Chapter Four

THE INFORMATION REVOLUTION IS AFFECTING MECHANISMS OF GOVERNANCE AND EMPOWERING NEW POLITICAL ACTORS

The information age is reconfiguring some processes of governance, as well as changing both the character and distribution of political power.

SOME TRADITIONAL MECHANISMS OF GOVERNANCE ARE BECOMING PROBLEMATIC

Some traditional mechanisms of governance (e.g., taxation, regulation and licensing) are becoming increasingly problematic, as the information revolution allows action beyond the reach of national governments. For example:[1]

- E-commerce is making transaction taxes (e.g., sales taxes) more difficult to collect. This could over time lead to more reliance on other types of taxes.
- Regulations are often not keeping up with new business models, leading in some cases to unstable excesses, in others hindering the advance of IT-related activities.
- Regulation and licensing are becoming increasingly difficult when service providers are beyond national jurisdictions.
- Limits on offensive or dangerous information (e.g., pornography, hate literature, bombmaking instructions) are not always honored by others.

In these and other areas, governments that are particularly affected[2] will have to find new mechanisms of governance, or will have to create new, near-universal international control regimes.[3]

NEW GOVERNMENTAL MECHANISMS ARE BEING ENABLED

At the same time that some traditional mechanisms of government are facing challenge, the information revolution is also enabling new governmental mechanisms, generally falling under the heading of "e-government." In general, this usually implies the use of IT to improve and (eventually) transform

- the manner in which governments interact with their citizens and provide public services to those citizens
- the management of governments' supply chains
- the conduct of internal governmental processes.

The first of these is analogous to the use of IT in business to improve and transform customer relationship management; the second, to businesses' use of IT in supply chain management; the third, to the way in which businesses are using IT to speed up internal communications and process efficiency and even, in some cases, to change the architectural organization of companies.[4]

These three thrusts of e-government are analogous to those in business, but today, at least, the business world is far ahead in exploiting IT.[5,6] It remains to be seen how truly transforming IT will be for governments and how long the process will take,[7,8] particularly in the developing world.[9]

NEW POLITICAL ACTORS ARE BEING EMPOWERED

The distribution of political power is changing, as new nonstate actors are being empowered by the information revolution, in the business, social, and political realms, at the subnational, transnational, and supranational levels. These new political actors include transnational business organizations, sub- and transnational special affinity groups (ranging across the religious, ethnic, professional,

criminal, etc., spectra), other nongovernmental organizations, and, unfortunately but most assuredly, terrorist organizations.[10]

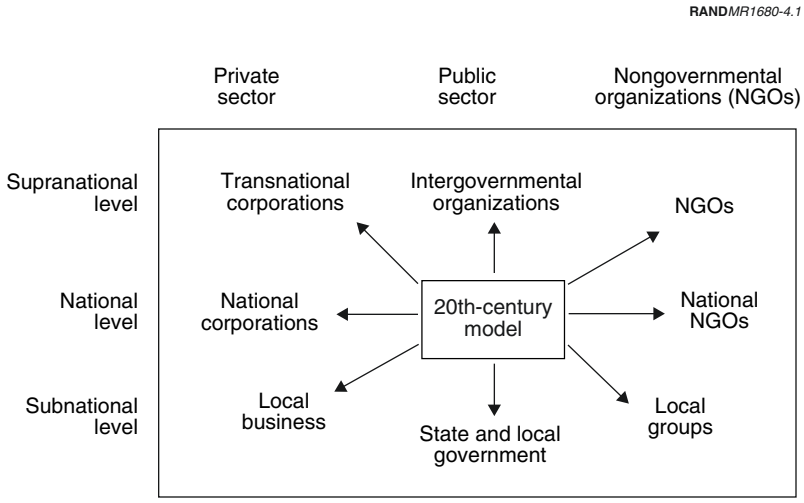
This leads to various concerns: What will the role and authority of national governments be vis-à-vis these emerging nonstate actors? Will there be new allocations of power? Will power be shared in new and different ways? Who will be accountable in the future information age? Will more and more decisions affecting nation-states be made by actors not accountable to the citizens of those states?

Such concerns are just beginning to manifest themselves.[11] How they play out could affect the course of the information revolution.

At the same time that these new political actors are emerging, advances in IT are making new Internet-based modes of interaction possible between citizens and their elected representatives, between candidates and voters, and among citizens themselves (when discussing political issues). Some have suggested that this could over time change the dynamics of politics, much as the advent of television did in the 1950s and 1960s. Others, however, question the imminence of such a change in political dynamics, if not its ultimate extent. The jury is clearly still out on this issue.[12]

THE INFORMATION REVOLUTION COULD OVER TIME CHANGE THE ROLE OF THE NATION-STATE: THE JURY IS STILL OUT

The nation-state has been the dominant governmental organization in much of the world for the past 400 years. Some scholars suggest that as the information revolution increasingly allows action beyond the reach of national governments and empowers new political actors, the role of the nation-state could change. For example, one leading scholar postulates that a diffusion of governance activities may occur, away from the centrality of the nation-state, with some functions migrating to supranational or intergovernmental organizations, some devolving to local governmental units, and some migrating to private market and nonmarket organizations (at the subnational, national, and supranational levels).[13] Figure 4.1 illustrates the diffusion of governance this scholar has in mind.



