John F. Kennedy School of Government
Harvard University
Faculty Research Working Papers Series

Information Power: International Affairs in the Cyber Age

Viktor Mayer-Schoenberger
and Gernot Brodnig

November 2001

RWP01-044

DRAFT - NOVEMBER 1, 2001

Information Power: International Affairs in the Cyber Age

Viktor Mayer-Schönberger / Gernot Brodnig*

"Knowledge is more than equivalent to force"

Samuel Johnson: *Rasselas*

INTRODUCTION

Ever since Sun Tzu, information and power have been considered intricately linked in shaping the political landscape. It is, therefore, a rather banal observation that the recent advances in information and communication technologies (ICT) should have significant effects on the conduct of international affairs. Indeed, every day provides new evidence for such transformations.

Governments around the world are reevaluating the functions and purposes of their diplomatic services in the age of CNN and the Internet. After a series of introspective studies,[1] the U.S State Department, for example, is trying to streamline its archaic communication structures, while Switzerland is exploring an alternative approach to traditional diplomacy altogether: it recently opened the world's first digital consulate, the Swiss House for Advanced Research and Education, in Cambridge, MA.[2]

The tremors of the information revolution are also shaking the increasingly global and transnational corporate sector. The modern "knowledge company" creates value more by processing bits than things. The valuations and financing prowess of high-tech companies such as Cisco or AOL are primarily based on future revenue potentials embedded in their intellectual property.[3] Similarly, the recent Global Competitiveness Report has highlighted

* Viktor Mayer-Schönberger (Viktor_MS@harvard.edu) is Assistant Professor of Public Policy at Harvard University's John F. Kennedy School of Government ; Gernot Brodnig (gbrodnig@ksg.harvard.edu) is a Research Fellow at the Kennedy School. The authors would like to thank Joseph Nye, Anthony Oettinger, Anne-Marie Slaughter, Jessica Stern, David Lazer, Charles Schmitz, the participants of the 1999 and 2000 Harvard Information Infrastructure Project' Seminars, and the participants of the 2000 Carnegie Endowment for International Peace Symposium "Rethinking Our Foreign Policy Structure", for invaluable insights and feedback.

the critical role of intellectual capital as a growth engine through its economic creativity index.[4]

Even more dramatic is the impact of ICT on the "third force" in international affairs: non-governmental organizations (NGOs) and civil society. Their power usually derives from persuasion and manipulation rather than military might or financial wealth. The "laptop campaign" that resulted in the Landmine Ban Treaty[5] or the sophisticated use of the Internet by the Zapatista rebels[6] have become classic symbols of cyber politics.

These and other examples have sparked considerable debate in academic and policy-making circles about the direction of international affairs in the information age.[7] Preliminary conclusions cover the whole spectrum from the end of the nation-state to rather minor adjustments in existing structures and processes. What makes these analytical efforts so difficult is the fact that both the information revolution and the numerous dimensions of international affairs are constantly evolving, dynamic, and complex phenomena that easily elude simple trends and certainties.

It comes, therefore, as no surprise that even our understanding of what constitutes the "information revolution" is far from clear. Some analysts focus on technological change, intrigued by the various "laws" successfully predicting the exponential explosions of computer processing power and bandwidth.[8] Others argue that the information revolution is less about integrated circuits and cell phones than about the primacy of information and knowledge in politics, economics, and social relationships, a dynamic that can apply equally to more or less wired societies.[9] Somewhere between these camps, analysts of information infrastructures focus on both the technology and concomitant regulatory, economic, and social issues.[10]

Scholars of international affairs, too, have been struggling to keep pace with the rapid transformations of recent years. The traditional Westphalian system is increasingly challenged by transnational forces, blurring the lines between domestic and international politics, and changing the balance of capabilities between nation-states and non-state actors.[11] This struggle, in turn, is a function of shifting power distributions between states

and the impacts and repercussions of domestic regime changes such as democratization and liberalization. To use Stanley Hoffman's image, the international system's horizontal (relations between major players), vertical (hierarchical aspects), and functional dimensions are all moving at once and into each other.[12]

Against this backdrop of analytical unease, conventional wisdom has it that the information revolution is reshaping the environment in which foreign policy and international relations are conducted by generally increasing the influence of non-state actors and undermining the authority of the nation-state.[13] More cautious voices, however, stress that the extent to which such outcomes are caused in a direct and unmediated manner is not clear and that the workings of such a transmission belt have not yet been demonstrated.[14] While there is mounting anecdotal evidence about certain trends, hard indicators and data are difficult to come by. The relationship between the information revolution and political outcomes remains largely a black box.

The purpose of this paper is to attempt a peek into this box by proposing a framework for assessing the impact of the information revolution on power structures in international affairs. We begin with an examination of the importance of information as a source of power and the ability to control information access as key to information power. We then propose that recent years have seen significant shifts in information access categories, both deliberate and unintentional. In the main section of the paper, we introduce the concept of "denationalization" of information infrastructures as the central phenomenon facilitating these shifts. We conclude with some implications of these developments for the conduct of international affairs.

INFORMATION POWER

Nature and Sources of Power

Most scholars and practitioners of international affairs agree on two things about power: 1) that it is one of the fundamental variables in international affairs; and 2) that it is an ever-changing and elusive phenomenon. Often compared to other abstract notions, such as

love[15]– difficult to describe, but easy to recognize – the concept of power has had its fair share of dissection by sociologists and political scientists.[16] A number of dimensions, sources, and manifestations of power have been identified, and the latter has served as the key explanatory variable in many a theory of international politics. While it is beyond the scope of this paper to delve into the intricacies of power concepts, several brief observations are necessary to better appreciate the notion of information power and the analytical framework derived from it.

Power is essentially a relational concept that involves at least two actors, a targeted object or outcome, and a certain mode of control based on a number of sources/assets. In international affairs, power theories have long been dominated by the "control over resources" approach.[17] Tanks and oil, as well as indicators such as military expenditures or GNP, were the benchmarks used to determine a nation's power. At best, however, this approach can provide an approximation of a power potential that needs to be converted/translated into the control of other actors and – finally and fundamentally – certain outcomes.[18]

What type of outcomes? Most power theories in international politics tend to define power as the ability to shape decisions and particular actions. These one-dimensional approaches focus on "behavior in the making of decisions over key or important issues as involving actual, observable conflict."[19] Critics of these theories have pointed out that they do not reflect structural and institutional factors. Their alternative – two-dimensional approaches – emphasize those mechanisms that shape the agenda and determine which decisions/actions are being taken.[20] Three-dimensional approaches, finally, introduce the dimension of ideology: not only decisions and agenda-setting crystallize power, but even more so "the capacity of elites and their intellectual servants to structure public beliefs, values, and desires to secure compliance with the norms and behavior that serve their needs."[21]

Irrespective of the target – decisions/actions, structures/institutions, or ideologies – power operates through a number of control modes. Various typologies exist, which include such phenomena as force and coercion, authority, manipulation, and persuasion.[22] Nye[23] collapses these variations into the two archetypes of hard and soft power. While hard power draws

largely on the coercive force of traditional military and economic assets, soft power relies on the persuasive and manipulative strength of ideas and values.

As noted by Hoffman, these "salient ingredients" of power – object, control mode, assets – have undergone such transformations that we are faced with "bewildering uncertainties and complications that affect the exercise of power." [24]As we will see, one such recent transformation is the information revolution, which has made information/knowledge an omnipresent variable of modern society and is redrawing the geometry of power in international affairs.

Information as Power Source

Data, information, and knowledge have always figured prominently in the power equation. There can be no doubt that most power sources rely on accurate, comprehensive, and timely information. Whether it be cruise missile targeting coordinates or management information systems, information is instrumental in maintaining and enhancing the power potential of other sources, such as military assets or economic competitiveness. This trend is accelerating rapidly with the development and proliferation of modern ICT. The revolution in military affairs, for example, is largely about achieving information superiority, while comparative advantages in the corporate world are increasingly derived from the endowments and sound management of intellectual capital.

Information is, however, not only a multiplier of other power sources; it is a power asset in its own right. Power theories that focus on structural features have long attributed to informational variables a decisive role in configuring and structuring power. Foucault's work on power/knowledge relations, for example, identifies scientific bodies of knowledge and their proponents ("experts") as mechanisms of control and regulation through knowledge-producing systems.[25] Based on this work, other scholars, such as Wrong on the authority of competence,[26] Strange on knowledge structures[27], Rosenau on scientific evidence and proof in international politics,[28] and Haas on epistemic communities and regime formation,[29] have all highlighted various facets of information power.

In international affairs, all major actors derive some of their power from information sources. For state actors, the classic example has long been the intelligence function. Defined as "information relevant to a government's formulating and implementing policy,"[30] the intelligence role has traditionally emphasized the instrumental nature of information in support of other power sources, primarily military and security. With the expansion of what constitutes national security issues to encompass questions such as migration, AIDS, or environmental degradation, information requirements and operational modes have shifted. Governments have little comparative advantage in these areas, where open-source information dominates, calling for a re-assessment of the functions and value-added of intelligence.

For the international corporate sector, information is increasingly becoming the key to global competitiveness. The nature, demands, and constraints of the knowledge economy are particularly evident in the growing importance of intellectual property. Its value is easily apparent in the economic distortions and revenue losses caused by copyright piracy. It is estimated that, in 1999, American companies alone forfeited about U.S. $9 billion in lost trade revenues.[31] In response, international regimes such as the TRIPS Agreement have emerged and made intellectual property issues a major topic of discussion in international affairs. In addition to patents and trademarks, success in the "new economy" is measured by the ability of a company to attract and manage knowledge workers. Labor market and regulatory restrictions can often be overcome through telecommuting. Call centers, software programming, and accounting are outsourced to developing countries.[32] In India, for example, 250,000 to 300,000 software programmers[33] are working around the clock in high-tech centers such as Bangalore.[34]

For the third category of actors in international affairs, NGOs and their transnational networks, information is frequently the only available power source. Keck and Sikkink[35] have described the forms of information politics of issue-oriented advocacy networks: these non-state actors gain influence by serving as alternate sources of information. International campaigns typically take a two-level approach linking technical/statistical information to testimonial evidence. This strategy allows NGO networks to frame issues by using individual

cases and their motivating/persuasive power. Furthermore, information is the glue that holds members together, an essential ingredient in network effectiveness.

These example areas illustrate the pervasiveness and importance of information in international affairs for all actors, both as a multiplier of other power sources and increasingly as a major power asset per se. At the same time, several intrinsic features of information make it difficult to capture the implications of the growing information commodification.[36] First, information resources are often unquantifiable, given the subjective nature of certain "data" such as beliefs and values. Second, information power tends to be diffused, as it appears embedded in other forms of power. Third, the power is often not so much a positive capacity to convey knowledge and ideas but rather derives from the ability to exclude others from particular categories of information.

Information Access

Intelligence, intellectual property, and cyber-campaigns all represent data that, by themselves, do not convey any power. To find ICBM launch codes on the Internet renders them strategically useless. To keep testimonial evidence about human rights violations shelved away has the same effect. In other words, it is not the content of the information, but the access to it or the ability to control access, that converts information assets into power sources.

This view of information access builds on and extends the propositions developed by Keohane/Nye,[37] who distinguish three types of information: free, commercial, and strategic. Free information is shared without financial compensation. Commercial information is made available in exchange for payment. Strategic information is priceless in the sense that access to it by others erases its value. As argued above, the same data can be strategic, commercial, or free depending on the manner of access control. The designs for a new product, for example, are often trade secrets in the early phases of development and thus strategic information, access to which would negate a competitive advantage. Further on in the product cycle, and once protected by some form of intellectual property right, this information becomes commercial and can be licensed for a fee. Once the intellectual property protection ends, the same information becomes freely available.

None of the information access categories is specific to any actors in international affairs. Governments use a considerable amount of free information in their public diplomacy and propaganda initiatives. So do corporations through advertising and communication campaigns. At the same time, NGOs rely on the commercialization of certain data, particularly those that involve extended research efforts, for revenue-generation. They also guard some strategic information, such as the modalities of undercover investigative research or the timing of campaigns, the release of which would jeopardize their mission.

Nor is there a hierarchy among the information access categories in terms of their power potential. Under some circumstances, free information will have a greater impact than the well-guarded possession of secret knowledge or expensive data. The toolboxes of psychological warfare and advertising campaigns provide ample evidence for this proposition.

Shifts in Access Categories

As indicated above, information may shift from one access category to another. Such a shift can be the result of a deliberate strategy by an actor controlling information access categories. Traditional diplomacy, for example, has long been associated with the maximization of strategic information. Woodrow Wilson, convinced that World War I had started because of opacities, announced his "new diplomacy," which advocated a deliberate shift of diplomatic information from highly restricted and strategic to free access.[38] Similarly, one of the hopes of bringing the United States Information Agency (USIA), with its policy of free access to information, more closely under the wings of the State Department was to deliberately change some of the traditional, restrictive information access policies at State and make them more open and collaborative.[39]

Deliberate shifts in access categories occur not only among state actors. Corporations frequently decide to open up strategic information to public scrutiny. A recent example is the trend towards "open code" policies among large information technology firms. For at least a quarter century, the accepted dogma was that the most valuable part of a software company is the source code of its software products; releasing it to others would rob the

company of its crown jewels. Such was the protection of this piece of strategic information that frequently competitors spent many millions of dollars examining the complex inner workings of software in the absence of having access to the source code. Lately however, more and more software companies have "opened up" their source code, transferring it from the strategic to commercial or even free access categories. Netscape has published the source code of its central software piece, the web browser. Apple has done the same with the core of its new operating system. Even Microsoft, despite strong rhetoric to the contrary, has recently permitted its largest customers access to its most valued treasure, the source code of its latest operating system. The reasons for this rather sudden movement towards deliberate openness are not altruistic. Instead, companies expect that opening up at least some of their strategic information vaults may not only help them improve their products through modifications made by their users, but also increase their market share.[40]

Finally, non-governmental actors, too, may opt to switch information across categories. In contrast to governments and corporations, most of them are in the business of providing free information. But keeping access to some information limited may help them in maximizing certain impacts. A case in point are the campaigns of the anti-globalisation movement, which resemble military planning exercises. Moreover some of these actors have a globally recognized brand name. Licensing their brand to increase funding is another instance of shifting previously free information to the commercial access category. Greenpeace is a point in case. Its number of worldwide monetary supporters had dwindled from almost five to 2.5 million over the last decade. It is not surprising then that Greenpeace has decided to increase its revenue streams by actively commercializing its brand, recently valued at USD 410 million, thus reasserting control over parts of its information vaults.[41]

Clearly, deliberate shifts of information across access categories rearrange the power structure. But they occur in situations in which actors still maintain control over information access categories and can effectively prevent "leakage" of information from one category to another. As such, deliberate shifts are actions of power, aimed at maintaining or even enhancing the actor's overall power position.

In a different scenario, information shifts from one category to another may occur without the deliberate will or consent of the player involved. These unexpected changes happen when the actor who used to control access to a particular information category can no longer effectively do so. Such shifts are facilitated by some of the intrinsic qualities of information that distinguish it from physical objects. Information is as Norbert Wiener remarked "neither matter, nor energy"[42] and can be easily transported at high speed. These properties make its use non-exclusive and render it generally difficult and costly to exclude others from it. These qualities are usually associated with public goods. The public good character poses particular challenges for an effective policing of information access categories. In the following, we contend that a potent, but largely overlooked, such factor is linked to governments' loss of control over various parts or choke points of information infrastructures. This development as a whole we call the global move towards "denationalization" of information infrastructures.

DENATIONALIZATION OF INFORMATION INFRASTRUCTURES

Information Infrastructures

To understand the modes and implications of information access control and its unintentional loss, it is important to review some of the structural features of the acquisition, processing, and dissemination of information. Information infrastructures consist of the information itself, physical hardware such as our vocal cords or fiber-optic cables, techniques and standards for the manipulation of information such as sign language or computer programs, and the regulatory framework that governs the system as a whole as well as its various parts.

Information infrastructures have existed in one form or the other since human beings began to communicate and come in various shapes and shades of complexity: carrier pigeons, for example, were an important tool of military communication in World War I. The infrastructure consisted of a specific species of birds, a network of breeders, a certain message format. Access control for carrier pigeons was proportionate to the ability to shoot them down.

In the past, many information structures were owned or at least tightly controlled by governments. In most countries, postal services were – and in some still are – state monopolies. Supercomputers and their applications such as cryptography, too, have until recently been a prerogative of the public sector and its allies in research institutions.

This "information monopoly" of governments has been gradually eroded by three developments that make up the information revolution of the last decades.[43] First, digitization – the translation of data into one universal binary code – makes it possible for different forms of data, such as text, sound, and images, to be easily transmitted and exchanged. "Being digital,"[44] in turn, has made it technically possible and economically viable to span the globe with networks of data pipes, routers, and switches. Finally, global information transfer was revolutionized by several universal standards such as the TCP/IP protocols.

This new generation of information infrastructure – epitomized by, but not limited to the Internet – creates an informational space of flows that is global, real-time and "always on".[45] It is also increasingly "denational" in two ways: 1) the transnational nature of these networks has eroded a country's capacity to control the acquisition, processing, and dissemination of information; and 2) many of these infrastructures, or at least critical parts of them, are coming increasingly under the control of non-state entities. This pincer movement of denationalization, we argue, has facilitated the unintentional loss of information access control by governments in three dimensions: physical, economic, and regulatory. Physical and technological control has been lost, as many infrastructures are owned and managed by non-state entities and/or transcend the boundaries of the nation-state. The dramatic cost reductions, in tandem with exponential increases in capabilities, have all but broken down economic barriers of control. These two developments have made it increasingly difficult for governments to cast their regulatory shadow over access control.

Information Acquisition

The proliferation of ICT and the growing commodification of information have made the collection of data everywhere and any time not only a realistic technical proposition, but a political and economic necessity as well.

One subset of information affected by these transformations is geographic information. We have come a long way from the "science of the princes," as geography and cartography were once called. In today's world, geographic information is acquired by a set of sophisticated technologies including remote sensing, which images and measures spatial objects with ever-growing precision.[46]

Satellite remote sensing illustrates the increasing difficulties of states to maintain information access control. After the launch of the first spy satellite in 1960, remote sensing was, for almost three decades, firmly controlled by the governments of the superpowers. The technical capacities and know-how to launch and operate these satellites and to process images were their exclusive property. Military satellite programs were and still are part of the inner sanctum of national security, shrouded in secrecy.[47]

A major shift in access control occurred in 1986, with the launch of the first fully commercial remote sensing satellite, SPOT 1. Operated by a private French company, it rapidly opened a commercial market for a number of civilian applications, such as mapping or natural resources management. The political potential of SPOT and its implications for information power became apparent just a few months after its launch, when, in April 1986, it took an image of the burning nuclear reactor at Chernobyl. This image was purchased by a Swedish NGO and distributed widely to the world media, making it all but impossible for Soviet authorities to deny or play down the catastrophe. A new era of transparency was born.

The success of SPOT and some Russian high-resolution imagery[48] were partly responsible for the development and licensing of U.S. high-resolution commercial satellites. In

September 1999, the first 1m-resolution satellite, IKONOS, was successfully launched by Space Imaging, a private U.S. company whose investors include Lockheed and Raytheon.[49]

The U.S. government has given up physical control of the infrastructure, which includes the satellite itself as well as the ground stations. Admittedly, IKONOS was launched at Vandenberg Air Force Base, but foreign-currency-hungry launch capabilities exist in Russia and China and, recently, also on the high seas, where a joint venture among U.S., Norwegian, and Ukrainian investors has successfully deployed an off-shore launch pad on an old oil rig.[50]

Not only has the U.S. government all but lost its exclusive grip on the technological infrastructure of remote sensing, but economic developments in the manufacture of satellites and their components have also made it possible even for universities to launch their own vehicles.[51] For the private sector, the emergence of a lucrative civilian market is justifying major investments in satellite construction, launch, and maintenance capacities. Furthermore, the know-how, including the important area of image analysis, has been migrating to the corporate world.

As a result and short of shooting down satellites, the U.S. government is limited to regulatory measures, which consist of export restrictions and a system of "shutter control.", which limits the collection and/or distribution of data "during periods when national security or international obligations and/or foreign policies may be compromised". .[52] Such regulatory measures only apply to U.S. companies, limiting the control options to the national level.

What does this denationalization of information infrastructures and the ensuing restrictions on the control over strategic information entail for national governments, even one as powerful as that of the United States? Unquestionably, the commercialization of high-resolution imagery has limited and will continue to limit the portfolio of policy choices.[53] This will be particularly so as both market forces and mechanisms of "imagery activism" come to exploit the potential of commercial imagery.

A case in point is the Federation of American Scientists (FAS), a Washington, D.C.-based NGO, which has been ordering and purchasing images of nuclear and other military facilities from IKONOS and other commercial remote sensing satellites and is making them freely available over the Internet. These have included pictures of North Korea's No-Dong Missile Test Facility, which had long been at the heart of the debate about the country's ballistic missile capabilities and the need for a National Missile Defense System, permitting third-party assessment of the threats and the appropriateness of policies to address them.[54]

If commercial satellite remote sensing has chipped away at one prerogative of state sovereignty, i.e. control over territory, other technologies have similar far-reaching implications for another pillar of sovereignty, control over people. For centuries, the acquisition of personal data about a nation's citizens was a precondition for the exercise of most government functions. In a very real sense, there could be no taxation without such information. The modern welfare state has reinforced this trend of centralized information collection [55] and conjured up various images of Big Brother, gradually encroaching on civil liberties and privacy.

In the early stages of the information revolution, with the emphasis on centralized mainframe-based computing, governments were actually enhancing their information power vis-à-vis civil society by building up and maintaining comprehensive centralized databanks. Only with the advent of a more network-oriented approach, epitomized by the proliferation of personal computers and their connection through the Internet, has this mode of information acquisition shifted away from state-centered databanks and towards the private sector, as more and more corporations could afford the technology to collect and store customer information. The network-centric approach gave a boost to marketing, which until recently had to rely on cumbersome and costly household surveys and polls to acquire consumer data. Through data-mining techniques,[56] companies are increasingly able to put together consumer profiles from an ever-expanding number of everyday transactions. One single company, Acxiom Corporation, claims to own a database with detailed information on about 95% of American households,[57] a much higher coverage than East Germany's Stasi, the most pervasive example of government surveillance, could ever hope for.

Nations that have attempted to regulate the use of personal information have felt a particularly acute sense of loss of control as more and more multinational corporations transfer their customer information to jurisdictions with less stringent regulatory regimes. Here again, the two prongs of denationalization become apparent: the technology is vastly dispersed in the private sector and linked to a global network largely outside of any one specific jurisdiction. This, for example, prompted the European Union, fully aware of the weakening of its regulatory grip, to pass a stringent Data Protection Directive,[58] restricting the transfer of personal information outside its jurisdiction. The resulting verbal saber-rattling between the Union and the United States provides an interesting glimpse into what can happen when actors realize that an information shift between access categories is occurring.

Another recent example of the denationalization of information acquisition control is to be found in the area of biotechnology. In June 2000, the race for sequencing the human genome reached its final stage.[59] The contenders, a multi-national government-sponsored research initiative, the Human Genome Project, and a private company, Celera, crossed the finish line together when they announced the first draft of the key to life. Technically a tie, it was a huge triumph for Celera, a commercial startup, which had overcome the Human Genome Organization's (HUGO) eight-year lead-time. This stunning success was largely due to two technological factors. First, the availability and affordability of gene-sequencing technology allowed Celera to make rapid strides. Second, coming late into the game, Celera could employ powerful networks and fast computers, while HUGO relied on its legacy setup. U.S. President Bill Clinton and British Prime Minister Tony Blair, who linked up via satellite to salute the work of the scientists, could only acknowledge the fact that their governments had effectively lost one of mankind's most important datasets to a comparatively small private company. All they could do was to express their belief that "society had a duty to use the new information responsibly and for the benefit of all humankind."[60]

The information power gained by international pharmaceutical and biotechnology companies is, however, not without challenge. In the same way that new technologies have helped to shift the balance from governments to corporations, the latter are losing some of it

again The most illustrative example evolves around the proliferation of generic drugs, particularly for AIDS, which are being produced in developing countries and exported for sale at significantly lower prices than those from the big drug producers. The advent of new information acquisition technologies has made it possible to reverse-engineer the synthetic formulas of the brand drugs. A number of large pharmaceutical companies brought lawsuits to protect their intellectual property in South Africa, and their governments pressured India and Brazil, the biggest generic drug producers, to tighten their intellectual property regimes. But neither could stop the information shift from happening. India and Brazil are still producing these generic drugs, and, in South Africa, a coalition of NGOs, international organizations, and the governments of developing countries has exerted considerable pressure to have the drug companies bow out and accept new laws that effectively encroach on their intellectual property rights.[61] Two important lessons can be drawn from these cases. First, the seemingly powerful position of the international pharmaceutical companies was undermined by the ability of firms in developing countries to apply new information acquisition technologies to break the formulas. Second, this international battle was all about information power: Both the subject of the dispute – chemical formulas, i.e. bits of data – and the means of conducting it – law suits and public relations campaigns – symbolize the new world of information politics.

Information Processing

The initial development of computers is intricately linked to American military efforts in World War II and the Cold War that followed it. The Department of Defense funded the first large digital computer, ENIAC.[62] It was estimated that there was a global need for perhaps five or six computers.[63] Later, the software design for North America's air defense system, SAGE, involved one-eighth of all of the world's programmers.[64] Until 1970, only government agencies and large corporations could afford computers to automate their information processing. In the late 1960s, in fact, the United States as well as European nations envisioned the creation of a few huge databases to be shared among the major players.[65] For a few precious decades, public funding ensured governments substantial control of information processing capabilities.

This all fundamentally changed in the 1970s. The personal computer, the mouse, word processing, graphical user interfaces, and the laser printer were all conceived in a single corporation's research lab, Xerox PARC, and without formal government funding.[66] Today, we live in a world of hundreds of millions of PCs and billions of microprocessors, each one more powerful than SAGE and ENIAC combined.

Three interconnected factors have contributed to the government's loss of control over information processing capabilities: the dramatic changes in computer technology, a shift in associated research spending, and the loosening of regulatory controls and standards.

Computer technology evolves at a dramatic pace. Gordon Moore, one of the co-founders of Intel, the world's largest semiconductor company, suggested in the early 1960s that processing power would double every year and a half at constant prices.[67] His "law" still holds today, as processing power has doubled twenty times, and, in 2001, is roughly a million times greater than in 1965. But Moore's law has another even more important ramification. It implies that, at constant processing power, prices will be halved every eighteen months. A computer that cost a million dollars in 1965 can be built for a dollar today. Such rapid technological development has ensured that computers have lost their exorbitant price tags to become affordable, first for smaller and smaller corporations and then for individuals.. In fact, today's mobile phones have more processing power than the entire NASA computer network for the Gemini missions. This affordability has made it all but impossible for governments to argue that information processing needs to stay centralized in order to be efficient.

Governments have also lost another avenue for controlling the development and use of information processing. Originally, the government, specifically Department of Defense contracts, funded much of the information technology industry in the United States. ENIAC and SAGE were government projects. But the developments at Xerox PARC were not, and this signified the imminent shift of the center of gravity for funding from the public to the private sector. Today, government funding for information technology research and development pales compared with that from the commercial sector. In 2000, Microsoft's R&D budget alone was double that of the Defense Department's main research agency,

DARPA.[68] Similarly, Intel, Cisco, and other industry players have overtaken major government players in funding IT R&D.[69]

Losing the power of the purse coincided with government's partial loss of regulatory control. Initially, government-controlled procedures, mechanisms, and organizations, from NIST to ANSI to ISO, were involved in standardizing many aspects of information technologies.[70] With the rapid ascent of new, highly competitive hardware and software companies, like Microsoft and Cisco, much of the standard setting today has shifted away from existing channels and towards de facto standards set by industry leaders.

The struggle to control cryptography provides a vivid example of all three of these factors working together.[71] Cryptography is possibly the most critical access control mechanism, as it provides information processing tools that limit information access to the intended recipient. Hence, cryptography is essential in protecting strategic and commercial information. It is little wonder then that governments have kept a tight lid on cryptographic developments. For many decades, the state held a monopoly over the ability to restrict access to information through encryption. Today, that monopoly has vanished. The state no longer controls the means to restrict access to information. Encryption is available for everyone, stronger and easier to use than ever before, enabling corporations, non-state actors, and individuals alike to guard strategic and commercial information, and thus to maintain effective information access categories.[72]

Technological advances have made encryption fast and easy to use. At the same time, the government has lost its primacy of processing power. It is no longer the state alone that can afford to have its supercomputers try to break encoded messages. Corporations and NGOs have access to tremendous computing power, especially when they team up. In fact, the largest physical computer in the world is no longer operated by the U.S. Department of Energy, but by the startup Celera to sequence the human genome.[73] And the largest computing power available to anyone on the globe – an average of 100 trillion instructions per second – is administered by Setiathome, an NGO in California, that is searching for extraterrestrial intelligence in radio telescope data through a massively distributed computing

network built into popular PC screen savers.[74] Even strongly encrypted information would eventually succumb to such a powerful onslaught.

The second factor coming into play is the shift in research. For many decades, the U.S. government, through its top secret National Security Agency (NSA), kept tight control over the field of cryptography, mainly by employing and funding most of the relevant research.[75] In the 1970s, three MIT researchers not associated with the NSA discovered a cryptographic method whose strength was independent of its underlying workings, among other advantages. They published their findings.[76] Suddenly, the most precious information on cryptography shifted from highly confidential and strategic information to free information. With the ascent of the Internet and e-commerce, private sector research in encryption soared, and the resultant funding now easily outstrips that which can be provided by the government.

The only remaining strategy for the government to retain some control over this development was to regulate the use of cryptography. For many years, the Clinton administration put forward a number of regulatory frameworks,[77] which would permit encryption, but provide a master key and thus total access, to the government. Eventually all such plans folded. Towards the end of his tenure, under industry pressure not to allow companies from other countries with looser restrictions fill the void, President Clinton even lifted most of the remaining restrictions on export of encryption technology.[78]

The encryption example is paradigmatic for the broader changes in information processing. Through technological developments, the shift of funding to the private sector and the loss of regulatory mechanisms, governments have lost their primacy in controlling important parts of the information processing landscape. To be sure, they are still powerful and wield substantial influence. But their singular importance has vanished.

Information Distribution

This trend is perhaps even more apparent with respect to the various means of information dissemination. For many decades and with the notable exception of the United States,

broadcast media such as radio and TV were state-owned and controlled in many nations around the world. In the vast majority of these cases, ownership of the distribution infrastructure implied control over content. Governments could, in effect, keep information within their chosen access categories.

At least three fairly recent global developments have fundamentally undermined this traditional governmental grip: the rise of private ownership of broadcast media; the advances in satellite distribution technology; and – by far the most important – the dramatic ascent of the Internet.

Between 1980 and 2000, the market share of privately owned broadcast corporations rose continuously.[79] In Europe, and assisted by a number of watershed decisions by European Union and national courts, privately owned media corporations were permitted to introduce broadcast services.[80] Their audiences have grown ever since. Of course, not all state-owned broadcasters have fared badly. Some withstood the onslaught of the marketplace quite well. But they all find themselves operating in a vastly different environment, in which, due to market forces and fierce competition, direct government control over content is hardly an option any longer, not even for state-owned broadcasters.

The opening up of the national broadcast markets and the pressures on governments to give up direct control over the broadcast distribution infrastructure were not only prompted by judicial decisions and a substantial shift in public opinion. They were also enhanced by the introduction and rapid acceptance of satellite technology permitting the distribution of a multitude of television and radio programs directly to individual homes. In 1988, Direct-to-Home (DTH) satellites reached 4.4 million receivers in individual homes worldwide. Only seven years later, in 1995, more than 33 million such receivers had been installed.[81] DTH satellites are especially attractive in areas where there is no cable television service. Studies indicate that, even in the United States, with its well built-up cable infrastructure, households with DTH receivers will outnumber those subscribing to cable television by 2003.[82]

DTH satellites are not just a commercial success story. They also create an information infrastructure for radio and TV distribution largely beyond government influence. Unlike

conventional transmitters, the satellites themselves, once in orbit, are outside the practical physical control of national governments, while terrestrial relay stations for the uplink can be located at great distances from the target broadcast area – even on the high seas. Governments could use regulatory means to prohibit the reception of satellite signals. In fact, this is what the Islamic Republic of Iran has done. But today, DTH receivers are very small – the size of a sheet of paper – cheap – well below US $100 – and easy to install. Enforcement, therefore, is difficult, costly and – as the case of Iran, as well as previous regulatory attempts in Saudi Arabia have demonstrated – largely ineffective.

Except for tremendously costly measures like regulatory control on the receiving end or brute force methods like frequency jamming and economic blackmail, governments have lost control over a very substantial and rapidly increasing part of the global broadcast information infrastructure. Much has been written about the "CNN effect," for which DTH satellites provide a key element.[83]

The third, and by far most important, development in the denationalization of information distribution has been the rise of the Internet. Originally funded entirely with U.S. government money, through the Department of Defense's ARPA (later DARPA) program, the Internet provides an efficient, robust, and decentralized information network of global reach. In stark contrast to existing information distribution structures like TV or radio, the Internet provides bi-directional communication channels for anyone and everyone using it. Everyone can be an information provider and information receiver at the same time. In Internet jargon, traditional distribution networks provided one-to-many information flows, while the Internet is – at least in principle – built to permit many-to-many information exchanges.

These technical foundations restrict governments' ability to control information flows. As the network is built to automatically reroute information flows around bottlenecks, stopping or restricting the flow of information on the net is quite difficult. In the wake of the Tiananmen Square uprising, the Chinese government experienced this problem first-hand. At the start of the military clampdown, they disconnected international telephone and fax lines, and even the official Internet connection. Still, e-mails updated from the student

protesters were received at MIT and other U.S. universities. These messages, when encountering the disconnected main network link, were automatically rerouted on a Beijing subsidiary of a large multinational corporation, which was connected to its headquarters in the United States by an internal network connection. The U.S. headquarters was connected to the Internet. It was through this back door that the e-mails from the beleaguered Beijing protesters traveled. Nobody had thought about this connection, neither the Chinese government, nor even the student protesters. The important lesson is that they did not have to. The Internet takes care of routing information itself, attempting to find ways around every obstacle en route to the desired destination.

Despite of this setback, the Chinese government has been continuing its efforts to control the Internet. Although it seems to have dropped earlier plans to build a China-only intranet, separated from the Internet by a "Great Firewall", a series of efforts are in place to limit access to the net and to censor its contents. A Ministry of Information Industry has been created to regulate Chinese access to the Internet, while the Ministry of State Security has been assigned to monitor local use of the Internet. A series of regulations have been introduced, which limit direct foreign investment in Chinese Internet companies, ban the dissemination of any information "that might harm unification of the country" and obligate all service providers to monitor content in chat rooms and to restrict controversial topics.[84] Testimonial evidence[85] suggests that the Chinese control system is less than perfect. Rules and regulations are difficult to enforce in a country where the number of Internet users doubles every six months, and where technical fixes such as anonymous proxy servers are easily available to bypass government restrictions.

Concerns about this largely uncontrollable, yet powerful, global information infrastructure are not limited to the Chinese government but must worry anyone who wishes to maintain information control. The tremendous pace of acceptance of the Internet throughout the world only exacerbates these fears. The Internet has grown from a few hundred thousand users ten years ago to a community of a couple of hundred million throughout the world. Its growth rate is even faster than that for information processing. Bandwidth, the amount of information that can be transmitted over a network, triples every year.[86] Because of the Internet's many-to-many structure, adding a single new user does not just increase the

possible information channels of the network by one, but by the number of already existing network users. In other words, the value of the network rises with the square of the number of participants, because every new user can theoretically communicate with every other existing user on the net. Taken together, bandwidth growth and network value increases help explain the tremendous power pull witnessed over the last few years. They also lay the foundation for the Internet's distributed and rapidly expanding structure, which makes it very difficult to control access to and information flows within the network. To be sure, control is still possible but it comes at a very high price that few are willing to pay.

In addition to the inherent lack of physical bottlenecks permitting control of the Internet, ownership over the network infrastructure has shifted over the last two decades. The central "backbone" of the network used to be funded and operated by the U.S. National Science Foundation (NSF) to link together research facilities and academic institutions across the country. The NSF divested itself from this role in the early 1990s. Today, backbone functionality is provided entirely by the private sector, with communication giant MCI contributing the largest share. This commercialization is not just limited to infrastructure. While, in 1990, most Internet users came from public sector institutions, including universities, today the majority is using the Internet through an extensive network of commercial Internet service providers (ISP), who offer access as well as storage and information distribution facilities, such as web servers, to anyone who chooses to pay for them.[87]

The denationalization of control and ownership, as well as the commercialization of the Internet, extend to the network governance structures. For decades, the U.S. federal government maintained overall control of the assignment of network addresses and Internet domain names. It later subcontracted this task to a private corporation. The Clinton administration then took the bold step of abdicating its regulatory role and transferring all these governance functions to a newly established non-profit entity called ICANN (Internet Corporation for Assigned Names and Numbers). A board of directors, who represent industry, non-profit stakeholders, and – through global electronic elections – Internet users, governs ICANN.[88]

Taken together, the Internet's decentralized structure, the commercial ownership of many of its central facilities, and the state's retreat from regulating its name space create a fundamentally open infrastructure for everyone to use. This does not imply that all is lost for state actors, but that the rules of the game have fundamentally changed.

Despite some rhetoric to the contrary, state actors have been fairly slow in adapting to the new situation. Government bureaucracies are prone to inertia. Changing the way they operate is a difficult and time-consuming task. Organizational power is still derived from the size of one's budget, not one's contribution to the bottom line. This is exacerbated by the long-term procurement cycles in many public institutions. These and other reasons have made it difficult for the public sector to quickly and pragmatically embrace the 'net.

Corporations and NGOs, on the other hand, have fairly quickly adapted to the new rules. E-commerce has taken off and is responsible for a steady stream of more than six million individual commercial transactions every week. Many corporations that have hoarded information for years absent a viable market now find that the Internet is a very effective tool for commercializing their information vaults. Hence, large amounts of information are moved from the strategic to the commercial access category. Other actors, especially NGOs, see the Internet as an ideal information distribution structure, permitting them to reach a global audience for the cost of dial-up access.

The Zapatistas in Mexico were among the first to supplement their actions with cyber-campaigns. Long after all military operations had ceased, news of the Zapatistas and their struggle were fed through the Internet to media around the world. The Zapatistas may have lost their battles on the ground, but on the net their strategy proved far more successful. Similarly, it has been said that one reason why the United States lost the Vietnam War was that the North Vietnamese had attacked its enemy's real center of gravity – domestic public opinion. David Ronfeldt and others make a similar argument when they point to the strategic shift from actual military conflict to information warfare through the constant re-imagining and re-telling of the struggle on the Internet.[89]

A Serbian private radio station, B92, provides one of the best examples of the shifting control of information distribution structures. B92 was among the first private radio stations licensed in Yugoslavia. Broadcasting from Belgrade, it quickly gained credibility among the public for its independence and provided a fresh alternative to the state-controlled radio and television channels. Fearing B92's impact, the Milosevic regime restricted the station's reach by limiting the power of its transmitter. When other private radio stations in the country wanted to link up with B92 and transmit B92's news, the government prohibited the build-up of such a terrestrial private network. Undeterred, B92 worked out a deal with the BBC. News broadcasts would be uplinked from Belgrade's B92 studio to a BBC satellite, then downlinked into Yugoslavia. Local radio stations could then use affordable satellite receivers to pick up the signal and rebroadcast it locally. Thereby, B92 effectively circumvented governmental restrictions on a terrestrial network by using a satellite–based infrastructure instead.

Escalating the conflict, the government then confiscated B92's transmitter. Unrelenting, the radio station continued, however, to produce its popular programs. It digitized its broadcasts and transferred the audio files via the Internet to Vienna, where they were broadcast towards Serbia through the Austrian Broadcasting Corporation's strong medium-wave transmitter.

This arrangement ended when the Milosevic government seized the offices of B92, forced its journalists into hiding, and installed a group more to its liking. But few tuned in to the "new" B92. The original B92 journalists went underground or left the country. Within a few days, they had moved their reporting to the Internet, this time to a website hosted by a Dutch NGO. Soon, they received millions of page hits, many of them from Serbian Internet users who once again had found their trusted source of information.

The Milosevic government tried no less than three times to control the distribution of information it disagreed with. And all three times, B92 was able to shift its information distribution infrastructure so that it could escape these restrictions. The government's forceful actions were not completely in vain, however. Each time B92 had to shift its infrastructure, it lost some of its listeners. But at each level, the government incurred a very

substantial political cost – and ultimately still failed to completely quash B92's independent voice.

Milosevic's failure to effectively contain B92 at reasonable cost has little to do with his lack of ingenuity or effectiveness. It is a result of the fact that the information distribution infrastructures used by B92 have become less and less controllable by national governments. It is relatively easy to prevent a private broadcaster from building a national network by denying it the terrestrial relaying capabilities. Once B92 overcame that hurdle, however, the government had to take much more direct action – the confiscation of the transmitter – and pay the political price for it. When B92 began to use a transmitter outside of Serbian territory, Milosevic was foiled again. He could have prohibited the use of radios in Serbia or listening to B92's broadcasts. But enforcement of such measures would have been difficult and costly. He could have tried to jam B92's frequency. But this, too, would have been very costly and, given Serbia's geography, might have been only partially effective. Instead, Milosevic opted to use the one choke point he still controlled, B92's physical location in Serbia. Closing the office silenced the radio station. But it did not silence the individuals, who, using the phone system and laptops, could still send their reports over the net to the Netherlands, where they were posted on the website. Milosevic's only option then would have been to disconnect from the Internet. This he did not dare. Not because he feared domestic public opinion. His concern was that he would lose his international soapbox as well as the ability to manage the country (and his war efforts) financially and economically. In addition, his gain would have been limited. He would have taken out B92. Yet many Serbs own DTH satellite receivers, providing them with dozens of alternative news channels.[90]

B92 is only one example of a larger trend. More and more information distribution infrastructures around the globe have become "denationalized" by residing outside of national territory, by using technology that is small, cheap, easy to use and difficult to interdict, and by employing quickly growing network structures based on a decentralized, many-to-many paradigm. Control is still possible but its price has risen steeply.

CONCLUSION

This paper aimed to contribute to the discussion about the effects of the information revolution on the conduct of international affairs. It provides a framework that highlights the role of information power and its shifts among and between the key stakeholders – governments, corporations and NGOs. We attribute these power reconfigurations to shifts of control over the underlying information infrastructures.

Information has become a key asset in global affairs, transcending its instrumental role as a multiplier of other power sources to evolve into a potent resource in its own right. And unlike military might, information is not the exclusive domain of states, but used by corporations and civil society as well. In fact, each of the three actor groups increasingly resorts to information assets to foster their relative power positions.

Keohane and Nye suggested that much of information power is about controlling various forms of information. They identified three types depending on the value attributed to certain data - strategic, commercial, and free information. We expanded this approach by highlighting that these categories are determined by the form of access control rather than the nature of the information. The paper also stipulated that all forms of information - the well-guarded secrets of military intelligence, the intricacies of software programs, or the testimonials of human rights violations -, affect the power equation.

Actors may attempt to deliberately shift information from one access category to another to further enhance their relative power positions. A government, for example, may decide to publish confidential intelligence information to solidify international public support for its foreign policy objectives. Corporations may shift information between access categories as well, as evidenced by the open code movement in software - a shift from strategic to free information. Finally, several NGOs have begun to merchandise their brands - a shift from free to commercial information.

The focus of this paper, however, is less on these deliberate than on the unintentional shifts in access categories. While deliberate shifts are attempts to enhance one's power, an

unintentional shift typically causes a relative loss of power. Such is the case when intelligence information becomes available commercially through another source, or when businesses are forced to disseminate their commercial information for free.

We suggest that these unintentional shifts happen when actors lose power over the underlying structures of access control. We demonstrated that these shifts have disadvantaged governments as a result of what we termed the "denationalization" of information infrastructures. This phenomenon describes both the growing privatization of information acquisition, processing, and distribution, and its parallel transnationalization. Together, these two aspects have made it increasingly difficult for states to maintain their erstwhile monopolies of information control.

This erosion occurs at various levels. First, many governments no longer physically own major parts of the information infrastructure. Whether it is remote sensing satellites, supercomputers or the Internet, governments are increasingly taking a back seat. This is largely due to the second factor, the economics of information control. The corollary of the exponential growth in technological capacities was a paradigmatic shift in affordability, which broke down many economic barriers protecting governmental control of information access. Third, the removal of technological and economic obstacles also made it increasingly, costly for governments to use regulatory means. This is particularly evident in the ease with which information infrastructures transcend national jurisdictions.

While our analysis does not claim to provide a comprehensive and complete theory of international power in the information age, the paper's framework about the relationship between the control over information infrastructures and the ability to control access to information has two apparent benefits: First, it permits us to identify one of the levers through which modern information and communication technologies affect a critical ordering factor of international affairs, i.e. relative power. It thus offers an alternative to the largely intuitive postulations about the consequences of the information revolution.. Second, the framework applies to all major actors in international affairs, thereby avoiding a rigid model of state decline. Insofar as they control substantial parts of information

infrastructures, corporations and civil society organizations are also subject to unintentional shifts in information access categories.

Although the denationalization of information infrastructures is at the core of our paper, we do not advocate the demise of the nation-state. While the erosion of state monopolies over information access is a clear and present pattern, this process is not irreversible. States – as well as other actors – do have the possibility to recapture lost power by regaining control over information infrastructures. Such an option, while often not realistic given the economic and regulatory constraints of today's information infrastructure regimes, might become feasible again in the not so distant future. Furthermore, actors that are under pressure of losing control over information access might be particularly poised to make effective use of their dwindling resources by using deliberate shifts to regain relative power. Last but not least, control of information access is just one, albeit important, asset in the portfolio of power. While information has "infiltrated" other traditional power sources it has not substituted them.

Consequently, we have refrained from pronouncing the end of the nation-state as the logical and unavoidable outcome of the denationalization of information infrastructures. Any such declaration would be premature in light of the dearth of quantitative data and our still embryonic understanding of the scope of information power. We do, however, believe that the ascent of information as a power source and its diffusion among actors are opening a new chapter in defining and understanding international affairs.

Notes

[1] See United States Department of State. Diplomacy for the 21st Century: Information Technology Goals for the First Five Years – Building the Information Organization, Washington 1998; Center for Strategic and International Studies (CSIS), Reinventing Diplomacy in the Information Age, Washington 1998; Henry L. Stimson Center. Equipped for the Future: Managing U.S. Foreign Affairs in the 21st Century. Washington 1998.
[2] See http://www.creativeswitzerland.com/, and for experiences in Slovakia and Norway also Jozef Batora, Jr.: Challenges and Opportunities: Slovak Diplomacy in the Information Age, Slovak Foreign Policy Affairs, Spring 2000, pp. 86-101; Jozef Batora, Jr. and Iver B. Neumann: Fear of Surfing: The Norwegian Ministry of Foreign Affairs Negotiates the Wave of the Information Age, (currently in the submission process in Diplomacy and Statecraft).
[3] Andy Grove's Rational Exuberance, Interview by John Heilemann, WIRED June 2001, pp. 136-147.
[4] Michael Porter et al., Global Competitiveness Report 2000, Oxford University Press, 2000.

[5] Maxwell Cameron et al., To Walk Without Fear: The Global Movement to Ban Landmines, Oxford University Press, 1998.
[6] David Ronfeldt / John Arquilla / Graham E. Fuller / Melissa Fuller, The Zapatista Social Netwar in Mexico, RAND, 1998.
[7] See, for example, Susan Strange, States and Markets, Blackwell 1988; Jean-Marie Guehenno, The End of the Nation-State, University of Minnesota Press, 1995; Robert O. Keohane and Joseph S. Nye, Jr., Power and Interdependence in the Information Age, Foreign Affairs 1998, vol. 77 (5), pp. 81-94; Joseph S. Nye, Jr. and William A. Owens, America's Information Edge, Foreign Affairs 1996 (March/April), pp. ; Walter Wriston, The Twilight of Sovereignty, Scribner's 1992.
[8] Gordon E. Moore, Moore's Law, in Richard Rhodes (ed.), Visions of Technology, Simon & Schuster (1999), pp. 243-244.; George Gilder, Telecosm: How Infinite Bandwidth Will Revolutionize Our World, Free Press, 2000.
[9] See, for example, Manuel Castells, The Rise of the Network Society, Blackwell 1996.
[10] See, for example, the chapters in William Drake, The New Information Infrastructure: Strategies for U.S. Policy, Brooking 1995; Brian Kahin and James H. Keller (eds), Coordinating the Internet, MIT Press 1997.
[11] See, for example, Jessica T. Matthews, Power Shift, Foreign Affairs January/February 1997, pp. 50-66.
[12] Stanley Hoffman, Notes on the Elusiveness of Modern Power, International Journal 30 (Spring 1975), p. 204.
[13] See, for example, the three reports of the Carnegie Endowment for International Peace Study Group on the Information Revolution and World Politics available at http://www.ceip.org/programs/info.
[14] Ibid.
[15] Joseph S. Nye, Jr., Bound To Lead: The Changing Nature of American Power, Basic Books, 1990, p. 25.
[16] See, for example, Peter Bachrach and Morton S. Baratz, The Two Faces of Power, American Political Science Review 56 (1962), pp. 947-52; Steven Lukes, Power: A Radical View, Macmillan, 1974; Steven Lukes (ed.), Power, Blackwell, 1986; Barry Barnes, The Nature of Power, Polity, 1988; Dennis H. Wrong, Power: Its Forms, Bases, and Uses, Transaction Publishers, 1995.
[17] For an overview, see Jeffrey Hart, Three Approaches to the Measurement of Power in International Relations, International Organization, 30/2 (Spring 1976), pp. 289-305.
[18] Hart, ibid.; Robert O. Keohane and Joseph S. Nye, Power and Interdependence, Second Edition, HarperCollins, 1989.
[19] Steven Lukes, Power: A Radical View, Macmillan, 1974, p.13.
[20] See particularly Peter Bachrach and Morton S. Baratz, Decisions and Nondecisions: An Analytical Framework, American Political Science Review 57 (1963), pp.641-51.
[21] Steve Breyman, Knowledge as Power: Ecology Movements and Global Environmental Problems in: Ronnie D. Lipschutz and Ken Conca (eds.), The State and Social Power in Global Environmental Politics, Columbia University Press, 1993, p. 126.
[22] See, for example, Peter Bachrach and Morton S. Baratz, The Two Faces of Power, American Political Science Review 56 (1962), pp. 947-52; or Dennis H. Wrong, Power: Its Forms, Bases, and Uses, Transaction Publishers, 1995.
[23] Joseph S. Nye, Jr., Bound To Lead: The Changing Nature of American Power, Basic Books, 1990.
[24] Stanley Hoffman, Notes on the Elusiveness of Modern Power, International Journal 30 (Spring 1975), p. 183.
[25] Michel Foucault, Power/Knowledge: Selected Interviews and Other Writings 1972-1977, Pantheon Books, 1977.
[26] Dennis H. Wrong, Power: Its Forms, Bases, and Uses, Transaction Publishers, 1995, pp. 52-60.
[27] Susan Strange, States and Markets, Blackwell 1988.
[28] James Rosenau, Turbulence in World Politics: A Theory of Change and Continuity, Princeton University Press, 1990, pp. 198-209.
[29] Peter Haas, Introduction: Epistemic Communities and International Policy Coordination, in Peter Haas (ed.), Knowledge, Power and International Policy Coordination, pp.1-36, University of South Carolina Press, 1992.
[30] Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence, Second Edition, Revised, Brassey's, 1993, p. 1.
[31] See, for example, the 1999-2000 estimated trade losses due to copyright piracy, compiled by the International Intellectual Property Association (IIPA) and available at
http://www.iipa.com/pdf/2001_Apr30_LOSSES.pdf/
[32] Outsourcing to India: Backoffice to the World. The Economist, 5 May 2001.

[33] http://www.newstimes.com/archive98/feb2098/cpb.htm.
[34] Boomgalore. WIRED March 2000 available at http://www.wired.com/wired/archive/8.03/bangalore_pr.html.
[35] Margaret E. Keck and Kathryn Sikkink, Activists Beyond Borders – Advocacy Networks in International Politics, Cornell University Press/ Ithaca, 1998.
[36] See, in particular, the visionary analysis in Susan Strange, States and Markets, Blackwell 1988.
[37] Robert O. Keohane / Joseph S. Nye, Jr., Power and Interdependence in the Information Age, Foreign Affairs 1998, vol. 77 (5), pp. 81-94.
[38] The first of Woodrow Wilson's Fourteen Points (http://www.yale.edu/lawweb/avalon/wilson14.htm) states: "Open covenants of peace, openly arrived at, after which there shall be no private international understandings of any kind but diplomacy shall proceed always frankly and in the public view."
[39] The struggle within the State Department about how much control over information is necessary spans decades; Anthony Oettinger wrote in 1968 about the resistance of ambassadors to permit the use of telephones by their staff, fearing loss of control over the information flows; Anthony Oettinger, Education Technology, in Foreign Policy Association (ed), Toward the Year 2018 (Cowles 1968), p. 75.
[40] For descriptions and analysis of the Open Software Movement, see Chris DiBona, Sam Ockman, Mark Stone, Open Sources – Voices from the Open Source Revolution, O'Reilly 1999; Glyn Moody, Rebel Code – Linux and the Open Source Revolution, Perseus 2001; Eric S. Raymond, The Cathedral and the Bazaar – Musings on Linux and Open Source by an Accidental Revolutionary, O'Reilly 1999.
[41] The limits to growth?, The Economist, 30 July 1998.
[42] Norbert Wiener, