## Stephen L Squires, PhD

SLSq@usa.net

Dr. Stephen L Squires is a consultant to industry, academia, and government in diverse areas of information technologies, information system security, and high performance computing and networking. He is a recognized IT expert with a demonstrated ability to provide leadership based on over 30 years of experience in formulating and translating long term visions into practical executable programs that build on existing and emerging science and technology.

He served as vice president and chief science officer for Hewlett-Packard Company with responsibility for providing leadership in establishing overall strategic scientific and technical directions, including the architecture of the digital renaissance for the 21st century Internet. During his five years at HP from November 2000 through January 2006, he made major contributions enabling HP to improve its position in National Security sectors. He led the Accelerating Trustworthy Internetworking and related community building activities in the aftermath of 9/11. He developed a Trusted Systems Initiative that provided important guidance to the HP information system security programs including its implications for HP Laboratories and HP Business. He introduced the concept of Critical and Pervasive Information Systems as essential to enabling sustained growth in the context of public and private sector information technology based systems. He also continued to work closely with DARPA and other parts of the US Government National Security Community. Most recently, he contributed to the vision and overall strategy for the National Terabits Initiative in the context of a Petaops Technology base within the US Government focused on enabling Integrated Reality.

Prior to joining HP in November 2000, Squires was the special assistant for Information Technology to the director of the Defense Advanced Research Projects Agency (DARPA). During his career at DARPA, he was responsible for advancing the frontier of progressively larger sectors of information technology. He developed plans for, managed, and directed the scalable systems parts of the DARPA Strategic Computing Program, the Federal High Performance Computing and Communications Program and its extension to the National Information Infrastructure. These programs are recognized as having helped enable the modern Internet, including its scalable parallel and distributed high-performance computing systems and the introduction of an explicit service layer. He formulated the vision and framework for the DARPA Bio/Info/Micro Initiative that became the foundation for the Nano-technology programs. He joined DARPA in 1983 as a program manager.

Squires was recruited by the National Security Agency (NSA) at age 18 while he was a freshman undergraduate electrical engineering student at Drexel University. He worked as an engineering intern in the advanced computing and communications laboratories of the NSA. Throughout his career as an electrical engineer and computer scientist at NSA, gaining early access to the full range of advanced technologies as they emerged, including many in cooperation with DARPA, such as early interactive time sharing systems with graphics, UNIX, ARPAnet, extensible programming systems, local area networks, the early Internet, personal computing, VLSI design, rapid prototyping and the highest performance information system technologies.

Squires earned his Ph.D. from Harvard University.

# Essential Pieces for Solving the Cyber Security Puzzle

**Stephen L Squires**

The essential pieces for solving the cyber security puzzle are described in terms of what is needed to gain strategic advantage over the increasing threats of the 21st century at a time when information systems are becoming critical and pervasive.

## Historical Context: Fundamental Trends, Limitations, Futures

Modern information technology began to emerge at the end of World War II with the invention of the von Neumann computer architecture in 1945 and the transistor in 1947. The impact of these inventions was accelerated with the invention of the integrated circuit along with progressively more advanced technologies for processing, storing, and communicating information through the end of the 20th century. The Internet and Scalable Parallel Systems further accelerated the process in the 1980s along with the development of the associated software and systems to enable ubiquitous information systems with wired and wireless access. These advances have enabled extraordinary growth including information systems that have become critical to a wide range of activities including National Security.

## Threats in Cyber Space: Global Characterization

The continued growth of the Internet is challenged by increasing threats. The challenges are limiting the transition of information systems from the ubiquitous systems of the 20th century to the more advanced pervasive systems needed for the 21st century that are also capable of supporting critical applications. The horrendous events of 9/11 illustrate the need to overcome these challenges and achieve critical and pervasive trustworthy information systems. A characterization of threats in cyber space from individual hackers to the higher grade threats of criminal activities to transnational terrorists and beyond to advanced information warfare of nation states is described in general terms. The continued geometric growth in vulnerabilities, exploits, and incidents is explained in terms of the limitations of the existing generally used information system technology base. An overall framework for discussing the issues is presented.

## Intrinsic Trust: Essential Pieces

A new approach to achieving trusted systems, called Intrinsic Trust is presented with an explanation of how it overcomes threats in cyber space by providing effective geometric advantage. The approach builds on selected existing and emerging technologies to enable fundamental strength of information systems on the existing Internet by 2010 while preparing for further advances needed for Internet 2020.

## Internet 2020: Achieving Critical Pieces by 2010

A vision for the Internet achievable by 2020 is presented. Internet 2020 will be as fundamentally more advanced than the existing Internet as the existing Internet was from the plain old telephone system (POTS) that existed before the Internet. Internet 2020 will operate as an evolutionary extension of the Internet while having revolutionary capabilities including Intrinsic Trust. The critical pieces for solving the cyber security puzzle through Intrinsic Trust can be available by 2010 for critical applications.

## Integrated Reality: Achieving Strategic Advantage

A vision for fundamentally more advanced systems, called Integrated Reality, enabled by Internet 2020 is presented. Integrated Reality includes Terabits to desktop Teraops systems that provide full immersion virtual reality operating at the limits of human acuity. The system includes access to extraordinary performance services operating in the context of distributed sensor networks. Integrated Reality systems will, among other things, support the use of ensembles of faster than real time simulations of high fidelity physics based models. A variety of applications are described across the private and public sectors in a global context including critical and pervasive trusted systems for finding and connecting the dots.