The Role of Information Technology in National Security Policy

Robert E. Neilson

This article presents a descriptive model that links governmental information technology (IT) policy making processes with the capacity building processes that add to the economic and military dimensions of national security. The model uses a "systems thinking" approach.[1] It attempts to integrate perspectives on national security into a multidisciplinary and coherent body of theory and practice from a holistic "systems thinking" view.

INTRODUCTION

A discussion of the role of information technology (IT) in national security does not fit neatly into a particular field of study or discipline. It is

1 The overall conceptual basis for the model presented in this article capitalizes on two of the five disciplines mentioned in Peter Senge's book *The Fifth Discipline*. Senge's *Mental Models* – "the ability to unearth our internal pictures of the world, to scrutinize them, and to make them open to the influence of others" and *Systems Thinking* – "the discipline that integrates others by infusing them into a coherent body of theory and practice" influenced the descriptive systems approach of the model (a theoretical perspective). Yet, the model is bounded by pressures and threats indicating that the model operates in an imperfect environment (a practice perspective).

Mr. Neilson is a Professor of Systems Management at the National Defense University's Information Resource Management College. He is a graduate of Norwich University in Vermont and holds an M.P.A. degree from the University of Georgia and is a graduate of the Industrial College of the Armed Forces. He is a doctoral candidate at the University of Southern California.

neither fish nor fowl. The study of the role of IT in national security is multidisciplinary and multidimensional in nature. It has economic, political and military dimensions. Discussion of this topic borrows heavily from the fields of political science, policy analysis, international economics, macroeconomics and military science. Few models exist that describe the effects of government policies in building the necessary infrastructure and human capacity needed to take competitive advantage of information technology.

BACKGROUND

The concept of national security is multidimensional. In earlier eras, national security was equated with a nation's ability to withstand military aggression. Large standing armies advanced weapons, and logistical and battle planning were the cornerstones of this historical national security concept. This historical concept is evolving to include the economic health of a nation (The White House, 1993), and economic health is increasingly recognized as a key factor in national security (President's Council of Advisors on Science and Technology, 1992). Military might is no longer the single variable in the national security equation. The USSR was a superpower but suffered economic collapse. Japan is proscribed from maintaining a large army, yet has become a world economic superpower.

LITERATURE REVIEW

Gurbazani, et al., Dumas, Poirier, Weidenbaum, Thurow, Tolchin, Toffler (1990, 1992) and others have developed models or descriptions that attempt to show the relationship between military and economic dimension of national security in an ever increasing global information based economy. For example, Gurbazani, et al. (1990) attempt to conceptualize governmental activities concerning information technology in a country. Their approach distinguishes two key factors: the level of government involvement in information technology and the nature of that involvement.

Dumas (1990, June) presents a mathematical model of the production of national security. His model attempts to sketch a way in which the "tools of economics can be applied to developing more realistic and effective national security policy." Dumas includes the following variables in his economic national security model: strength of own forces, strength of enemy forces, economic strength, technology, capital, labor and social welfare. Dumas' model suffers from an economist's cause and effect mentality—a logical positivist approach. It fails to address the internal and external pressures on the national security policy process.

Poirier, Weidenbaum, Thurow, Tolchin and Toffler offer qualitative information regarding possible linkages between a government's involvement in IT policy and its effects on the economic and military dimensions of national security by describing the importance of the economic dimension of national security in a global information based economy. What is missing from the literature is a discussion of the IT policy leadership role of industry and government in a world awash with political, military, economic and technologic change. Also missing are descriptive models that illustrate the dynamic nature of the policy process.

The descriptive model presented in Figure 1, entitled "Information Technology and Government Policy – Role of IT in National Security," illustrates a process for determining roles of government and industry in national security. The model specifically focuses on the IT policy process and the level of government IT policy involvement. Why a descriptive model? There is no consensus regarding IT's contribution to national security. Existing models are unidimensional and unidisciplinary and do not account for the dynamics of a rapidly changing environment. Evidence of IT's linkage to national security is anecdotal, contained in the form of past prescriptions and case studies (Gurbazani, King & Kraemer, 1992, March-April). Descriptive model building is a necessary first step in a longer journey to develop systems dynamics models that simulate the effects of policy decisions in a changing political, technological and increasingly international environment.

MODEL DEVELOPMENT

Figure 1 graphically illustrates the major components and actors in the IT policy process. The model is a generic model. It can be used to describe policy processes of countries, states or political sub-divisions within countries, or geopolitical entities (the European Community).

