"**ORGANIZING FOR IT POLICY:** A PRAGMATIC APPROACH TO THE INFORMATION REVOLUTION AND THE NATIONAL "INTEREST"

Ernest J. Wilson III
Director

Center for International Development and Conflict Management University of Maryland

Senior Advisor,
Global Information Infrastructure Commission
Washington, D.C.

Earlier versions of this paper were presented to the RAND Corp., Santa Monica, CA., The Secretary's Open Forum, U.S. State Department, the Stimson Center, and to the Institute for International Communications Policy Forum, Washington, D.C. Thanks to Randi S. Bessette who provided research assistance for this article.

Introduction

There is growing concern in Washington today about the effects of the Information Revolution on a wide variety of U.S. foreign and domestic interests. Since the early 1990's, government officials, academics and policy analysts alike have focused on and puzzled over the impacts of the Information Revolution on U.S. interests.[1] A number of trends emerge from a close reading of this small but growing body of work:

1. The Information Revolution is driven by real trends and deep changes that are consequential for U.S. interests;
2. Most of the writing concentrates on information warfare, and the remaining literature is balkanized across disparate subfields treating issues as diverse as encryption and trade;
3.The literature, however, ignores the next step, how to think coherently and strategically about the diverse issues that make up the Information Revolution, and how should governments be organized today to better act on them tomorrow?"

This essay addresses the last point: how should senior government officials conceptualize the Information Revolution in order to make more informed and strategic decisions that recognize the complexity and "interelatedness" of the many diverse issues that together make up this new and quickly changing policy area?

Thus far, most writing on the impact of the Information Revolution on U. S. national interests has been narrowly defined. Authors concentrate overly on traditional national security concerns, with cyberwar, netwar and other terms predominating. Much of this work has been quite innovative and insightful, from Rondfelt's (Rondfeldt, 1993) more academic ruminations

[1] 'These include: Martin C. Libicki, "What is Information Warfare?" *Strategic Forum* no. 28, May 1995; Joseph Nye, Jr. and William A. Owens, "America's Information Edge," *Foreign Affairs* March/April 1996, pp.20-36; David Ronfeldt, "Institutions, Markets, and Networks: A Framework About the Evolution of Societies." (Santa Monica, CA: RAND, 1993)..

about the societal implications of cybersecurity, to Libicki's (Libicki, 1995) careful writings defining the key terms of cyberwar, and Molander and his colleagues' (Molander et. al., 1996) simulation work with senior government officials

As important as it is, the national security focus alone is too limited. One needs a fuller explication of information's impacts on national interests broadly defined. This would include impacts on other critical policy areas of the information age such as trade agreements and conflicts, bilateral and multilateral treaty negotiations, economic development, foreign investment and international standardization issues. The use of the term "national interest" in no way minimizes the importance of traditional national security issues in the information age. In fact, traditional national military concerns remain a critical component of the definition of U.S. national interest. The term "national interest" is intended, however, to reflect the evolution and growth of the concept of national security to include non-traditional "security" issues such as trade and the environment that are increasingly important in the post-Cold War era.

Ultimately, the effective management of the intersection of new global information realities and traditional policy paradigms will require that some federal units, offices, or agencies be given the authority to identify, track, and where appropriate, to act on the national interest implications of both traditional and non-traditional security concerns.

Why the Information Revolution is Difficult for Governments to Manage

While the urgency of the coming "infosphere"(Rothkopf, 1997) appears unique, similar urgent concerns have accompanied other big new policy issues that also forced their way onto the crowded agendas of busy senior government officials. Other examples might include the energy

crisis of the 1970s and the environmental movement of the 1980s and 1990s. (Wilson, 1987)

These other issues share certain features with the Information Revolution.

- previously handled by mid-level technicians, they quickly get advanced to the Assistant Secretary level and above where they are invariably politicized and meshed with other complex national security issues;
- they hinge on fast-paced technological developments and assessments, and involve especially high uncertainties, and are often confounding to non-specialists; they always cut across disciplinary as well as bureaucratic boundaries;
- they are typically defined in overly-technical terms that discount the institutional, political and societal implications involved;

The Information Revolution shares all of these features, which challenge the capacity of policy makers to put each separate issue into its broader context.

