CHAPTER 2

A FRAMEWORK FOR ANALYSIS

This section establishes a framework for understanding the status of the Internet and related capabilities within a country and the factors that led to current conditions and will likely influence future development. The "dimensions" represent a time-slice view that facilitates both assessment of the Internet within a country and comparisons between countries and regions. Compilation and analysis of the "determinants" and relevant government policies not only establishes how the current situation came to be, but can inform decision-makers of the likely consequences of future regulatory or investment decisions on the further development of Internet capabilities. Finally, the concept of national security is broken down into components that are affected by the proliferation of the Internet; these components and their relationship to the Internet are described in the final paragraphs of this section.

There are five basic issues of governance that every government seeks to address which, in turn, contribute to the establishment and maintenance of national power, which also has five principal elements. Table 1 lists these issues and elements.

Table 1. National Security Components

Issues of Governance	Elements of National Power
National Security	Political/Diplomatic
Internal Security	Coercive
Economic Viability	Economic
National Values	Technological
Process of Governing	Information

Governments, and most bureaucratic organizations, generally seek to maximize applicable elements of power as a means to enhance their ability to carry out their governance functions. Information technology (IT), including the Internet, can contribute to or hinder the attainment of these goals. The diffusion of the Internet presents the potential to impact these issues and elements through enhanced or novel information dissemination that offers opportunities and challenges to the established civil order.

Dimensions of Internet Diffusion

The knowledge that a country has a connection to the international Internet does not establish the significance of that connection to either domestic or international affairs. Once a connection is established, a country, and individual sectors within that country, attain an "Internet capability" that usually develops and grows more important over time. The Internet capability of a nation is based upon a number of interrelated factors that this framework[1] is represented along six dimensions (Tables 2-3 and 6-9), each of which attempts to quantify the degree of presence or an aspect of the Internet's employment. Of the six dimensions, three answer the question: "How much?"

[1] Adapted from the framework developed by Peter Wolcott for Peter Wolcott, Seymour Goodman, and Grey Burkhart, *The Information Technology Capability of Nations: A Framework for Analysis,* MOSAIC Group report (January 1997).

While the number of theoretically reachable hosts on the Internet is the network's "most fundamental metric,"[2] it is less useful for establishing the degree to which the Internet has been established and is being used in a particular country or region. This framework evaluates the extent of Internet presence and use based upon Pervasiveness, Geographic Dispersion, and Sectoral Acceptance. The final three dimensions reflect structural variables: Connectivity Infrastructure represents the degree to which users can effectively communicate via the Internet and the number and speed of a country's international connections. Organizational Infrastructure describes the richness and robustness of the Internet service provision market, and hence the potential for further proliferation. It also is the dimension that best reflects one of the most important variables in Internet diffusion, government policy. The final dimension, Sophistication of Use, represents the degree to which the technology has really caught hold within a country and become an integral part of that country's social, economic, and management fabric. In the following descriptions of the dimensions, the State of Qatar will be used to illustrate the application of each metric.

Pervasiveness is a function principally of the number of users per capita, but also reflects the growth of Internet use beyond a core group of technical experimenters and "early adopters" to the general public, and ease with which the population can get Internet service. The elements of pervasiveness are listed in Table 2. To be truly pervasive, the Internet must be available in the local

Table 2. Dimensions of Internet Diffusion: Pervasiveness

Level 0	*Non-existent:* The Internet does not exist in a viable form in this country. No computers with international IP connections are located within the country. There may be some Internet users in the country; however, they obtain a connection via an international telephone call to a foreign ISP.
Level 1	*Experimental:* The ratio of users per capita is on the order of magnitude of less than one in a thousand. There is limited availability, and use of the Internet is embryonic. Only one or a few computers are connected to the international IP network. The user community comprises principally networking technicians.
Level 2	*Established:* The ratio of Internet users per capita is on the order of magnitude of at least one in a thousand. The user community has been expanded beyond networking technicians.
Level 3	*Common:* The ratio of Internet users per capita is on the order of magnitude of at least one in a hundred. The infrastructure of supporting and related goods and services has become well-established, although is not necessarily extensive.
Level 4	*Pervasive:* The Internet is pervasive. The ratio of Internet users per capita is on the order of magnitude of at least one in ten. Internet access is available as a commodity service.

[2] Anthony M. Rutkowski, "Internet Hosts Approach 20 Million As Growth Shifts from Exponential to Linear," Global Communications Newsletter, p. 1, in *IEEE Communications Magazine* 35 (October 1997).

area of every citizen, either due to the proximity of servers and Internet service providers (ISP), or the ubiquity of toll-free service available over good quality telephone lines.

For example, the national telephone company of the State of Qatar, Qatar Public Telecommunications Company (Q-Tel), began offering public access Internet services in mid-1996 and had about 8,200 users one year later. With a population of 550,000, that means that the penetration of the Internet is about 1.5 percent, resulting in a rating of Level 3 (Common) for the Pervasiveness dimension, which is typical of the wealthier countries in the region.

Geographic Dispersion describes the physical dispersion of the Internet within a country, there being benefits to having multiple points-of-presence, redundant transmission paths, and multiple international access points. Internet development in a country typically starts with a single provider and site in the capital or largest population center, from which the infrastructure spreads out as the user population grows and becomes more diversified. A mature Internet network will feature an infrastructure distribution that is proportional to the population. Table 3 summarizes the characteristics used to evaluate geographic dispersion.

Table 3. Dimensions of Internet Diffusion: Geographic Dispersion

Level 0	*Non-existent:* The Internet does not exist in a viable form in this country. No computers with international IP connections are located within the country.
Level 1	*Single Location:* Internet points-of-presence are confined to one major population center. There is an international IP link from only one city.
Level 2	*Moderately Dispersed:* Internet points-of-presence are located in at least half of the first-tier political sub-divisions of the country. There is an international IP link from only one city.
Level 3	*Highly Dispersed:* Internet points-of-presence are located in at least three-quarters of the first-tier political sub-divisions of the country. There are international IP links from two or more cities.
Level 4	*Nationwide:* Internet points-of-presence are located in all first-tier political sub-divisions of the country. Rural access is publicly and commonly available. There are international IP links from more than two cities.

In Qatar, there is only a single Internet point-of-presence and international link. They are both in Doha, which is also the main population center. Thus, geographic dispersion in Qatar is at Level 1 (Single Location) and is likely to remain at that level, given the small size of the country and the concentration of its population in the capital.

Sectoral Absorption recognizes the differing impacts of the degrees to which four major Internet-using sectors of society have taken up the technology: the academic, commercial, health, and public (government) sectors. While the sectors describe the major social and economic divisions in society, none are homogeneous, as depicted in Table 4. Personal use is not considered in this metric.

Internet use within each sector is rated as rare, moderate, or common, according to the guidelines listed in Table 5. To rate the country as a whole, each sector with a “rare” rating is assigned one point, each “moderate” sector two points, and each “common” rating three points. The overall rating for Sector Absorption is derived from the matrix shown in Table 6.