Construction of the model is based on a content analysis of the national security, industrial policy, and information technology literature.[2]

2 The literature review and subsequent content analysis included an automated search of the Business Periodicals Index, readers' Guide to Periodical Literature, Social Sciences Index, PAIS and ABI Inform was conducted in using the terms "information technology and national security," "Industrial Policy and National Security," "economic national security," and derivatives of these key words. In addition, documents from the Directorate-general for Telecommunications, Informations Systems Market and Exploitation of Research, Commission of the European Communities and the National Computer Board of Singapore were reviewed. A total of 28 documents were included in an annotated bibliography that formed the basis for the content analysis.

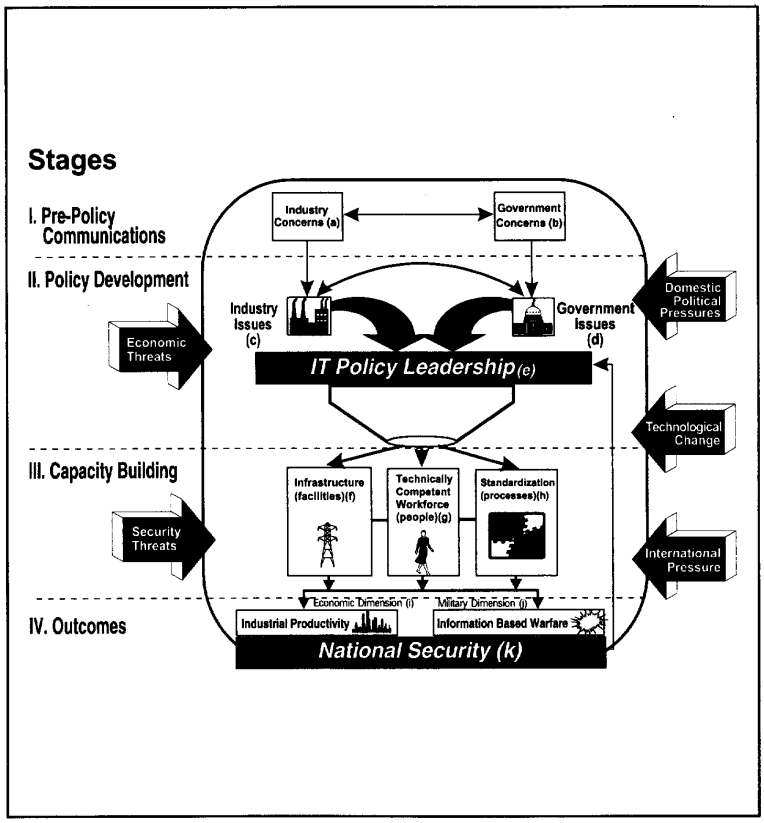

Figure 1. **Information Technology (IT) & Government Policy: Role of IT in National Security**

The object of the content analysis of these distinct subject areas was to identify similarities within the content of scholarly articles, books, reports, and contemporary news articles. Stage III of the model entitled, "Capacity Building," represents the results of the content analysis. Issues surrounding *infrastructure (facilities), workforce (education and training*), and *standardization (processes and products)* were the three major themes authors most often mentioned in their respective publications regardless of their professional discipline or pro or anti stance on industrial policy. An additional product of the content analysis was the emphasis placed on a newly emerging dimension of national security; economic national security. Authors increasingly rec-

ognize the importance of the sum total and holistic effect of information technologies on two key areas:

- global commerce; and,
- the growing military dependence on information.

These two concepts are represented in Stage IV "Outcomes" section of the model as *economic dimension* and *military dimension* of national security.

MODEL COMPONENTS

The model presented in Figure 1 is composed of four stages —(I) *Pre-policy Communications,* (II) *Policy Development*, (III) *Capacity Building,* and (IV) *Outcomes*. The first stage, *Pre-policy Communications*, attempts to capture all the informal dialogue, communications, and negotiations that go on between representatives of government and industry *before* a concern becomes a public policy issue.[3] This stage is similar in concept to the pre-competitive research and development stage of product development. It is the precursor to actual product or policy development. The two major actors in the *Pre-policy Communication* stage are industry and government.[4] For example, a public policy concern of topical interest is the ongoing dialogue between information industry and government officials regarding high definition television (HDTV). The debate focuses on which standard will be used as a United States standard to broadcast digital images. When informal dialogue reaches the disagreement stage and the concern affects the public, as in the case of HDTV, a policy concern becomes a policy issue.

3 An intentional distinction is made between a *public policy concern* and a *public policy issue* in the model. A *public policy concern* develops when an existing or proposed governmental action has broad impact on an industry or society. Usually there is controversy and disagreement among the stakeholders in the pre-policy communications stage of policy development. A *public policy issue* is an actual or proposed governmental action intended to remedy a given social, economic or political condition. See William D. Copin and Michael K. O'Leary, *Public Policy Skills* (Croton-on-Hudson, NY: Policy Studies Associates, 1988) for more information.

