon to address various aspects of the development.**

**Raytheon’s research in Compound Semiconductor Materials on Silicon(COSMOS) will enable a new class of high-performance mixed-signal integratedcircuits (ICs) that enhance the capabilities of U.S. Department of Defense (DoD) systems through direct monolithic integration of compound semiconductors — such as gallium arsenide (GaAs) and indium phosphide (InP) — and silicon (Si) CMOS on a common, low-cost silicon substrate.** [**http://bit.ly/mgi82D**](http://bit.ly/mgi82D)

**Protecting SOA Systems Against Determined Adversaries**

[**http://bit.ly/k5GJs7**](http://bit.ly/k5GJs7)

**Service oriented architectures (SOAs) are proliferating because they allow developers to incorporate previously developed software components and apply them in innovative ways, which means they can build reliable new applications faster and at lower cost. Because of these benefits, more and more military information systems and other critical systems are based on SOAs.**

**Critical SOA systems must not only tolerate accidental failures, but also continue to deliver an acceptable level of service despite being under attack. Yet the very characteristics that make SOA systems appealing--dynamism, loose coupling, and novel messaging and interaction patterns—also make them a challenge to protect. Current SOA environments lack adequate protection, detection, and adaptation capabilities to survive against motivated, well-resourced, and determined adversaries, putting them at significant risk of corruption, loss of service, and maliciously initiated leakage of information.**

**Protecting SOA environments requires a synergistic combination of protection, detection, and adaptation capabilities, complemented by validated design principles such as defense-in-depth, single point of failure avoidance, containment and isolation. Furthermore, novel techniques such as automatic generation of configurations and policies from high-level specifications are needed to address the additional risks and vulnerabilities introduced by service-oriented method of system construction. We are developing security features to handle the multifaceted and dynamic information exchange demanded by network-centric operations more quickly and cost effectively to enable future SOA systems to detect, protect and adapt to survive attacks from motivated, well-resourced, and determined enemies. Our strategic combination of innovative approaches is designed to bring the same level of resiliency to SOA systems that we have previously demonstrated in a distributed object based system. Our solution is focused on the following areas:**

**Architecture Enhancements to introduce isolation, containment, redundancy and to enable adaptive behavior.**

**Innovative Defense Mechanisms, including new security and adaptive technologies.**

**Safe and Secure Composition to ensuring safety, proper configuration, and freedom from residual vulnerabilities.**

**Quantum systems and the emerging, underlying technologies are maturing rapidly and proof-of-concept system-level capabilities are a reality.**

[**http://bit.ly/mxqdOZ**](http://bit.ly/mxqdOZ)

**Engineering proof-of-concept for communication privacy applications, such as the Raytheon BBN quantum network, and commercial systems for quantum key distribution are available now.**

**Quantum systems not only take sensing, communication, and processing “faster and farther,” they fundamentally change information processing and transmission, enabling new applications and privacy paradigms. Tangible benefits to important communications, sensing and processing systems are on the horizon.**

***Raytheon BBN is developing complete, vertically integrated, next generation communication, sensing, and computation systems, from the physical layer to applications, using new quantum, superconducting, and optical technologies*.**

***Our scientists are an interdisciplinary team of physicists, mathematicians, information theorists, and systems engineers with expertise in superconducting quantum circuits, quantum memory physics, quantum and classical information theory, and classical optical networking. We can provide fully integrated, practical systems that solve real problems***

**Our research is on the leading edge of quantum and optical phenomena and information science. You can find a selected list of our publications as well as note our strong collaboration with other leaders in the community here.**

**Bits and Waves Lab. Petabit Highly Agile Robust Optical System (Pharos)**

**Quantum Cryptography Quantum Sensors**

**Superconducting Digital Receivers and Coprocessors**

**Superconducting Qubit Systems**