

The Information Sphere Domain – Increasing Understanding and Cooperation
Dr. Patrick D. Allen, Johns Hopkins University/Applied Physics Lab
Dennis P. Gilbert, Jr., Booz Allen Hamilton

Abstract

Recent discussions regarding the emerging field of cyber warfare have focused on the term “cyberspace,” and have included cyberspace as being considered its own war fighting domain, much like air, land, sea, and space. As the global community continues to wrestle with the legal and authority challenges of these increasing conflicts in cyber, it is interesting to note that the militaries of most nation-states, including the United States’ own Department of Defense (DoD), do not have an official definition of a domain, nor a set of criteria for what constitutes a domain.

The Information Age brings increased benefits through global interconnectivity. However, these benefits come with increased risk. Our computer networks are vulnerable to intrusion and abuse, while the increasing trend toward massively interconnected information systems exacerbates the problem globally. More and more resources and transactions ride on the security of our information systems and our confidence in them. Moreover, “national security” and “economic security” have become more tightly intertwined as the Information Age blurs the lines between civilian, political and military objectives.

In this stage of the Information Age, the international community is grappling with whether it needs to define this information realm as a domain, similar to the air, land, sea, and outer space domains that already exist. This presentation will present previously unpublished strategic analysis on this nascent domain, and subsequent discussion may result in enhancing the cooperative cyber defense capability of NATO and NATO nations. History shows that there is always an advantage in a conflict to the side that *understands and operates* within a domain better than the opponent. The authors desire to increase the understanding and operating parameters of the Information Sphere Domain, thus improving the NATO Alliance's interoperability in the field of cooperative cyber defense and cyber warfare.

In this paper, the authors propose a definition of a domain, define what constitutes a domain, posit how new domains are created over time, and describe the features of what is and is not a domain. These definitions and features lead to our proposal that the “Information Sphere” should be the preferred international term, and it is this “InfoSphere” that qualifies as a new domain, with features both similar to and different from the four existing physical domains. This paper will explore the reasons the authors believe the Information Sphere does qualify as a domain, and will describe some of the steps necessary for NATO Nations to defend against, and when necessary compete against, potential adversaries and win the cyber war within the InfoSphere domain.