Framing the Issues

How can we frame the perplexing information-national interest nexus in a way that helps senior policyrnakers reach more informed decisions? A guiding principle in designing such a framework should be the perspective of the senior official who typically has only limited time to be briefed by her aids, and needs to get the maximum amount of relevant information in the shortest time possible. Such an analytic framework should both identify the wide range of substantive issues involved and be sensitive to the distinctive bureaucratic and organizational features that characterize them.

The Open-to-Closed Continuum

Information policies differ according to whether they are targeted at relatively transparent

and open activities, or they are inherently more secretive and closed.(Geller, 1996; Steele-Vivas, 1996) Much of the thinking today on information and national security concentrates on the closed end of the continuum -- especially the veritable cottage industry on'cyberwar' and 'information warfare'. At the closed end, analysts not only weigh the effects that new information technologies may have on traditional military roles, but also consider more salient modem concerns like information terrorism. IT is often discussed as it contributes to the Revolution in Military Affairs (RMA). Much of the cyberwar analysis is (appropriately) classified, involving sensitive intelligence collection techniques and military procedures.[2]

While this type of "closed" analysis remains essential, the other more open end of the spectrum, that of "public diplomacy," has become an equally pressing piece of the informationnational interest puzzle. These activities have the goal of informing and influencing foreign publics, to advance mutual understanding and to promote U.S. policies and goals. "Public Diplomacy" activities include: Voice of America (VOA) and WorldNet television broadcasts; shortwave programs to Russia and Eastern Europe; American book and magazine publishing; and international citizen exchanges. (Snyder, 1996)

This unique role of the government, however, is currently beset by new challenges and questions about the most appropriate public diplomacy role of the United States in a post-Cold War world. More recently, the 1994 decisions by the President to reorganize and consolidate the operations of Radio Free Europe (RFE), Radio Liberty (RL) and Voice of America to create Radio Free Asia, to retain Radio Marti (in which this author was involved[3]) is an example of this.

---

[2] 2 For a more detailed description and anylsis of "cyberwar" and "information warfare" see Bruce Berkowitz, "War in the Information Age," *Issues in Science and Technology* Fall 1995. pp, 59-66. Peter A. Wilson, Robert A. Manning and Col. Richard L. Klass, (ret.) "Defense in the New Information Age: A New Blueprint," Policy Report No. 26, Washington, D.C.: Progressive Policy Institute, 1995.

[3] This author worked on RFE/RL consolidation at the NSC at the White House in 1993 and 1994.

While Senator Jesse Helms recommends the elimination of many of these activities, the fact remains that in the post-Cold War information age, most believe there is some role for government's informational service. More and more, all diplomacy must have a substantial public diplomacy component in order to reach and influence civil society and mobilized publics, especially on new "national interest" topics like global democratization, the environment, and information access. Nye and Owens argue convincingly that the need for'soft power' resources of public diplomacy indeed has increased substantially with the Cold War's end. (Nye and Owens, 1996:29;Thurow, 1996; Matthews, 1997)

Between the two poles of the "open-closed" continuum one encounters other policy issues neither fully open nor fully classified. They include, for example, the psychological operations of the army ("psy ops" radio broadcasts and dropping leaflets from airplanes, as used in Somalia and Haiti). The conduct of traditional behind-the-scenes diplomacy by State Department diplomats channelling the U.S. government's views to other nations is also a form of information policy. (Solomon, 1997; Wriston, 1997; Schultz, 1997) New information communications (IC) technology has so affected this middle band that some analysts question whether traditional embassies and diplomats are still necessary in an age of instant, real time communications. "Some recent analyses of American foreign policy argue that embassies and diplomats have lost relevance, the victims of modem technology ... [and] the proliferation in parallel lines of transnational communication. Despite technological change and the rapid growth of nongovernmental communication, in the foreseeable future the nation-state will remain the dominant actor. "(Harrop, 1996: 1)

The 'Open' to 'Closed' Continuum takes this form:

OPEN===Pub Dip=====Psy Ops====Trad Dip~===Intel====CyberWar======CLOSED

The Public to Private Contiunuum

Because the private sector has become the driving force of the Information Revolution and hence increasingly problematic, a public-to-private continuum is a second important dimension in an information-national interest framework. At the public end of the spectrum are promotional and educational activities designed to inform the citizenry about their opportunities in the IT Revolution. (The NII Task Force is an example of this, as are presidential speeches on the "Information Superhighway"). Government officials from Vice President Gore to Speaker Gingrich praise new information technologies because they see them strengthening American democracy, our greatest national resource. This is an appropriate and unappreciated aspect of government's public role.

