

In the 2006 Quadrennial Defense Review, a request was made to have the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), develop a theory of cyberpower. It was noted that there was a need to develop a holistic framework that would enable policy makers to address cyber issues in proper perspective.

To satisfy that tasking, CTNSP convened five workshops, drawing on experts from government, industry, academia, and think tanks. Those workshops addressed a broad set of issues related to the evolution of cyberspace, cyberpower, cyberstrategy, and institutional factors that influence those factors (e.g., governance, legal issues).

To develop the desired theory, this paper systematically addresses five key areas. First, the paper defines the key terms that are associated with cyberpower. Particular emphasis is placed on the terms “cyberspace”, “cyberpower”, and “cyberstrategy”. Second, the paper categorizes the elements, constituent parts, and factors that yield a framework for thinking about cyberpower. Third, the paper explains the major factors that are driving the evolution of cyberspace and cyberpower. To support that effort, the paper presents strawman principles that characterize major trends. Fourth, the paper connects the various elements of cyberstrategy so that a policy maker can place issues in proper context. Finally, the theory anticipates key changes in cyberspace that are likely to affect decision making.

In view of the dramatic changes that are taking place in cyberspace, it is important to stress that this effort must be regarded as a preliminary effort. It is expected that the theory will continue to evolve as key technical, social, and informational trends begin to stabilize.