Abstract

The focus of this poster is on an analysis of the relationships between U.S. Department of Defense (DoD) networks and policy, including policy about technology acquisition and usage. Policy affects technology research, development, test, evaluation, transition and refresh. Specific network-related technology areas support military command, control, and communications (C3). Some of these technologies are described with a view toward assessing the status of policy in specific areas. The relationship between policy and network technology is explored with questions such as, “What is policy doing for technology and vice versa?” and “How should we set policy priorities?”

Network policy can be divided into at least two categories. The first is policy that governs acquisition and life cycle support, such as research, development, test, evaluation, fielding, funding, and upgrading existing network technology. The other category of network policy pertains to how networks are used, user requirements for protocol, training, and rules to prevent user-created problems of all kinds. Factors that affect military network policy include the following.

a. Policy has a cascading effect that is similar to the inheritance property in object-oriented design.

b. Changes in user requirements and funding levels affect policy and vice versa.

c. An increase in the number of deployed networks and their use has increased the number, frequency, and level of detail of policy changes and refinements.

d. Policy should support new ways to use network technology. New and recently available network technologies necessitate policy updates.

e. A trend is developing toward an increase in the need for training of network administrators. More training is required to include network policy and its interpretation in the context of heightened threats and greater reliance on networks for distributed, secure communications.

f. Technology that enables multi-level security usage and development needs to rely on sound technologically sensible policy for its implementation.

g. Policy relies on modern, dependable technology for communication, refinement, and enforcement.

h. When policy changes, technology must be designed to accommodate that change without degrading every other aspect of the system.

i. Systems must be change compliant and change tolerant. Policy must reflect this.

j. Policy must meet the need for constant usage of critical, mission-essential technology (such C3).

k. Policy must address how new networks and network types will be funded, tested, certified, fielded, and maintained.

l. Policy should promote design and implementation of an open-network architecture with “plug-and-play” modularity.

m. Scientists, technology developers, and users need to suggest policy changes that affect all aspects of science and technology.

The defense community needs to improve methods of selecting priorities with regard to military network policy, its formulation, enforcement, and modification. As the joint military is becoming more net centric, policy makers and technology developers need to become more aware of how these priorities affect readiness and the ability of operational personnel to respond. Policy should be more responsive and flexible to include changes and upgrades according to feedback from end users so that networks can provide better, more efficient and dependable service to the war fighter. Most DoD policy was formulated with robust, persistent, and working networks in mind. Policy, standards, and technology need to be expanded to cover discontinuous and frail networks. Fault tolerance in joint combat-system networks must be upgraded. Ideally, policy development should parallel closely the development of technology and not lag far behind it.