Table 4. Subsectors of the Social Structure		
Sector	Subsectors	
Academic	Primary and Secondary education University education	
Commercial	Distribution Finance Manufacturing	Retail Service
Health	Hospitals Clinics	Research Centers Physicians/Practitioners
Public	Central government Regional and Local governments Public companies Military	

Table 5. Assessing Sectoral Absorption			
Sector	Rare	Moderate	Common
Academic-primary and secondary schools, universities	< 10% have leased-line Internet connectivity	10-90% have leased-line Internet connectivity	> 90% have leased-line Internet connectivity
Commercial-businesses with more than 100 employees	< 10% have Internet servers	10-90% have Internet servers	> 90% have Internet servers
Health-hospitals and clinics	< 10% have leased-line Internet connectivity	10-90% have leased-line Internet connectivity	> 90% have leased-line Internet connectivity
Public-top and second tier government entities	< 10% have Internet servers	10-90% have Internet servers	> 90% have Internet servers

Table 6. Sectoral Absorption Rating		
Sectoral point total	Absorption dimension rating	
0	Level 0	Nonexistent
1-4	Level 1	Rare
5-7	Level 2	Moderate
8-9	Level 3	Common
10-12	Level 4	Widely used

With respect to Qatar, at this stage of development the principal users of the Internet are commercial and government organizations. While exact figures are not available, the take-up is apparently between 10 and 90 percent in both of these sectors. Neither the academic nor the health sector has started to use the Internet, however. This results in ratings from Table 5 of zero

for the academic and health sectors, and two each for the commercial and public sectors, for a total of four points. Thus, Qatar receives a Sectoral Absorption rating of Level 1 (Rare) from Table 6.

Connectivity Infrastructure comprises four components: the aggregate bandwidth of the domestic backbone(s), the aggregate bandwidth of the international IP links, the number and type of interconnection exchanges, and the type and sophistication of local access methods being used. Table 7 depicts how these factors are related to the assessment of the infrastructure's level of development, with Level 0 assigned to a country with no Internet presence (and hence, no infrastructure) and Level 4 assigned to a country with a robust domestic infrastructure, multiple high-speed international links, many bilateral ("peering") and open Internet exchanges—facilities where two or more IP networks exchange traffic, and a variety of access methods in use.

Table 7. Dimensions of Internet Diffusion: Connectivity Infrastructure

	Domestic Backbone	International Links	Internet Exchanges (IX)	Access Methods
Level 0	None	None	None	None
Level 1	< T-3[3]	≤ 128 Mbps	None	Modem
Level 2	T-3 — OC-4[4]	T-1[5] — T-3	1	Modem 64 Kbps leased lines
Level 3	OC-4 — 100 Gbps	T-3 — 10 Gbps	More than 1; Bilateral or Open	Modem > 64 Kbps leased lines
Level 4	≥ 100 Gbps	≥ 10 Gbps	Many; Both Bilateral and Open	< 90% modem > 64 Kbps leased lines

Qatar does not at present have a domestic IP backbone (Level 0), since the servers are concentrated at one location. There is only a single international link to the Internet, but at 2.048 Mbps it is relatively large (Level 2). There are no Internet Exchanges within Qatar, as it connects to other Internet-connected networks in the United States (Level 0 or 1). Connections available within Qatar to Q-Tel's servers include dial-up lines at conventional (up to 28.8 Kbps) speeds and 64 Kbps leased lines (Level 2). Although Qatar's configuration does not fall explicitly into one of the rows (levels) on Table 7, the overall lack of infrastructure, despite some modern elements, suggests that the country should be rated as Level 1.

Organizational Infrastructure Just as the connectivity infrastructure assessed the extent and robustness of the physical structure of the network, organizational infrastructure (Table 8), derived from the number of ISPs and the competitive environment, assesses the robustness of the market and services themselves. Generally, an open, competitive market with low barriers to market entry is more conducive to high rates of take-up by subscribers, wider proliferation of the physical infrastructure, and the provision of a wider variety of services.

[3] 44.736 Mbps
[4] 207.360 Mbps
[5] 1.544 Mbps

Table 8. Dimensions of Internet Diffusion: Organizational Infrastructure

Level 0	*None:* The Internet is not present in this country.
Level 1	*Single:* A single ISP has a monopoly in the Internet service provision market. This ISP is generally owned or significantly controlled by the government.
Level 2	*Controlled:* There are only a few ISPs because the market is closely controlled through the maintenance of high barriers to entry. All ISPs connect to the international Internet through a monopoly telecommunications service provider. The provision of domestic infrastructure is also a monopoly.
Level 3	*Competitive:* The Internet market is competitive and there are many ISPs due to the existence of low barriers to market entry. The provision of international links is a monopoly, but the provision of domestic infrastructure is open to competition.
Level 4	*Robust:* There is a rich service provision infrastructure. There are many ISPs and low barriers to market entry. The provision of international links and domestic infrastructure are open to competition. There are collaborative organizations and arrangements such as public exchanges, industry associations, and emergency response teams.

In Qatar, as with all of the other countries in the Persian Gulf region, the telephone company is a public organization with a monopoly on the ownership of the telecommunications infrastructure and the provision of telecommunications services. The provision of Internet services is considered part of this monopoly, and no privatization or licensing of competitive operators is under consideration. Qatar thus receives a rating of Level 1 (Single) for Organizational Infrastructure.

Sophistication of Use To truly understand the Internet capability of a country, it is necessary to understand not only how many and where people use the services, but how the Internet is employed. Of particular interest is the "elbow" reached when the service is mature enough to attract interest and use outside the narrow community of technicians. A second major milestone is reached when the user community transitions from only using the Internet to creating new applications, sometimes eventually having an impact on Internet use elsewhere. Table 9 depicts the development stages that reflect an increasing sophistication in the use of the Internet.

To the extent that Internet use has been taken up in Qatar, the usage appears to be conventional (Level 2), with subscribers using the Internet to automate such routine functions as messaging (substituting e-mail for telephone and facsimile) and research (using the Worldwide Web). News dissemination and advertising are also being experimented with by the state's satellite television station and commercial organizations. As yet, however, there is no evidence that use of the Internet is transforming Qatari bureaucratic life in any substantive way.

Proximity to the Technological Frontier, one of the dimensions used in the earlier Wolcott, *et al.*, framework, has been omitted from this analysis. At this stage of the development and proliferation of the Internet, the hardware and software used is relatively uniform, and the state-of-the-art has not advanced far beyond current commercial deployments. The Internet itself may be considered the current state-of-the-art in wide-area networking; those less proximal to the technological frontier are using legacy networking protocols such as X.25. Given the current homogeneity, adding a seventh dimension to the current analysis would not be useful in differentiating between types of Internet deployments or use. However, this situation will change over the next several

years, as advanced protocols, such as the Resource Reservation Protocol (RSVP) and Internet Protocol version 6 (IPv6), and improved routers and transmission equipment are fielded. Countries or ISPs that do not continue to invest in new equipment and software will fall behind the commercially-deployed state-of-the-art, producing another level of differentiation in Internet development.

Table 9. Dimensions of Internet Diffusion: Sophistication of Use

Level 0	*None:* The Internet is not used, except by a very small fraction of the population that logs into foreign services.
Level 1	*Minimal:* The small user community struggles to employ the Internet in conventional, mainstream applications.
Level 2	*Conventional:* The user community changes established practices somewhat in response to or in order to accommodate the technology, but few established processes are changed dramatically. The Internet is used as a substitute or straight-forward enhancement for an existing process (e.g., e-mail vs. post). This is the first level at which we can say that the Internet has "taken hold" in a country.
Level 3	*Transforming:* The user community's use of the Internet results in new applications, or significant changes in existing processes and practices, although these innovations may not necessarily stretch the boundaries of the technology's capabilities.
Level 4	*Innovating:* The user community is discriminating and highly demanding. The user community is regularly applying, or seeking to apply the Internet in innovative ways that push the capabilities of the technology. The user community plays a significant role in driving the state-of-the-art and has a mutually beneficial and synergistic relationship with developers.