At the private-oriented end of the spectrum government policy creates incentives for the private actors to behave in new ways, using law, regulation, education or executive "jawboning." Here are found some of the thorniest national interest issues, both closed and open, including open regulatory and legal issues like intellectual property rights (IPR), to more closed issues of private industry encryption standards. Encryption issues, for example, pose very tough trade-offs among domestic First Amendment rights; security against foreign attack and terrorism; and international trade competitiveness. They require careful balancing of desirable yet often competing imperatives. For example, while law enforcement and intelligence agencies fear that private encryption techniques will thwart their capacity to protect sensitive security operations,

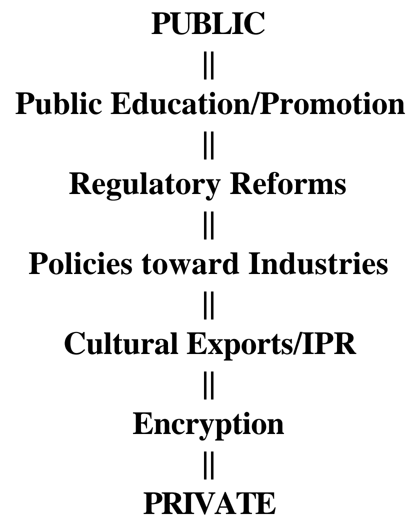
private information companies worry that government-mandated controls using 'public-key encryption' will diminish their ability to compete with other exporters in overseas markets. (Studeman, 1995:15) In addition, many individual Internet "netizens" claim that any government regulations in this area constrain their privacy and/or First Amendment rights. (Browning, 1997)

Aside from constitutionality and morality is the question of policy effectiveness. Many industry specialists argue that most controls over IT are ineffective and irrelevant. The new technical reality of the changing global marketplace has already made cryptography and information security in general a necessity for private firms to compete. Already, this technology is widely used in the private sector, and much in demand.

Beyond security, the economic components of national interest are also a key consideration on the private end of the continuum. This is especially true for intellectual property laws. The Clinton Administration has repeatedly defined job-creation and high wages through exports as central to long-term U.S. national interests. The entertainment business is moreover one of the most profitable sectors of the American economy but its massive cultural exports suffer billions of dollars of losses each year at the hands of CD and movie pirates, many from nations whose governments similtaneously decry the sale of American films as cultural imperialism.

Government officials, therefore, need to better understand the limits, possibilities and liabilities in private information and communication markets, and how they might impact on what government can do to advance the national interest. Today, officials need to track private sector dynamics in an open, transparent fashion to better understand the activities it could ignore before -- private information providers, transporters and consumers. Because private consumer demand and innovation are driving the Revolution on a global scale, IC issues have shifted from being

mainly in the domestic economy, to issues imbedded in world markets. More and more, IC policy is tied to trade policy. Therefore, suitable trade strategies must be developed to promote the competitive position of American IC firms in an increasingly liberal world environment. William Drake argues the U.S. government should pay more attention to the newer, smaller firms who represent America's future competitive position as much if not more than the huge, long established multinationals. (Drake, 1996) Indeed, these cutting-edge smaller firms give the United States much of its distinctive edge over European and Japanese competitors. Minimally, government needs to monitor private sector dynamics to consider their impacts on government's own goals and means. Monitoring private sector dynamics in this context means the government getting smarter, not necessarily more interventionist. The 'Public' to 'Private' Continuum includes the following:



The Issue Matrix

The following four cell matrix illustrates the ways these multiple issues of information and national interest fit together where the open-closed and private-public dimensions intersect. This matrix meets the need of senior government (and private sector) strategists for an analytic framework that is parsimonious but provides for the full range of substantive issues that officials need to address today. Combining the open/closed and public/private dimensions creates a simple and accessible 'issue space to visualize one information policy issue vis-a-vis another. (Boisot, 1995)

This illustration is only a snapshot at one point in time of the major policy issues to be monitored, evaluated and acted upon by government. Presented here in static form, some policy issues will 'migrate' over time from one quadrant to another. If this essay were presented in multimedia form, we could show a moving picture of these issues as their configuration changes, as when issues that were private become public and those that were closed become open. Indeed, there are continuous pressures by different interest groups to shift these matters from one quadrant to another. In general, the Information Revolution and its technological advances tends to shift issues such as encryption from the closed side of the matrix more toward the open, and from the public to the private arena.