4 Nongovernmental organizations (NGO's) and academia, although vocal, are not considered major policy players in the IT policy process. See Carnegie Commission Report, *Facing Towards Governments – Nongovernmental Organizations and Scientific and Technical Advice* (New York: Carnegie Commission, January 1993).

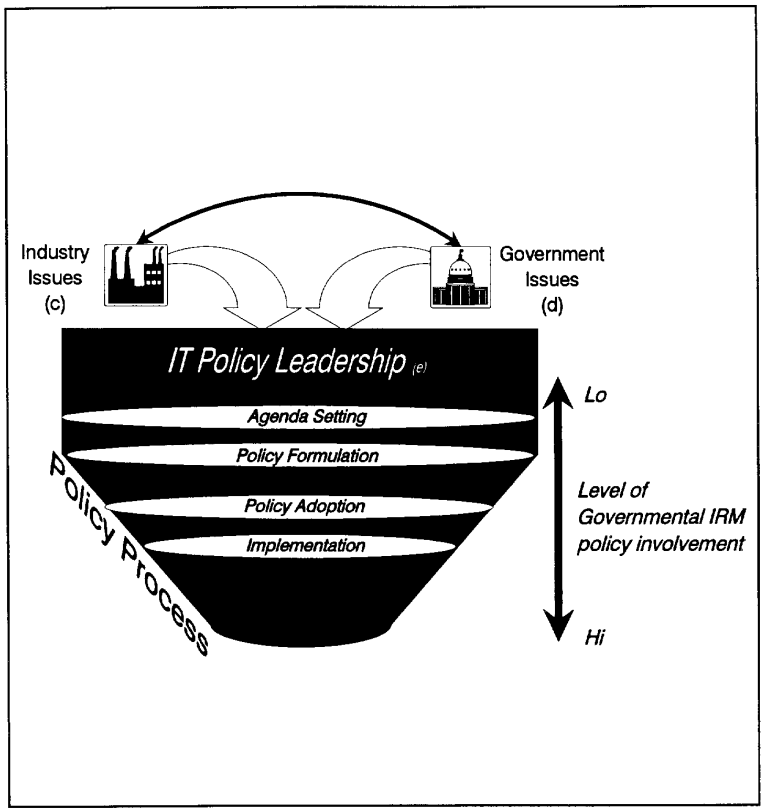

Figure 2. **Stages of Policy Development Process**

Governmental action may be necessary to remedy disagreement among the stakeholders especially when policy decisions have broad societal impact.

Once there is a determination that a public policy issue exists, with broad societal impact, the next step in the policy process is to ascertain the level of governmental action. The level and scope of governmental action is represented in Stage(II) *Policy Development* section of the model. Figure 2 – "Stages of Policy Development Process," based on the Radin and Hawley (1988) public policy process model, breaks out the IT Policy Leadership (e) portion of the model.

Within the policy development stage, the IT Policy Leadership (e) section of the model is best described as a mixing bowl or funnel of

policies, interests, visions, and agendas of affected parties from both government and industry. The funnel metaphor is apropos, in that the policy process is a filtering process, filtering the varying interests of government and industry into a coherent body of public policy. The filtering process can involve a relatively low (LO) level of governmental involvement at the agenda setting stage to a high (HI) of governmental involvement at the implementation stage.

The results of the IT policy development process do not neatly fall into distinct categories. However, the aforementioned content analysis indicates that there is some consensus that government IT policy is intended to have a salutary effect on three major areas: a nation's *infrastructure*, *workforce* and *processes* that will enable it to compete internationally. Stage III of the model, *Capacity Building*, contains these three major areas. These three building blocks form the raw materials used for building increased capacity of the two main dimensions of national security: *economic national security* and *military national security*. Economic national security can also be categorized under the more commonly used heading of *industrial productivity*. The growing importance of information technology in modern warfare is now characterized under an emerging concept: *information-based warfare*. These components of the model are represented in Stage IV of the model entitled *Outcomes*.

The entire model operates in a larger dynamic environment. Environmental influences (domestic and international pressure, security and economic threats and technologic change), represented by large arrows pointing inward, exert pressures on the boundaries affecting *all* stages of the model.

To help explain the dynamics of the model, metaphors from branches of physics, fluid dynamics, and hydraulics, are used to describe the ever changing nature of the policy process. Fluid dynamics and hydraulics are applied sciences that deal with fluids in motion or at rest.[5] Hydraulics is concerned with liquid properties such as density, viscosity and compressibility. Density is the weight of liquid per unit volume. Viscosity measures a fluid's resistance to flow. Compressibility refers to the reduction of volume of a liquid when pressure is applied. Most liquids can be compressed only to a limited extent. Fluid dynamics is concerned with fluids in motion.

The IT policy leadership process is similar to the study of fluid dynamics and hydraulics. Ingredients in the policy process can be thought of as having properties of density and viscosity in a volatile political

5 Information about fluid dynamics and hydraulics was taken from *Merit Students Encyclopedia* (New York: MacMillian Education Corp., 1974) Vol. 9, 162-164.

environment (compressibility). For example, let us trace the case of HDTV through the model presented in Figure 1 using fluid dynamics metaphors. The information industry's (a) contribution to the policy process far outweighed the federal government's (b) contribution in the form of several Advanced Research Projects Agency (ARPA) research grants. Industry's "policy flow rate" was a torrent in comparison to a trickle of government policy direction and funding. The "viscosity" of ARPA's policy contribution was equivalent to a thin layer of glycerin, a colorless, odorless, slippery, syrupy liquid. The ARPA's policy direction and seed funding coated the policy funnel (e) with a thin layer of a "policy neutral glycerin" lubricating industry sponsored research and development. In the case of HDTV, the "policy viscosities" were such that the federal policy and the industry policies did not mix. Industry policy rode on top a thin layer of government IT policy.

Further borrowing from the field of fluid dynamics, it is important to recognize the shape of the funnel below the IT policy leadership function. Daniel Bernoulli, a Swiss physicist, formulated a fluid dynamics principle that states that pressure exerted by moving fluids decreases as the fluid speeds up and increases as fluids slow down. The policy process is similar to the Bernoulli Principle. If the policy process is moving swiftly, there is less political pressure needed to keep the process going. Conversely, pressure builds when there is little agreement among the stakeholders in the policy process. The policy process slows down. At the agenda setting stage of the policy process (see Figure 2), it is incumbent on the major actors in the policy process to agree to the on a policy strategy ranging from a laissez-faire approach to heavy government involvement depending on:

- Past history of government involvement,
- Level of potential governmental funding,
- Social benefit, and
- Nature of the IT policy.

For example, if an IT policy deals with a controversial telecommunications infrastructure (f) issue involving equity, access, and social benefit issues, government policy officials (e.g., the Federal Communications Commission) would probably be involved through the implementation stages. Government policy in this case may take the form of regulation. On the other hand, if the policy issue deals with IT standards, a

rapidly changing field, and the policy issue does not involve equity, access or social benefit issues, governmental policy officials may want to take a laissez-faire approach by permitting corporations in the information industry to develop standards.

SUMMARY

The key to defining government and industry's respective roles is determining what constitutes a public policy. Policies that involve equity, access, and social benefit issues are considered public issues in the United States. The nature of what constitutes a public issue, however, is evolving. For example, the continuing debate over health care has moved from the notion of health care as a private concern to its present incarnation as a public policy issue. Much of the debate regarding health care is framed in terms of health care as a "right"—a public policy issue.

With construction of the National Information Infrastructure (NII) before us, it is conceivable that access to information could be framed as a "rights" issue. Discussion of information "have's" and "have not's" is becoming part of the NII policy debate lexicon. Public access rights to the NII may also evolve into a "rights" issue. Using the model presented in this paper as a heuristic device may help frame policy concerns and issues in future policy debates surrounding the design, construction, and operation of the NII. Descriptive modeling is the first step in a longer journey. Developing systems dynamics models illustrating joint efforts by government, industry, and eventually citizens is the next step. Simulating the effects of policy decisions in a changing political, technologic, and increasingly international environment will help illuminate policy choices and take the guess work out of IT policy.

REFERENCES

Dumas, L. J. (1990). Economic Power, Military Power and National Security. *Journal of Economic Issues*, Vol. XXIV, No. 2, 654

Ibid., p. 656.

Gurbazani, V., et al. (1990). Government as a Driving Force Towards the Information Society: National Computer Policy in Singapore. *The Information Society*, Vol. 7, 155-185.

Gurbazani, V., King, J. L. & Kraemer, K. L. (1992, March-April). Economic Development, Government Policy and Diffusion of Computing in Asia-Pacific Countries. *Public Administration Review*, Vol. 52, No. 2, 146-156.

Hawley, W. D. & Radin, B. R. (1989). *The Politics of Reorganization.* New York: Pergamon Press. 219-223.

President's Council of Advisors on Science and Technology. (1992, December). *Science, Technology and National Security*. Washington, D.C.: Office of Science and Technology Policy. 1.

The White House. (1993, December). *National Security of the United States.* Washington, D.C.: U. S. Government Printing Office. 1.

Thurow, L. (1992). *Head to Head*. New York: William Morrow & Co.

Toffler, A. (1990). *Powershift*. New York: Bantam Books.

Tolchin, M. & Tolchin, S. J. (1992). *Selling Our Security*. New York: Alfred A. Knoff.