The six dimension ratings for Qatar from the preceding analysis are depicted in Figure 1 and summarized in Table 10.

The shape of a single hexagram is not very informative, although in the case of Qatar it does suggest that the popularity of and degree of comfort in using the Internet have out-stripped development of the infrastructure. This is the pattern that one might expect of a government-monopoly situation, in which the service provider has limited motivation to respond to consumer demands. Comparing the hexagrams developed for the countries assessed in this report with the national determinants of the Internet's dimensions may provide insight into commonalties in development patterns.

Figure 2 shows a time-series representation of Qatar's Internet development, starting from a uniform Level 0 before the Internet was introduced, through the initial installation and commissioning to the level at which it exists today. Over the past year, the Pervasiveness and Sophistication

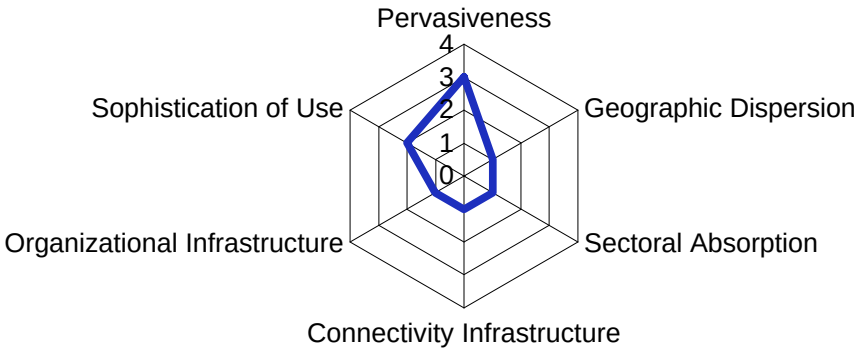

Figure 1. Internet Dimensions for Qatar

Dimension	Level	Explanation
Pervasiveness	(3) *Common*	Qatar has about 8,200 Internet users, more than one user for every 100 people. Use of the Internet has spread beyond a core of computing professionals.
Geographic Dispersion	(1) *Single Location*	Internet servers are located at only a single site and international connectivity is from this one location.
Sectoral Absorption	(2) *Moderate*	The Internet is in moderate use in two of the four sectors, but virtually not at all in the other two.
Connectivity Infrastructure	(1)	There is little connectivity infrastructure in Qatar, principally due to geography and the distribution of the population. Such infrastructure that exists is modern but not robust.
Organizational Infrastructure	(1) *Single*	There is a single ISP in Qatar, the state monopoly telecommunications company. There are no plans for privatization or competition.
Sophistication of Use	(2) *Conventional*	The Internet is used to enhance current processes, such as messaging, without fundamentally changing those processes.

Table 10. Internet Dimensions for Qatar

of Use have increased, while the other dimensions have remained static, as the general public and government employees signed on and became familiar with the networks basic functions. Based on the country's geography and government policy toward telecommunications, the Geographic Dispersion and Connectivity and Organizational Infrastructures dimensions are expected to remain static for the foreseeable future. The Pervasiveness dimension is likely to continue growing, and along with it the Sectoral Absorption dimension, as Internet use proliferates throughout Qatari society. Whether or not the Sophistication of Use dimension will grow over time will be determined by a number of factors, including government policy and education, social acceptance

of the Internet, and the openness of the various social sectors to new ways of functioning that could be facilitated by the Internet.

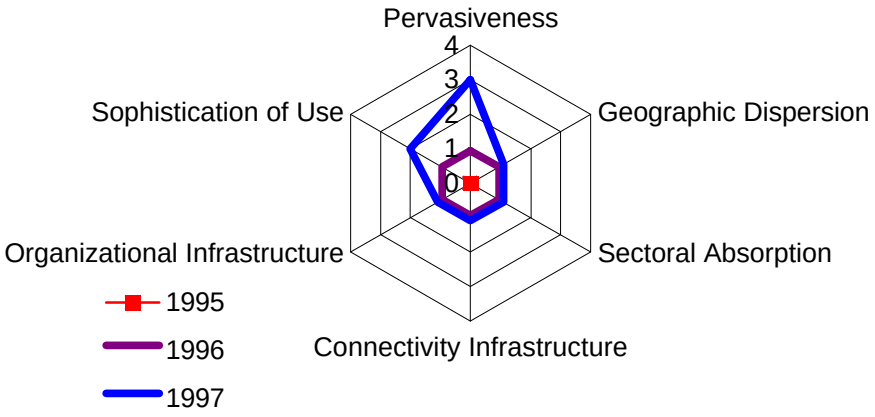

Figure 2. Internet Development in Qatar

Determinants

Understanding a country's current capabilities with respect to the Internet is crucial to understanding how that country or its various sectors of users might use the Internet to achieve particular objectives. Equally important, however, is an analysis of the factors—the determinants—that influence that capability and shape its development over time. The current dimensions of a country's Internet capabilities resulted from the interactions of these determinants, which were in turn affected by the diffusion of the Internet. A country's future Internet capabilities will continue to be the result of the actions and interactions of these dimensions, most of which are not themselves static. Not every government policy nor all of the determinants discussed in the following paragraphs will be addressed for every country studied. Discussion of these elements will be limited to those policies or determinants that have had a significant impact on the diffusion of the Internet.

The Role of Governments

The most important determinant, government policy, belongs in a category by itself, since the policies of government overlay all other determinants, affecting both their nature and their effectiveness, based upon a government's ability to exercise coercive power. The policies created by a government are generally intended to achieve the fulfillment of that government's goals, which may be more or less closely related to the goals of those governed, depending upon the form of government. The government's policies may also appear to be more or less rational, depending upon how well the policy reflects the realities of its milieu, but governments can—and all too often do—create policies that reflect a lack of awareness or understanding of its environment, or an excessive optimism regarding the government's ability to overcome obstacles to its policies. Government policies that affect the development of the information technologies in general and the Internet in particular are listed in Table 11.

Table 11. Government Policies	
Policies	Examples
Economic	State monopolization of the telecommunications sector Licensing policies and other barriers to competition Taxation/fees Collaboration or competition with private sector Loans and subsidies to attract capital Capitalism vs. degree of statist control Foreign investment restrictions, incentives
Foreign Relations	Diplomatic relations Trade relations
Information	Content and dissemination controls
Politics	Responsiveness to cultural concerns
Security	Internet access controls Encryption Surveillance of population Dissidents Computer crime Infrastructure protection
Technology	Development Research and development investment Transfer of technology Standards
Social Equity	Equal access to IT resources Redistribution of wealth Human resources and education investment Educational content and standards Public projects

Economic policy lays the groundwork for the competitive environment. Government policy toward the Internet in this respect, and to telecommunications more generally, falls into two categories: a tightly controlled market with a single monopoly provider or a few licensed providers, or an open market generally featuring many competing providers. Competition policy is often closely related to information policy. Developing countries, especially, often consider telecommunications a strategic resource with significant national security considerations. The Internet in particular has been a source of national security concern to countries with closed political systems. Pricing can be used both to limit competition (e.g., high entry costs, such as licensing fees) and access (e.g., high subscription costs).

A government's investment choices may affect the development of the Internet, again especially in developing countries, to the extent that such technological development is either the exclusive domain of the government or heavily dependent upon government subsidies. These are closely related to the national technology policy, whether or not such a policy has been made explicit.

Some countries may experience difficulty in getting and developing an Internet capability because of a lack of foreign exchange (to pay for the international connections) and/or poor or adversarial

relations with neighboring or regionally important countries which hamper developing open information borders and international communications links.