SOURCE: Modified from Nye (2002), p. 4.

Figure 4.1—The Diffusion of Governance in the 21st Century

One scholar has termed this the "retreat of the state."[14] Some scholars go even further, foreseeing the "end of the nation state."[15] But others feel that trends in this regard are by no means clear, pointing out the many essential functions that the nation-state will continue to play.[16] Considering these vastly different visions of the future presented by various "experts," one must conclude that for now the jury is still out regarding the future role of the nation-state in the information age.

Further, there are (at least) two different aspects of sovereignty:

- Constitutional sovereignty—the legal authority and primacy of national governments within their territorial domains.[17]
- Operational sovereignty—the ability of governments to exercise effective control within their territorial domains.

Constitutional sovereignty is not being challenged by the information revolution. But operational sovereignty is, both technically and with regard to cost.[18,19]

DIFFERENT NATIONS WILL TAKE DIFFERENT APPROACHES TO DEALING WITH THESE CHANGES

Governments will have to deal with these changes in mechanisms of governance (both positive and negative), with these new political actors, and with these emerging challenges to the traditional roles of the nation-state. Different nations may take different approaches.[20] How they do this will affect the future course of the information revolution in their regions and help define the role(s) of the nation-state in the information age. Smaller nations may more readily give up some prerogatives of the nation-state. Larger nations may be less willing to give up any prerogatives and may try harder to preserve the traditional roles of the nation-state. It is early regarding these issues; time will tell how this plays out.

In some cases, the paths that nations choose will adversely affect their relations with other nations, including, in some cases, even their closest allies. For example, in response to the many challenges confronting the nation-state in recent years, Europeans have willingly transferred many functions, responsibilities, and authorities traditionally within the purview of national governments to supranational organizations (most notably to the European Union but also to other supranational organizations). The United States has been much slower to move down this path. At least one observer believes that this differing approach may reflect a much deeper issue of principle regarding where the ultimate source of democratic legitimacy lies.[21] If he is correct, this could well lead the United States and Europe to define (and attempt to implement) greatly differing future roles for the nation-state—with continuing stress resulting for the U.S.-European relationship.[22]

THE EVENTS OF 9/11 MAY LEAD TO INCREASED GOVERNMENTAL INTERVENTION INTO IT DEVELOPMENTS

The events of September 11 should bring a heightened awareness of cyberspace security issues, as concern regarding future terrorist attacks expands beyond using hijacked aircraft as guided missiles to include a broader range of attack mechanisms, including cyberspace-mediated attacks on critical infrastructures.[23]

This may lead to increased governmental intervention into IT developments, to ensure that greater weight is given to security considerations in the design, implementation, and operation of IT systems and networks.[24]

NOTES

[1]These difficulties of governance in the information age were discussed in general terms at the November 1999 RAND information revolution conference (see Hundley et al., 2000) and are discussed in much more detail in Jones (2000).

[2]Some governments will be affected more than others. For example, those that rely heavily on transaction taxes, use regulations and licensing to closely control their business communities, or strictly limit pornography will have increasing problems over time. Those that practice a more laissez-faire style of governance in these (or other) areas will have fewer problems.

[3]Jones (2000) discusses the pros and cons of various new modes of governance that may prove feasible.

[4]These uses of IT in business are discussed in Chapter Three of this report.

[5]According to one authority on the status of e-government efforts in the United States (Mechling, 2002):

> The initial progress on e-government has followed a predictable pattern. As with most technologies in most settings, the early applications have been decidedly incremental. In essence, the Internet has been used to make services more convenient—available twenty-four hours a day from home and work and without time-consuming trips to government offices. So far, however, neither the Internet in particular nor computer networking in general has been used much for dramatic improvement in service efficiency, customization, and integration. In addition, we have made scant headway on concerns about the impact of e-government on privacy, security, equity, and the very legitimacy of our institutions of governance. The final success or failure of this trip remains very much yet to be determined.

[6]Even in the developed world, the transformative power of e-government is limited by the fact that government entities often cannot decide which customer segments to target—they have to serve everyone; and there are many other factors that differentiate governments' ability to exploit IT from the courses that private companies can pursue. (See Hundley et al., 2001, pp. 35–38.) In addition, *revolutionary* change is difficult to execute without creative destruction, and that is difficult to do in governments because they tend to be bureaucratic organizations.

[7]Mechling (2002) surveys how far federal, state, and local governmental agencies in the United States have come in using IT as an enabler to improve "bureaucratic government" and offers some thoughts on how IT might change the trajectory of government's evolution in the future. Picking up where Mechling left off in an earlier version of his paper, Donahue (1999) makes the following "five broad predictions" regarding the future evolution of e-government:

- For those governmental functions that are essentially similar to business functions, the information revolution will have essentially similar effects on cost, access, and innovation—but with a lag.
- Among the information revolution's most important impacts on government will be expanding opportunities for outsourcing.
- Wherever the information revolution improves potential *public* performance, it will also tend to ease privatization.
- The information revolution will tend to increase the productivity gap between public and private organizations.
- For those governmental functions that are essentially *dis*similar to business functions, the information revolution will have real but modest effects.

Generally speaking, these look like credible predictions, with one caveat regarding the last one: Even though warfighting is the governmental function probably most dissimilar to business functions, IT is already clearly having a major, transformational impact on warfare.

[8]The European Union has ambitious plans for e-government in Europe. The participants in the April 2001 RAND/NIC conference on the information revolution in Europe discussed the status of these plans and their prospects for success. (See Hundley et al., 2001, pp. 35–38.)

[9]PCIP (2002) provides a roadmap for e-government in the developing world, including 10 questions e-government leaders in developing nations should ask themselves before pursuing e-government, and details many of the obstacles that governments may encounter along the e-government path.

[10]International terrorist organizations such as al Qaeda are clearly empowered by their ability, for example, to carry out financial transactions and covert communications over the Internet.

[11]The demonstrations at international conferences over the past few years (e.g., recent World Trade Organization and Group of Seven meetings) may be one manifestation of such concerns. Arquilla and Ronfeldt (2001) discuss this issue.

[12]Applbaum (2002), Franda (2002), Hill and Hughes (1998), Kamarck (2002), King (2002), Norris (2002), Simon, Corrales, and Wolfensberger (2002), and Thompson (2002) present a sample of views on various aspects of this topic.

[13]See Nye (2002), pp. 3–5.

[14]Strange (1996) presents her vision of the "retreat of the state," or more precisely the "declining authority of states," as a result of the fact that "the territorial boundaries of states no longer coincide with the extent or the limits of political authority over economy and society."

[15]Ohmae (1995) presents the case for the "end of the nation state"—as a "meaningful aggregate in terms of which to think about, much less manage, economic activity."

[16]For example, Jones (2000) presents a detailed examination of the traditional purposes and forms of state action, the stresses that the information revolution and accompanying globalization are placing on them, the continued needs for governance

in a globalizing world, and alternative modes of governance to satisfy these needs. His conclusion: Although the information revolution and accompanying globalization do confront established states with serious challenges, the world will continue to need something like the nation-state to perform essential public governance functions.

[17]This is sometimes referred to this as "Westphalian sovereignty," in reference to the Treaty of Westphalia in 1648 at the conclusion of the Thirty Years War, which established the principle that nation-states do not interfere in the internal affairs of other nation-states.

[18]This point was made at the November 1999 RAND/NIC conference. (See Hundley et al., 2000, pp. 19–20.)

[19]It was also pointed out at the November 1999 RAND/NIC information revolution conference that this is not the first time national sovereignty has been called into question. Rather, national sovereignty has been viewed as challenged by each new communication media. See Hundley et al. (2000), p. 19.

[20]Jones (2000, particularly pp. 200–216) identifies a number of possible approaches that nations may take, including micro-, meso-, and macro-regionalism, various intergovernmental modes of public governance, and various mixed modes of public-private governance.

[21]According to Fukuyama (2002), which should be read in its entirety for a detailed exposition of this view:

> Americans tend not to see any source of democratic legitimacy higher than the constitutional democratic nation. To the extent that any international organization has legitimacy, it is because duly constituted democratic majorities have handed that legitimacy up to them in a negotiated, contractual process. Such legitimacy can be withdrawn at any time by the contracting parties. International law and organization have no existence independent of this type of voluntary agreement between sovereign nation-states.
>
> Europeans, by contrast, tend to believe that democratic legitimacy flows from the will of an international community much larger than any individual nation-state. This international community is not embodied concretely in a single, global democratic constitutional order. Yet it hands down legitimacy to existing international institutions, which are seen as partially embodying it.

The Economist (2002c, p. 24) has recently endorsed this view, saying:

> Americans, more than Europeans, see the nation as the ultimate repository of sovereignty and law. They may argue about the extent of federal powers. But Americans remain out of sympathy with European notions of international law or polled sovereignty. Indeed, their constitution forbids the transfer of Congress's sovereign powers.

[22]On this point, Fukuyama (2002) says:

> The U.S.-European rift that has emerged in 2002 is not just a transitory problem reflecting the style of the Bush administration or the world situation in the wake of Sept. 11. It is a reflection of differing views of the locus of democratic legitimacy within a broader Western civilization.

[23]The U.S. government has for some time been concerned regarding the cyberspace-related vulnerabilities of critical U.S. infrastructures. (See, for example, PCCIP, 1997). However, because most of these infrastructures are owned and operated by the private sector and therefore outside of direct government control, the government has thus far been unable to effect much of an improvement in their cyber security. (PCIPB, 2002, gives an assessment of the state of critical infrastructure cyber security today.)

[24]In response to market forces, up until now functionality has almost always been given much greater weight than security in the design of new IT systems and networks and their subsequent implementation and operation. This has led to a situation where security vulnerabilities are commonplace, security incidents are a frequent occurrence, and the business community—except for the financial services industry—has treated these incidents as a "cost of doing business." (See PCIPB, 2002, for an overview of the state of cyberspace security today.)