The Issue Matrix is constructed as follows:

PUBLIC

1.	2. Traditional Closed Diplomacy
Public Diplomacy	Traditional Intelligence
(VOA, OMRI Reports) "Psy	Ops" Cyberwar
	Netwar
Internet Development	
OPEN Standard	ization CLOSED
3.	4.
"CNN Effect"	
implementing WTO	
IPR	Encryption
Encryption	
Regulatory Reform	Electronic Commerce
Standards	EDI
Trade Policies	

PRIVATE

As we look at this matrix several types of issues stand out. First are brand new policy issues like cyberwar or the trade implications of telecommunications services (e.g. the WTO agreement) that policy makers have never had to confront before. Second are issues that have migrated from one quadrant to another, such as encryption which now spills over the northeast quadrant (2.) to the southwest (3) and southeast (4). Third are issues like IPR which have greater economic salience in today's global IT environment.

The Agency Matrix

Solving substantive problems is easier if the administrative structures are in place to facilitate them. The Agency Matrix indicates which groups or agencies are involved in or responsible for particular information and national interest-related activities. Currently, there is no one single agency responsible for monitoring and evaluating all the issues we have discussed under the rubric of "Information and National Interest." Instead, many agencies handle one or several pieces of the information-national interest puzzle. The Department of Commerce takes the lead in a number of areas through its National Technology and Information Administration (NTIA), but Justice and the FCC are starting to play larger and larger roles as controversial issues of competition policy and reciprocal market access grow. The United States Trade Representative's responsibilities have expanded greatly as previously trade-sheltered IC services move into overseas markets. The State Department has clearly taken a back seat to the Office of the Vice President in setting international information priorities, but retains a seat along with the NEC at the "high policy" table at the White House. To sort out the contribution each agency can make to integrating information and national interests, an Administration needs to answer at least four questions:

1. Are the relevant individual agencies doing the best possible job in their distinct areas of responsibilities?
2. Are these separate activities being effectively coordinated to create policies that are greater than the sum of their parts?
3. Are private sector perspectives and information being adequately incorporated into policy making?
4. If change is needed, what can be done to improve intra-agency, interagency and public private effectiveness?

There are several important points to be made here. First, in the "real world," these administrative questions will be asked and answered against the backdrop of rapid technological

and commercial convergence in the IT sector. In other words, these decisions must be made amidst a swiftly moving floodtide of change, demanding administrative flexibility and foresight. Second, convergence, globalization and privatization have undercut the abilities of the traditional front-line agencies of the Departments of Commerce and State to keep up with the rapid, radical transformation of the IC market. Likewise smaller, more nimble and more market-oriented agencies like the USTR and the FCC appear better equipped to address these issues, especially with the increasing involvement of the Justice Department in cases raising anti-trust and First Amendment issues. These issues are complicated further since virtually all federal agencies are experiencing their own downsizing to cut costs and positions.

Another very important matter is the tug between the military and civilian agencies. This is complicated because the Department of Defense is going through a major rethinking as part of the Revolution in Military Affairs (RMA). Since so much attention by analysts at RAND, CSIS and other institutions has been on the military side, and since electronic warfare did play an important role in the Gulf War, DoD is well placed to continue to define the national debate on IT and U.S. national interest. The State Department, which only recently relinquished its antiquated Wang computers, is well behind the curve on defining and managing the issue despite occasional small conferences around Washington on diplomacy and the IT revolution. Not surprisingly, in this increasingly important area as in most others, U.S. government agencies are vying for influence and control of the policy agenda, with substantial policy leverge potentially at stake.

A huge challenge facing the Clinton Administration is how to integrate the planning, policy and operational activities of all of these agencies, between the military and civilian

agencies, and among the latter. "Information policy," if it existed at all, varied according to which branch of government, agency or individual was involved. No single information policy exists today that

defines an overall policy or integrates the activities of DoD and civillian agencies. Arguably, this setup was once appropriate given prevailing technological and political priorities. Now this history constitutes one of the main barriers to the current need for greater policy integration. The following Agency Matrix indicates the current agency responsibilities:

PUBLIC

1 US Information Agency OPEN	2 CIA DIA NSA CLOSED
3. DOC FCC DOJ USTR	4. DOD CIA OVP DOJ NTIA

PRIVATE

The New Importance of the Private Sector

Faced with the new pressures of private global markets, the federal government must meet the new challenge of taking into account private sector perspectives and capacities in its ongoing reform of governmental processes on information policy and national interest. It must carefully balance the requirements for gretaer consultation with the risk of cooptation. Changes are underway, but building new relationships and developing mechanisms more responsive to the increased importance of the private sector is a painfully slow, step-by-step effort to build (and in

some cases rebuild) trust on both sides. Points of friction can develop at several points, especially over quadrant three issues of market access, foreign investment or standardization, and with quadrant four issues of IPR and encryption. While the progress of public-private sector coordination has been slow, in the last five years government has formed numerous groups (and a number have reorganized) in which the complicated task of mutual consultation can begin. The following are some examples of the leading private or private-public advisory or advocacy groups relevant to information and national interest (this list is indicative but by no means exhaustive): **International Information Task Force (IITF)/National Information Infrastructure (NU) Advisory Council-** created in 1993 and disbanded in 1996 was a thirty-seven member advisory committee to the Secretary of Commerce; **Security Issues Forum (SIF)-** government only, but conducts public meetings and hearings to coordinate security efforts across the Committees and Working Groups of the **IITF;United States Security Policy Board (SPB)-established** by Presidential Directive 29, is an interagency body tasked to develop integrated and coherent security policies across the range of security disciplines-government only; **Security Policy Advisory Board-** personnel selected by the President, advises the **SPB; National Security Telecommunications Advisory Committee (NSTAC)** along with its **Information Assurance Task Force** is the most robust private sector advisory group.

The International Matrix

Thus far,we have concentrated on domestic policy. To the domestic side can be added a third issue space matrix for international agencies and multilateral fora. The negotiations at the World Trade Organization (WTO) and International Telecommunications Union (ITU) remind us how IT issues of tremendous importance to the United States are increasingly internationalized and

increasingly decided in open international fora, not just behind closed doors at home, nor through mainly bilateral channels.

It is important to remember that the integration of information and U.S. national interest is increasingly shaped by the actions of international bodies and other countries. Once strictly domestic or bilateral negotiations have been pushed by technology and the globalization of trade into international fora. It is more and more difficult for any single nation to take decisions in this sector unilaterally; telecoms for example, is no long a sheltered domestic monopoly; it is a traded commodity like soybeans or toasters (Hundt, 1995). American firms want access to foreign markets; foreign companies want to buy our technology and compete in domestic markets. The Internet makes cross-border trade (and cross-border smut) as easy as a keystroke (Kahin and Nesson, 1997). The practical consequence is that U.S. decision makers must negotiate basic agreements in new arenas, whether through new bilateral arrangements, in multilateral fora or with large powerful corporations. Some of the most important negotiations of the past decade have occured in new fora, from the unprecedented global telecoms deal negotiated in the brand-new World Trade Organization (WTO), to the International Technology Agreement (ITA) negotiated mainly through the trade associations of North America, Europe and Asia, to the ongoing, low visibility but highly significant standard- setting talks of the International Internet Society (ISOC).

The difficulties involved for government officials to select the optimal forum within which their leverage over a particular policy issue is greatest, and where they need to negotiate extremely important IT deals, should not be underestimated. Here too, decisions made in one quadrant will interact with others in sometimes unpredictable ways. Other countries' governments are also facing similar challenges of reorganizing their own administrations to

respond to new global information challenges. The following international matrix, therefore, serves as an additional framework to categorize actors and issues in this global context, to increase U.S. policymakers' knowledge of how other nations organize their issue space, and perhaps facilitate their ability to conduct negotiations in each of the quadrants similtaneously.