Telecommunications in general and the Internet in particular are very dependent upon the acceptance of international standards. In the case of the Internet, these standards have been entirely voluntary; i.e., if one wanted an Internet connection, one established a link using the appropriate protocols; if one did not wish to adhere to the Internet standards, one simply could not connect. The issue of whether Internet standards should be taken under the purview of an international standards organization, such as the International Telecommunications Union (ITU) or International Standards Organization (ISO), is currently being debated.

Social policies are also relevant to the development of the Internet. The Internet is viewed by many as a potential source of unlimited information, whereby a developing country may advance more rapidly than before, and as a means for enhancing interactions between domestic and foreign scientists and researchers. On the other hand, almost every country has some concerns regarding the variety of information potentially available via the Internet, particularly pornography, weapons-related information, and hate-incitement sites.

Determinants of Internet Capacity

Porter postulated four basic determinants of national advantage, which serve here to describe the general nature of the determinants of Internet diffusion. *Factor conditions* refer to the factors of production, the inputs for any industry or enterprise. The *Constituents*, which Porter called "demand conditions" describe the nature of the market with respect to the demands of sophisticated users, the breadth and variety of demands, and the size and patterns of demand growth. Porter notes that the quality of demand is more important than the quantity of demand. *Related and supporting industries* refers to the quality of industries required for the introduction and development of, in this case, the Internet, and the relationships between industries. *Strategy, structure, and rivalry* refers to the ease of formation of new companies, barriers to market entry, and the competitive environment.[6]

Factor Conditions. Table 12 lists the seven factor conditions that appear to have meaningful direct or indirect effects on the development and diffusion of the Internet. Each factor comprises several (or more) components; the lists in Table 12 and the tables that follow are not exhaustive, but represent those components that appear to have the most bearing on Internet diffusion. While most of these factor conditions are subject to change caused by outside influences, such change, when it occurs, is generally slow and incremental. Other factor conditions, such as geography and natural resources, cannot be changed to any meaningful degree, although the exploitation of these factors may affect the long-term viability of particular government policies.

[6] Michael E Porter, *The Competitive Advantages of Nations* (New York: The Free Press, 1990), pp. 71-72. Porter's "firm strategy, structure, and rivalry" was shortened to "strategy, structure, and rivalry" for clarity in the context of Internet development.

Table 12. Determinants: Factor Conditions	
Factors	Examples
Culture	Technical orientation/openness to innovation Language Religion Cultural defensiveness/sensitivity
Geography	Obstacles to infrastructure development
Human resources	Demography Education/skill levels Work ethic
Financial resources	Liquid assets Investment sources Obstacles to flows of capital
Technological resources	Level of IT development
Infrastructure	Domestic telecommunications International telecommunications Data networking
Natural and Material resources	[these may have conditioned other determinants, but do not appear to have any direct effect on Internet diffusion]
Information resources	Availability of technical information Free flow of foreign information
Bureaucracy	Decision-making structures and methodology Collaboration vs. competition within bureaucracies Collaboration vs. competition between bureaucracies Presence of competing bureaucracies

Constituencies The Internet, like other technologies and innovations, usually does not simply appear in a particular country; it is introduced into the country to satisfy the demands of one or more constituent groups, such as the business or academic communities. The strength of these constituencies and their demands relative to conditions either supporting the *status quo* or specifically opposed to the Internet determine whether efforts to develop the Internet in a particular country will be successful, and are major factors in the speed with which Internet service proliferates. Table 13 describes some of the major constituencies of the Internet.

Related and Supporting Industries. The presence and condition of supporting industries (Table 14) is generally not as critical to Internet diffusion as it is to industrial activities. Related industries such as software development concerns can, however, act as a spur to Internet diffusion. Most important is the degree of development of the telecommunications infrastructure, the nature of the sector (monopoly or open), and the relationship between telecommunications operators and ISPs.

Table 13. Determinants: Constituencies	
Groups	Examples
Stakeholders	Communities: Academia, Business, Religious community, Politicians, Security Champions: traditionally the academic community in the case of the Internet.[7]
Potential consumers	Commercial Individual Trained and demanding users

Collaboration between the existing telephone company/companies and new Internet operators increases the rate of Internet development and can also increase the rate of its geographic dispersion.

Table 14. Determinants: Related and Supporting Industries	
Factors	Examples
Collaboration	Between the public and private sectors Between private sector organizations
Industry	Existence of supporting industries Stress on supporting industries Degree of reliance upon supporting industries
Information	Content providers Content creators

Strategy, Structure, and Rivalry factors (Table 15) assess the condition of the marketplace, especially barriers to market entry and anti-competitive practices, and the climate for innovation and

Table 15. Determinants: Strategy, Structure, and Rivalry	
Factors	Examples
Competitive environment	Barriers to Internet market entry Collaboration between private and public sectors Costs and prices Market concentration
National innovation environment[8]	Educational system Research and development organizations

entrepreneurship. A number of scholars have identified a competitive environment as a particularly strong determinant of technological capability.[9] Costs and pricing also come into play, as the

[7] Tim Kelly, H. Shawn Sharifi, Ben Petrazzini, *Challenges to the Network: Telecommunications and the Internet* (Geneva: International Telecommunications Union (ITU), September 1997), p. 15.

[8] Nelson, *ibid*.

[9] David C. Mowery and Joanne E. Oxley, "Inward technology transfer and competitiveness: the role of national innovation systems," *Cambridge Journal of Economics* 19 (February 1995), pp. 67-93; Michael A. Cusumano and Detelin Elenkov, "Linking international technology transfer with strategy and management: A literature commentary," *Research Policy* 23 (1994), pp. 195-215; Sanjaya Lall, "Policies for building technological

cost of establishing and operating an Internet service can be a significant barrier to market entry, a notable if implicit control on information technology in some countries, and the pricing of services is a major factor in the take-up of Internet connections by potential subscribers. Internet service may be price-inelastic, with at least private users still regarding Internet service as a discretionary purchase.

Governance and Elements of National Power

Having achieved an understanding of the status and history of the Internet in the countries covered by this study, and having assessed the factors that affected, and are likely to continue to affect, the development and diffusion of the Internet, we now turn to the question of what difference this diffusion makes to governments: how has (does) the rapid diffusion of the Internet affect the ability of governments to perform their traditional roles and functions or take on new functions, and how does use of the Internet affect the relationship between the government and those governed? This section reviews the major issues of governance and elements of a country's national power with a view toward determining what, if any, impact the diffusion and employment of the Internet by governments, average citizens, dissidents and others outside the mainstream, criminals, or foreign powers might have on the stability of each country and the related impact on U.S. national security.

The Internet has alternatively been characterized by various groups and countries as a major threat or a technological panacea for the world's ills. There are serious concerns about the access that the Internet might give malevolent individuals, groups, or powers to vital infrastructure elements such as the electrical power system or a country's financial network. The Internet, in principal, provides an international audience for anyone with a cause and a computer, but is anybody even listening, much less affected? Dissident groups have been quick to take up new communications technologies as they appear, and are making prodigious use of the Internet. To what effect? On the other hand, viewed as an enabling technology, it has been proposed that the unique form of inter-personal communications provided by the Internet (i.e., asynchronous, not face-to-face, potentially anonymous) will foster better relations between antagonistic parties and even countries. The potential for access to a wider range of more timely information about the activities of one's (or someone else's) government, coupled with a ready feedback mechanism that can also be used to rally support provides the potential for citizens to more directly attempt to influence the activities of government. The same attributes also give a government more opportunity to promulgate its views and cast its actions in the best light while identifying potential trouble-makers. Is the Internet, then, good or bad? There is no universal answer, although in the long run earlier improvements in communications technology (e.g., telegraph, telephone, radio and television broadcasting) have contributed to the raising of mankind's standards of living. A careful mapping of the potentialities of Internet usage to the critical functions and attributes of government can reveal specific concerns and areas of potential future problems or benefits within the context of the various countries being studied.

capabilities: lessons from Asian experience," *Asian Development Review* 11 (1993), pp. 72-103; Richard R. Nelson, "A Retrospective," chapter 16, in Richard R. Nelson, ed., *National Innovation Systems: A Comparative Analysis* (New York: Oxford University Press, 1993), pp. 505-523; Kelly, *et al*., pp. 10-11.