The International Matrix:

PUBLIC

1. UNESCO OPEN	2. Bilateral Treaty Negotiation NATO CLOSED
3. WIPO OECD ITU WTO WORLD BANK International Internet Society (ISOC) Cultural Exports Individual Corporations	4. OECD EU ASEAN

PRIVATE

The starting point of this essay is the dilemma faced by senior government officials simultaneously confronting too much raw data flooding into their offices too fast, and lacking an integrating framework to filter, contextualize and prioritize this vast information flow. Too often they lack a full perspective of the policy challenges they face. Information issues from key escrow encryption to French media policy are crowding willy nilly onto policy makers' agendas. To impose some order on this unruly universe, we have suggested several complementary

frameworks to identify the most critical elements of the Information Revolution and how they intersect. Decision-makers can thereby situate their own agency and their own substantive concerns in this more broadly-gauged context.

This approach differs from others in at least three ways. First, these matrices help frame the issues from the real-world, organizational, perspective of senior government decision-makers. Second, the frameworks identify and categorize the constitutent elements of an international information policy for the United States. Third, the frameworks tie policy categories to institutional bases and biases. Perhaps the greatest utility of this matrix is to indicate to decisionmakers other important but less familiar issues from another quadrant that may affect their own responsibilities.

Even the best analytic frameworks are useless, however, if they are not made operational by real officials in particular agencies. At the outset, coordination appears to be one of the larger tasks. Several prominent observers, including Henry Geller, have called for a single new federal agency with IC responsibilities, because the stakes in this field are so high. Geller claims that "[t]he nation has drifted along with the present fragmented and patchwork policy structure for too long. The global information economy demands that we put our policy house in order. "(Geller, 1996:135)

Conclusion

There are a variety of solutions proposed to the problems identified above. Some like Geller suggest a new Department of Information. However, there is not enough "broken" in the current system to warrant such a radical fix. Also, such a centralized agency would feel pressure to be proactive and "hands-on" to prove its worth. This contradicts a critical part of this proposal, that government needs to become more informed, not necessarily more interventionist.

The desired outcomes are: current agencies would anticipate and take advantage of positive new opportunities and preemptively reduce threats; agencies would ensure needed information is available to all key actors; and the President, the Vice President, and Cabinet officials would be aware of the actions of other agencies. What then is to be done? My experience in government and the private sector leads me to resist the idea of a new agency, especially in this period of budget stringency and when agencies are being eliminated not created. In shorthand, my preferred prescription is:

1) No new agency.
2) Reform existing agencies where necessary.
3) Better coordination among existing agencies through a formal, standing Interagency
4) Working Group (IWG) co-chaired by the NSC and the NEC.
5) Continuing close cooperation between the Administration and the private sector, and
6) the creation of new channels to ensure that private sector concerns get communicated effectively to government, and vice versa.

The best solution to these problems is establishing a standing Senior Interagency Group on Information and National Interests (SIGN). This monitoring body should be based at the White House; any other agency in the chair would provoke insurmountable turf wars and would not be taken seriously. It would be co-chaired by a senior director from the NSC and the NEC, with a very small staff of one or two, tasked with monitoring the information-national interest interface. It could include substantive working sub-groups on encryption, trade issues, offensive and defensive aspects of cyberwar, public diplomacy, and so forth. It should include representatives from the OSTP, the OMB, the Office of Emergency Preparedness, representation from the U.S. Information Agency, and the economic, military, and intelligence agencies.

This body would serve three broad purposes. First, SIGN would monitor the performance of individual information-related activities across the agencies to ensure that they are meeting their current responsibilities in this area. Who is responsible, for example, for responding to a massive computer virus attack in this country, or a forced shut-down of electrical or ransportation grids? Second, SIGN would squeeze greater *synergies* and medium-term strategic thinking on information-national interest issues from the relevant agencies, as well as encouraging consultation with the best outside thinking on this topic. Nye and Owens point to the difficulties of knowing how best to leverage the confluence of the once-separate information technologies in order to enhance U.S. interests into the 21 st century. (Nye and Ownes, 1996:22) SIGN would press the operational agencies to do so, and thereby meet the forward planning expectations of the White House.

The third responsibility of SIGN would be to ensure the adequate *coordination* of current and planned activities, and widely distribute information on 'best practices.' This would include providing "Big Picture" briefings for the President, Vice President and other Cabinet and subCabinet officials, to complement the more detailed agency-specific briefings now available. A big part of its charter would be to guarantee that private sector voices are regularly consulted through institutionalized public-company bodies.

The policy challenge of the late 1990s parallels the policy challenges of the mid to late 1970s in the then-emerging subject of 'energy policy'. Then, too, government was driven by a confusing welter of sub-sectoral policies, and top officials struggled to impose some conceptual and operational order on a group of heretofore independent domains -- petroleum policies, coal policies, hydroelectric power rates, nuclear plant construction, etc. It was only after years of wrestling with these separate concerns that the federal government was able to reach something

approaching a more holistic, integrated perspective, providing a clearer sense of cross-subsidies, inter-fuel substitution, and so forth. (Lindberg, 1977) Virtually the same process is underway in the information-communications field, as once-separate industries are driven by technological imperatives to converge, and new services and hardware appear on the market. Federal departments, independent agencies and the White House are all struggling to redefine a new and more inclusive policy domain called "Information Policy" that will advance the national interest.[4] The framework suggested here can contribute to that process.

[4] An important caveat. There is a risk of excessive hype and enthusiasm in this new field. Some studies classified and unclassified try to reduce all activities to 'information'. While there is an appropriate place for 'information' in the portfolio of important national interest issues, it should not subsume other substantive issues by dubbing everything as 'information.' Of course, better coordination and new tasks is no substitute for coherent strategies that set priorities for U.S. foreign policy. In the search for a coherent post-Cold War national security strategy, the government needs to construct its vision of the future. In this emerging global economy, the United States must carefully identify its strategic information assets. Finally, it must define the requisite bilateral, multilateral (and where necessary, unilateral) strategies the U.S. should pursue to achieve its interests. (Rutkowski, 1996:249) The time to take up this task is now.

Citations

Berkowitz, Bruce. "War in the Information Age" *Issues in Science and Technology* Fall 1995. pp. 59-66

Boisot, Max. *Information Space: A Framework for Learning in Organizations, Institutions and Culture* (London: Routledge, 1995).

Browning, John. "I Encrypt, Therefore I Am." *Wired* November, 1997.

Burton, Daniel F. Jr. "Brave New Wired World" *Foreign Policy* No. 106. Spring, 1997.

Drake, William J. "The National Information Infrastructure Debate: Issues, Interests, and the Congressional Process," in William J. Drake ed. *The New Information Infrastructure* (New York: Twentieth Century Fund Press, 1995).

Geller, Henry. "Reforming the U.S. Telecommunications Policyrnaking Process," in William J. Drake ed. *The New Information Inftastructure* (New York: Twentieth Century Fund Press, 1995).pp.115-136.

Harrop, William. "The Foreign Service After 2005," American Foreign Service Association Homepage, February 28, 1996.

Hundt, Reed. "The Need Continues," Keynote Address, BROADCAP Inaugural Conference. Washington, D.C., 1995.

Kahin, Brian and Charles Nesson, eds. *Borders in Cyberspace* (Cambridge: NUT Press, 1997).

Libicki, Martin C. "What is information Warfare?" Strategic *Forum* no. 28, May 1995.

Lindberg, Leon. *The Energy Syndrome.* (New York: **Heath,** 1977).

Matthews, Jessica Tuchman. "The Age of Non-State Actors" *Foreign Affairs* Vol. 76. No. I January/February 1997 pp. 50-66.

Moisey, Claude. "Myths of the Global Information Village" *Foreign* Policy Summer, 1997.

Molander, Roger C. Andrew S. Riddle, and Peter A. Wilson, *Strategic Information Warfare A New Face of War* (Santa Monica, CA: RAND, 1996).

Nye, Joseph, Jr., and Owens, William A. "America's Information Edge," *Foreign Affairs.* March/April 1996, pp.20-36.

Ronfeldt, David. "Institutions, Markets, and Networks: A Framework About the Evolution of Societies." (Santa Monica, CA: RAND, 1993).

Rothkopf, David. "In Praise of Cultural Imperialism?" *Foreign Policy* Summer, 1997.

Rutkowski, Anthony M. "Multilateral Cooperation in Telecommunications: Implications of the Great Transformation," in William J. Drake ed. *The New Information Infrastructure* (New York: Twentieth Century Fund Press, 1995).pp.223-250.

Schwartzstein, Stuart J.D. "Export Controls on Encryption Technologies," *SAIS Review,* Winter-Spring 1996. pp. 13-34.

Shultz, George P. "Diplomacy in the Information Age,"Keynote Address, *Virtual Diplomacy Conference.* Peaceworks No. 18. (Washington, D.C.:United States Institute of Peace, 1997).

Snyder, Alvin A. *Warriors of Disinformation: American Propaganda, Soviet Lies and the Winning the Cold War* NY: Arcade Publishers, 1995.

Solomon, Richard H. "The Information Revolution and International Conflict Management" Keynote Address, *Virtual Diplomacy Conference.* Peaceworks No. 18. (Washington, D.C.:United States Institute of Peace, 1997).

Steele-Vivas, Robert David. "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," *Government Information Quarterly.* Vol - 13, No. 2, 1996.

Strernlau, John. "Big Emerging Markets," *Foreign Policy* no. 94, Winter 1994-1995. p. 18.

Studeman, Adm. W.O. "The New Information Environment and National Security," presentation to The National Security Industrial Association, National Defense University, May 16, 1995.

Thurow, Lester *C. The Future of Capitalism: How Today's Economic Forces Shape Tomorrow's World* (New York: Penguin Books, 1996).

Wilson, III, Ernest J. "World Politics and International Energy Markets," *International Organizations* vol.4 1, no. 1, Winter 1987, pp. 125-149.

Wilson, Peter A. and Robert A. Manning and Col. Richard L. Klass, (ret.) "Defense in the New Information Age: A New Blueprint," Policy Report No. 26, Washington, D.C.: Progressive Policy Institute, 1995.

Wriston, Walter B. "Bits, Bytes, and Diplomacy." Keynote Address, *Virtual Diplomacy Conference.* Peaceworks No. 18. (Washington, D.C.:United States Institute of Peace, 1997).

Bibliography/Suggested Readings

Aspen Institute Program on Communications and Society. *Shaping the Future Telecommunications Structure* Queenstown, MD: Aspen Institute, 199 1.

Boal, lain A., "A Flow of Monsters: Luddism and Virtual Technologies," in *Resisting the Virtual Life: The Culture and Politics of Information,* James Brook and lain A. Boal, eds. (San Francisco: City Lights, 1995).p. 3-15.

Cowhey, Peter F. "The International Telecommunications Regime:The Political Roots of Regimes for High Technology" *International Organization* Vol. 44, No. 2, (Spring, 1990), pp. 149-176.

Drake, William J. *The New Information Infrastructure* New York: Twentieth Century Fund Press, 1995.

Dyson, Esther, George Gilder, Jay Keyworth, and Alvin Toffler. "A Magna Carta for the Knowledge Age," *New Perspectives Quarterly Vol.* 11, Fall 1994. Pp. 26-37.

Gellman, Robert. "Conflict and Overlap in Privacy Regulation: National, International, and Private," Conference Paper Presented at the Symposium on Information, National Policies and International Infrastructure, Kennedy School of Government, Harvard University, January 30, 1996.

Harasim, Linda M. Ed. *Global Networks: Computers and International Communication* Cambridge, MA: MIT Press, 1993.

Hills, Jill. *The Democracy Gap: The Politics of Information and Communication Technologies in the United States and Europe* New York: Greenwood Press, 199 1.

Jussawalla, Cheheroo. et al eds. *Information Technology and Global Interdependence* New York: Greenwood Press, 1989.

Nordenstreng, Kaarle and Herbert I. Schiller, eds. *Beyond National Sovereignty: International Communications in the 1990's* Norwood, NJ: Ablex Publishing Corp., 1993.

Ohmae, Kenneth. *The End of the Nationa State: The Rise of Regional Economics* (New York: The Force Press, 1995)

Oppenheimer, Michael F. "The Impact of Technology on Global Relations" (Unpublished Paper, December 1995).

Robinson, James. "Technology, Change, and the Emerging International Order," *SAIS Review* Winter-Spring, 1995.

Wasko, Janet and Vincent Mosko, eds. *Democratic Communication in the Information Age* Toronto: Garamond Press, 1992.

Wilson, Ernest J. III. "Inventing the Global Information Future" *Futures Vol 30,* No. 1. Forthcoming.

Wilson, Ernest J. 111. "Introduction: The What, Why, Where, and How of National Information Initiatives,"in Wilson and Kahin eds. *National Information Infrastructure Initiatives: Vision and Policy Design* (Cambridge:MIT Press, 1997).

Wriston, Walter B. *The Twilight of Sovereignty: How the Information Revolution is Transforming Our World* (New York: Charles Scribner and Sons, 1992).