Issues of Governance

For the purpose of assessing the relationship between technology and national security concerns, we have postulated five basic functions of government that are affected, in both positive and negative ways, by the implementation of modern international communications media. Most, if not all, legitimate functions of government are subsumed by one of these basic functions.

National Security The principal national security function of governments is to protect the country's citizens from foreign threats. This is generally interpreted to require the insurance of the sanctity of citizens and property both within and outside the country. The degree to which countries attempt to protect their citizens or their citizens' property outside the country varies greatly. Most countries are signatories to one or more mutual or collective defense pact that adds the requirement to assist other pact members in the event of attack. Some countries, such as the United States, define the defense of certain other foreign countries as an essential national security requirement. With respect to the Middle East, "assuring the security of Israel and our Arab friends and maintaining the free flow of oil at reasonable prices" are currently defined as fundamental task of American national security strategy. Additionally, "[t]he United States remains focused on deterring threats to regional stability, particularly from Iraq and Iran as long as those states pose a threat to U.S. interests, to other states in the region and to their own citizens."[10]

The implementation of a national security strategy in the structuring of armed forces and definition of a military strategy is predicated in large part on the location of people, objects, and territory to be protected (defended). This implementation is generally broadened to include the protection of key transit routes for critical (or more) imports, and possibly exports, and outbound transit routes for military forces whose mission is extra-territorial. Up until the "information revolution," the locus of these subjects of defense has been on land, in the water, or airborne. If indeed "information is becoming a strategic resource,"[11] then not only must the physical information infrastructure (e.g., computers and communications links) be defended, but national defense must be extended to cyberspace.

In addition to possibly becoming a locus and transit zone of objects of value (information), the Internet may support or undermine national security objectives to the extent that it can be used for intelligence collection and the propagation of misinformation.

Internal Security The effect of the Internet on the maintenance of internal security is one of the most important concerns of many governments. At the same time, internal security is important to a country's citizens and one of the most visible results of governance. Benefits to the citizen include the maintenance of internal order, a legal system, and a civil society that contribute to the personal safety and well-being of each citizen, ideally in equal measure. People may view internal security as a threat to their civil liberties to the extent that governments wield their power repressively. Government repression is more common, pervasive, and severe in countries with un-

[10] *A National Security Strategy of Engagement and Enlargement* (Washington, D.C.: The White House, February 1996), p. 30.

[11] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" in Arquilla and Ronfeldt, eds., *In Athena's Camp: preparing for conflict in the information age* (Santa Monica, CA: RAND, 1997), p. 25; reprinted from *Comparative Strategy* 12 (Spring 1993), pp. 141-165.

elected governments, which may have reason—and certainly believe that they have reason—to mistrust some portion of the population, including expatriates and émigrés.

The issue of individual empowerment via the Internet may be viewed as positive or negative, or a mix, depending upon the government's situation and objectives. While the empowering aspects of the Internet have been oversold (e.g., the common declaration that the Internet gives everyone a voice that can be heard around the world.), it certainly provides contacts and outlets not normally available to individuals. Empowerment is a particularly complicated question in conservative societies (which may or may not be repressive, but usually must be so to some extent to maintain their conservative character), such as those typically found in Islamic countries. In a society where "the rights of the community supersede the rights of the individual,"[12] typical of not only Islamic but many other non-Western cultures, a medium that facilitates the creation of new communities—"virtual communities" that often cross international borders—may be a cause for concern to the extent that these new communities may have no particular loyalty to or even use for various national governments. At the same time, in conservative Islamic societies, where women are restricted in their public movements and contacts, the Internet is viewed as a potential source of "virtual liberation" because of its potential for providing impersonal and even anonymous contact with the world at large.[13] It has yet to be decided whether "contact" through some contact-less medium such as a Usenet newsgroup between a woman and a man to whom she is not related is *halal* (permitted) or *haram* (forbidden) under Islamic law.

To the extent that a government believes that its grip on power is insecure, one of the forms of repression is the control on the content and dissemination of information, especially but not limited to information about the activities of the government and its prominent officers. The Internet is thus viewed as a potentially ominous expansion of the threat from opposition groups, including otherwise patriotic opponents, dissidents, and potential revolutionaries. Although the Internet is not as ubiquitous as the telephone, it has the potential to become so, in the worst case view, with the additional capability to create record materials (as opposed to ephemeral voice communications) that can be widely promulgated, including worldwide.

These threats to internal security are often not well-understood, and the opportunity cost (or in some cases the real cost) of information control is equally or more obscure, making any reasonable cost/benefit ratio calculation unfeasible. Thus, governments that perceive themselves to be threatened by increased information flows generally follow the more conservative route of controlling as much as possible. Some countries, most notably Iran, have taken the conscious decision to attempt to open themselves up to information flows that will enhance development and raise the standard of living while "protecting" themselves from undesirable or potentially dangerous information.

Computer crime is an area not well-understood in many areas of the world; indeed, OECD countries have not completely formulated either the dimensions of threats or potential countermeasures. To the extent that the Internet creates additional exploitable connections between locations and objects of value (e.g., goods available via electronic commerce), avenues for computer crime are opened up. In addition to the difficulty in detecting computer crime, identifying and locating the perpetrator is often much more difficult, especially if the criminal is located outside the country where the crime is committed (e.g., computer system violated or country of origin of stolen

[12] Prince Sultan bin Salman, personal communication, al-Riyahd, Kingdom of Saudi Arabia (20 May 1997).
[13] *ibid.*

items of value). Finally, even when a criminal is caught, establishing guilt—linking the criminal with the crime for an outside audience (the jury), which is likely not conversant in computer science—represents a final and often insurmountable obstacle at this juncture.

Economic Viability Although the citizenry of capitalist countries may turn to the government as the guarantor of economic well-being only as a last resort, government policy and financial activities play a major role in ensuring (or destroying) that well-being on a continual basis. It is a case where the government may receive little or no credit for good conditions, but is certain to be blamed for economic down-turns. The government additionally sets the rules for domestic and international commerce and maintains the means of exchange.

One of the most visible effects of the proliferation of the Internet is the potential for the dissociation of the government from its tax base as (if) commerce becomes more electronically-based.[14] Mail order commerce has already created tax collection problems that have been only incompletely ameliorated, although the physical movement of goods in the postal system permits governments to maintain control over international mail order commerce. To the extent that the Internet is used for the purchase of non-electronic goods, this will continue to be the case. However, much of the current electronic commerce, and thus far one of the apparent advantages of Internet commerce, is the rapid, electronic delivery of goods and services (principally software, but also news and other periodical services, images, and database resources). These transactions are currently un-taxed, and Western governments have thus far elected not to attempt to impose a (likely unworkable) tax regime on Internet commerce, but poorer or cash-strapped countries that rely heavily on tax and customs revenue may not take the same approach.

Although a global economy was created and is becoming increasingly more integrated through the implementation of financial data networking (including electronic funds transfers) and the automation of stock markets and exchanges, the use of the Internet by both the financial sector and its clients has increased the degree of interrelatedness of the world's economies. Due principally to security concerns, the financial sector is not yet making (and may never make) extensive direct use of the Internet. However, its participation in the Internet has increased the availability and timeliness of financial and economic data to the general public nearly worldwide. This has resulted in increases in the pace of trading and the number and variety of participants. This may in turn result in increased volatility in markets and a diminished market responsiveness to government attempts at stabilization.

To the extent that data and information are valuable in and of themselves, and some forms may be considered "strategic assets" by some states, there may emerge efforts on the part of some countries to control access to and/or the flow of information over the Internet for reasons of economic security.

As noted in the previous section, computer crime is increasing and is likely to be exacerbated by the proliferation of the Internet. In addition to the internal security and legal aspects of this problem, there are often direct, and always indirect, economic costs. The protection of intellectual property rights (IPR), a problem not yet completely solved in the non-electronic world, poses unique problems with respect to the Internet. In addition to the lack of consensus as to whether

[14] Richard Solomon, presentation at the Highlands Forum X, Chantilly, Virginia, 12 November 1997. Dr. Solomon is the president of the U.S. Institute of Peace.

and to what degree to enforce IPR on the Internet, it is presently unclear how this could be reliably accomplished.

National Values is another area of governance where the government's intervention is generally unseen and unsought in the absence of specific threats. As the "national conscience," however, and wielding the regulatory power of the state, the government has broad powers to affect the long-term value structure of society in general. National values include issues related to culture and language, religion and morality, privacy, and the philosophy of government (i.e., democratic principles). The Internet's effect on any of these areas can be positive or otherwise.

Civil libertarians hail the Internet as a new social leveler because of the facelessness, and potential anonymity, of personal interactions, similar to the Saudi view of the effect of the Internet on the "liberation" of Islamic women previously noted. This same potential for anonymity, however, offers enhanced opportunities for criminal activity and also empowers people to act in various other socially unacceptable ways that would be unacceptable in the context of a face-to-face confrontation (e.g., threatening or offensive language). The U.S. Department of Justice has proposed that the Internet protocols be modified to include source identifying information in every packet to overcome the problem of anonymity-enhanced crime and antisocial behavior, a solution, however, that one of the co-inventor of the existing Internet protocols said is unworkable.[15]

Privacy advocates, most commonly in some Western countries such as the United States and in Scandinavia, have expressed concern about the enhanced ability to collect personal information provided by Internet-based transactions, as well as violations of personal privacy possibly arising from various service sites on the Internet, such as the U.S. Social Security Administration's. Law enforcement officials in countries without such a strong civil libertarian current, however, probably view with favor the potential ability to extend surveillance via the Internet. Officials of more repressive governments might also welcome additional surveillance and data collection capabilities were it not for other, more serious, concerns about the negative aspects of the Internet.

The related issues of culture, language, morality, and religion those most commonly cited by governments or citizens advocating strict control over the Internet. The Internet, having been invented in the United States (by the Department of Defense, no less), is viewed in many societies as yet another American device to export American culture, overwhelming local values and superseding tradition, effectively invalidating alternative cultures. The issue of language is tied in with cultural questions, but has more far-reaching implications in that in today's largely English-language Internet opportunities are limited for those with an inadequate command of the English language. Even such a modern Western country as France officially (in its legal code) objects to the overwhelming use of English on the Internet. Middle Eastern, Asian, and African cultures that have long been required to learn English in order to interact with the rest of the world are now finding themselves in the position of needing to know at least some English in order to send e-mail to their own countrymen. Even in countries, or social groups, unconcerned about American cultural or English-language "imperialism," there are concerns about the long-term effects of the breaking down of spatial and temporal barriers between cultures, especially when the foreign cultures' value systems are significantly different or are contrary to local norms.

[15] "Internet Change Is Focus of International Law Enforcement," *Consumer Multimedia Report* (22 December 1997).

Among the moral issues, the availability of pornography on the Internet has raised concerns almost everywhere. Many countries attempt to control the production and dissemination of pornography, although the degrees of both legal sanctions and enforcement vary considerably. Typically, both are more restrictive, the more conservative the social milieu.

The issue of the availability of information on the Internet that is contrary to local values and/or laws (which reflect a mixture of local values and uniquely governmental concerns) is a major factor in the process of deciding whether and how to implement Internet services in Islamic countries. Access to pornography, which however mainly reflects a desire to acquire pornography on the part of those accessing it, and religious proselytization, generally by e-mail and therefore unsolicited, are major concerns, along with such social issues as the availability of information about how to commit suicide are often-cited concerns of mainly government and religious officials but also many citizens. For example, although the government of the United Arab Emirates (UAE) did not view the availability of pornography as a major issue (because it is merely available, not delivered unsolicited), initially no restrictions were placed on Internet access. However, citizens who became aware of the kinds of information potentially available to their children raised an outcry through the Parent-Teachers' Association in the Emirate of Dubai, with the result that controls were eventually instituted nationwide (see the section on the UAE for details).

In countries used to strict information control, generally through a combination of government and self-censorship, it appears incomprehensible that such socially undesirable material could not only be available on the Internet, but in such apparently large volumes. The natural tendency is to insist that this material be controlled at the source (i.e., censorship by the government of the country of origin). However, there is a growing awareness that such control is impossible in the absence of a nearly global effort, which implies the requirement for consensus on what material is morally objectionable. Although such a consensus is unlikely to be achieved on a multi-cultural basis, there is the possibility of cooperation between Islamic states.

Process of Governing refers to the routine tasks of a government in exercising its authority and managing itself and the country. As with the four issues already discussed, the Internet has created opportunities and problems for governments in the conduct of their daily affairs.

The most significant application of the information technologies to the process of government has been in the area of automation of government activities, a process that has been underway in the West for three decades but is only just beginning in many developing countries. The diffusion of Internet technology provides the additional potential to create or extend government networks relatively simply, and to offer new services (or existing services in a new way) to citizens via a public Internet presence.

Individuals are not the only ones who can be empowered by the Internet: as a communication and information-dissemination technology, the Internet provides a relatively simple and inexpensive way to expand government outreach programs, to national populations, expatriates and émigrés, and both government and civilian foreign audiences. The Internet can thus be another tool of diplomacy. It is unclear at present, however, whether governments will be able to use the Internet as effectively to promote their own views and interests as well as that medium is currently being used by the private sector, especially non-governmental organizations (NGO). The United States government has the most extensive Worldwide Web presence of any government today, but the sites concentrate on simplifying and speeding up access to government information. Efforts to

shamelessly promote the "American way" are only beginning to emerge, such as on the Web pages of the White House (www.whitehouse.gov). The Jordanian government has taken the unusual step of creating a home page for its General Intelligence Directorate (the "secret police") (www.gid.gov.jo), although it is not clear whether this is a real step toward openness or a smoke screen.

Governments process enormous amounts of information in the course of their daily business. To the extent that much of this information originates in or is destined for open (i.e., not subject to security classification) sources, the Internet may increase the efficiency of these activities and reduce or eliminate the requirement for parallel or redundant networks. These activities need not be limited to domestic processes, but are again useful for diplomatic and foreign intelligence operations. For example, the U.S. government collects and translates into English a large volume of open source material (radio and television broadcasts, newspapers and other periodical literature) from around the world via the Foreign Broadcast Information Service (FBIS). The FBIS has expanded its activities to include collection of information disseminated via the Internet which, among other things, has increased the timeliness of its coverage of those newspapers that are now published on the Internet in parallel with the printed copies that formerly took hours or days to acquire. Paper distribution of the translated products has all but ceased, with routine publication of non-graphical materials being handled via a Web site, the *World News Connection* (wnc.fedworld.gov), which is operated as a subscription service. In addition to providing more timely information at reduced cost, a by-product of electronic publication is the public availability of an historical database of previously-published material.

The issue of the Internet empowerment of groups and individuals also has an effect on the process of governing to the extent that it appears to give more people ready access to government agencies and officials. In fact, electronic mail only replaces the written letter, but there is an informality and immediacy to e-mail that encourages both its use and the attention of the recipients. Coupled with the ubiquity of information provided by the news media (including but not mainly via the Internet), there is a developing capability and tendency for citizens to critique government policies, based on observation of their effects, in near real-time. Such scrutiny and response to government activities was not previously possible and it is not yet clear what the implications may be. The result could be, as maintained by John Pavlik, the executive director of Columbia University's Center for New Media, a "media democracy,"[16] with the potential to subject every major government action to nearly-immediate public referendum. The downside of this trend is not only the difficulty posed by the greater amount of information to be processed by decision-makers in less time than previously coupled with the greater visibility accorded the results of their decisions, but also the fact that a significant amount of information available via the Internet is either untrue, less than completely accurate, or incompletely representative of the events being reported.[17]

[16] "The New Journalism," *The Site*, 26 January 1997, <http://www.thesite.com/0607w4/work/work620jump1_062697.html>.

[17] John Rendon, presentation at the Highlands Forum X, Chantilly, Virginia, 12 November 1997. Mr. Rendon is the president of The Rendon Group, a global strategic communications consultancy.

Elements of National Power

Based on the foregoing, it may be that the real problem created for governments by the proliferation of the Internet (and other IT-enhanced communications media) is not the proliferation of information so much as the proliferation of actors on the governmental and diplomatic stages.[18] Organized groups and individuals can build, and in fact are building, coalitions, both domestic and international, that can bring unprecedented pressure to bear on national governments regarding virtually any activity or area of interest. These groups may in fact create *faits accomplis* that require no more action of governments than to accept what has already been accomplished. This raises the question of whether the nature of sovereignty has changed in the area of instant and ubiquitous communications and, if so, how. What is the relationship between these new capabilities and the traditional sources of national power?

There are six classical elements to the *realpolitik* definition of national power: the monopoly by the state of the (1) means of war, (2) violence within the system, (3) information dissemination, (4) financial controls, (5) advanced technologies, and (6) expertise.[19] As previously noted in Table 1 (p. 4), we take a related approach that reorganizes the classical elements into five elements of power, principally to emphasize the importance of non-coercive directive and negotiating power, the internal and external elements of which are political and diplomatic power (or expertise), respectively. The coercive corollaries are military power (i.e., the means of waging war) and the internal security structure (i.e., the means of violence within the system), respectively. Our appreciation of economic power takes a broader view than just the monopoly of the state over financial controls (which, arguably, has diminished significantly), to include the freedom of action, both domestically but especially internationally, conferred by a robust and wealthy economy. In addition to information dissemination, we include creation, collection, and database (storage, manipulation, and retrieval) of information which, as previously noted, has become a fungible asset. Finally, we postulate that advanced technologies and human expertise are the "hardware" and "software" components, respectively, of national technological prowess. While not necessarily agreeing with our definitions of the modern elements of "*cyberpolitik*" power, David Rothkopf agrees that the foundations of world power are shifting due to a revolution that has only recently begun, the implications of which are still unclear.[20] Rothkopf further suggested that culture has emerged as a new power in the current era of globalization,[21] although cultural power may not accrue to a single or particular state and does not appear to be readily amenable to state control.

Economic power arises from wealth and the sources and fungibility of this wealth. Both domestically and internationally, the ability of a government to direct or at least influence the distribution of wealth, principally through grants, loans, and purchases, provides non-coercive leverage over other governments, groups/organizations, or individuals not otherwise amenable to government control. However, the exercise of this power is not certain to yield the desired results, for two reasons: many governments today have less control over the sources and disposition of

[18] Paul Saffo, presentation at the Highlands Forum X, Chantilly, Virginia, 12 November 1997. Mr. Saffo is the director of the Institute for the Future.

[19] Jeffrey Cooper, presentation at the Highlands Forum X, Chantilly, Virginia, 13 November 1997. Mr. Cooper is the director of the Center for Information Strategy and Policy at Science Applications International Corporation.

[20] David Rothkopf, presentation at the Highlands Forum X, Chantilly, Virginia, 13 November 1997. Mr. Rothkopf is managing director of Kissinger Associates.

[21] _____, "In Praise of Cultural Imperialism?" *Foreign Policy*, Summer 1997, <http://www.foreignpolicy.com>.

wealth, and there is no guarantee that the object of control will respond as intended. The lack of useful results from the imposition of economic sanctions against Cuba, Iran, or Iraq are good examples of the latter limitation.

The "promotion of domestic prosperity" has been defined by the Clinton administration as one of the fundamental requirements of American national security,[22] thus attempting to focus plans and actions, not all in the economic/financial sector, on the development of the domestic component of economic power.

The potential effects of the diffusion of the Internet on the economic viability issue of governance (pp. 19-20) are pertinent to development and maintenance of national economic power.

Political and Diplomatic power are the domestic and international means, respectively, of non-coercive influence other than the exercise of economic power. Both rely extensively on negotiation, proselytization, and propaganda. These areas where, in addition to the commercial sector, knowledge can be power if that knowledge is pertinent, exclusively held, and productively employed. Information and coordination are major elements of the creation and exercise of these forms of power, both of which elements are affected by the proliferation of the Internet.

While the Internet can be used to extend and enhance coordination and cooperation, and increase the efficiency and effectiveness of information collection and dissemination, it may also reduce the exclusivity of information, eliminating or limiting one source of non-coercive advantage.

A "central goal" of the U.S. national security strategy is the promotion of "democracy abroad."[23] The information technologies, including (and perhaps especially) the Internet are viewed as enabling technologies that will enhance American actions in support of this goal through increased international contact and information dissemination throughout otherwise denied areas. Thus, this American national security goal can be seen as diametrically opposed to the fundamental interests of undemocratic governments, and therefore a cause for caution in embracing the Internet.

Rothkopf postulates four principal effects of IT, to include the diffusion of the Internet, that especially effect the exercise of political and diplomatic power: disintermediation, decentralization/disaggregation, amplification, and acceleration.[24] Disintermediation refers to the apparently diminishing requirement for intermediaries, in this case to the increased direct access to government decision-makers provided by the Internet. This is especially true in the case of influence that can be rapidly organized and brought to bear on national governments and international governmental organizations by non-governmental groups, whereby the entire foreign policy apparatus of the states concerned is by-passed. Decentralization and disaggregation refer to the "Balkanization" of issues and interest groups. The Internet can be used to virtually unite dispersed individuals or groups with a common cause who are otherwise individually too few within their respective home locales to have an effect on government, thereby creating the critical mass required to be noticed and responded to. One of the results of this disaggregation is the exacerbation of the previously-noted problem of the proliferation of actors. Amplification and acceleration are related to the rapidity with which information is acquired, disseminated, and used to formulate demands for or critiques of government action. The proliferation of news gatherers and reporters, both formal and informal, results in increased and more diverse reporting or a

[22] *A National Security Strategy…*, *op. cit.*, p. 8.
[23] *ibid.*, p. 1.
[24] Rothkopf, presentation at the Highlands Forum X, *op. cit.*

particular event that might have passed unremarked in the absence of such reporting. A related problem is that many informal news reporters rely upon one another, creating multiple reports of a single event derived from a single, possibly unverified, source. Additionally, the near-simultaneous receipt of information by a concerned audience worldwide permits them to coordinate their response, contributing to amplification of the importance of the event.

Coercive power is the traditional means for establishing, expanding, and maintaining control, but its use is increasingly constrained by new perceptions of human rights and the impact of those perceptions on domestic and international law and the relationship between governments and those governed.

The application or threat of military power is used to influence external actors and events, being the companion of diplomacy. In the post-Cold War international regime, the major military powers are increasingly constrained in their ability to unilaterally apply force, while military power appears to continue to be the tool of choice in the developing world. The application of force on a multilateral basis requires not only increased cooperation between military forces, but places a premium on political and diplomatic coordination and consensus-building. The success of the coalition arrayed against Iraq in operations Desert Shield and Desert Storm contrasts with the inability to agree on goals and methods that delayed Western intervention during four years of war in the former Yugoslavia.

There is little evidence thus far on which to base judgments of the potential effects of the Internet on the external application of military force. Desert Storm pre-dated the emergence of the Internet as a major communications medium. To the extent that the Internet was used in relation to the war attendant upon the break-up of Yugoslavia, it appears that its major use was by actors outside the war zone attempting to influence world opinion with a view toward spurring the major powers to intervene. It is not apparent that this effort bore any fruit. In the future, the Internet might be used more aggressively during an international conflict, especially as the medium for launching computer-based attacks on the enemy's infrastructure and network-based critical operations.

The coercive alternative, or complement, to political power is the internal security apparatus, usually various types of police forces and security services, sometimes augmented by special military units. The mission of the internal security apparatus is generally first of all to secure the rights of individual citizens, that is, protect them from harm at the hands of other citizens. However, the same apparatus may also be used to abrogate individual rights for the benefit of the state; this may indeed be the principal function of some internal security services. Strict internal security is the norm in countries without a democratically-elected government, where the government cannot rely solely on non-coercive measures to secure its tenure.

To the extent that it provides an additional communications medium, the Internet can be seen as a threat to coercive control, whether internal or external. In its most basic form, it is merely another means of sharing information. However, the robust nature of the international network and the fact that it is a store-and-forward medium (asynchronous) presents unique problems to security services. To date, the principal use of the Internet in relation to internal security has been either from outside to encourage civil disobedience and even revolt inside, such as the activities of the London-based Council for the Defense of Legitimate Rights (CDLR) against the Saudi Arabian monarchy, or from inside to rally international support for a cause, as in the case of the Zapatista insurgency in Mexico. Although there may be the potential for the Internet to be used as the base

for computer-based attacks by dissidents or revolutionaries (or criminals) against a government, even the use of the Internet as a propaganda medium, to the extent that it by-passes the state's information control apparatus, is viewed as a significant security threat by many internal security services.

Technological power is accumulated through the establishment and maintenance of a robust scientific and technical infrastructure, including research and development facilities, programs, and funding; a technical higher education system; an educated cadre of engineers, scientists, and managers; and a manufacturing base capable of incorporating technological developments into useful tools. This presupposes the presence of a market, either commercial or military, or both. Historically, military demand has been one of the driving forces behind technical innovation; however, the demands of the consumer market may be more important in developed countries today.

Technology can be used by a government to enable it to pursue military and/or geopolitical objectives and enhance the economic and social development of the country.[25] Technology is also, and perhaps more importantly, employed by commercial firms to create new products, the trade in which increases the economic power of the country of origin even while the purchasing country may also achieve a net gain from the transaction (e.g., by increasing its own technological or military capabilities).

The diffusion of the Internet represents at once the diffusion of new technologies and the potential for increasing a country's technological power through enhanced access to foreign information and closer interaction with international scientific communities. Some governments are concerned that access to the Internet by their (potential) adversaries may allow those countries to rapidly develop or improve weapons or other threatening capabilities. In the same fashion that "corporate espionage" on the part of the Soviet intelligence services against American companies allowed them to improve or skip steps in their weapons development processes,[26] there are fears that the Internet provides an enhanced capability for this type of espionage.[27]

Information The rise of information to an element of national power, and hence international competition, was brought about by the "information revolution" and the emergence of knowledge as a fungible asset. Dr. Daniel Kuehl of the (U.S.) National Defense University defines "national information power" as the "broadest range of military, governmental and civilian information capabilities that enable national-level exploitation and dominance of the information environment."[28] The military component of information power comprises the country's command, control, communications, and (military) intelligence (C^3I) assets and stored information, as well as resources to counter an adversary's C^3I assets and other information resources. The civilian (private sector) component of information power "includes such diverse elements as our telematics infrastructure… . [and] [o]ther, less obvious elements, such as the computer science

[25] Wolcott, *op. cit.*, p. 1.

[26] *Soviet Acquisition of Militarily Significant Western Technology: An Update* (Washington, D.C.: Central Intelligence Agency, September 1985).

[27] John Leach, "Impeding Internet spies," *CommsMEA* 5 (November 1995), pp. 23-24.

[28] Daniel Kuehl, "Defining Information Power," *Strategic Forum*, No. 115, June 1997, <http://198.80.36.91/ndu/inss/strforum/forum115.html> (9 February 1998).

departments of our colleges and universities, or even the news media… ."[29] The government's contribution to national information power includes the resources of non-military intelligence organizations, the diplomatic corps, national (i.e., government owned and/or controlled) broadcasting organizations, and public affairs agencies (including the public affairs departments of all government agencies).

If the ability to acquire, process, assimilate, and productively employ information is indeed today a form of national power, then the Internet, as the only worldwide network that connects tens of thousands of computers and their extensive information assets, inevitably must be figured into the power equation and plans for (or fears of) international conflict. A lesser developed country cannot help but hope to improve its economy, and perhaps along with it the country's national power statistics, through the rapid acquisition of information critical to scientific and industrial processes, trade, education, and other critical needs (e.g., medical and health information), enabled by exploitation of the Internet. On the other hand, developed countries may have cause to fear an erosion of their power relative to traditionally weaker countries now rapidly improving themselves. The predominant information flows over the Internet, as in other media, is from the OECD countries to the developing countries. While some Third World reactionaries have criticized this as "cultural imperialism," none have complained about the ready access to advanced technical information.

The task, then, for the information "have-nots," as noted earlier (p. 19), may be to formulate a strategy to gain the benefits of enhanced information flows while limiting the potential liabilities. It is not yet clear that this is possible. The sources of information, the developed countries, have been pursuing the diffusion of the Internet, along with more traditional information exchange programs, in the belief that this will not only spur development but encourage the democratic processes that would make the world a safer place for all concerned. Their tasks are to reassure themselves that this is indeed the case, and to determine how to ensure the free flow and proper employment of only such information as cannot or will not be used to create or increase threats from the developing countries either to each other or to developed countries.

[29] *ibid.* Dr. Kuehl defines telematics as "the marriage of advanced telecommunications systems and computerized databases and networks. It is the world of storage, transmission, mainpulation and dissemination of electronic digital information and includes satellite communications systems, the microprocessor ('chip') production industry, and software designers and producers."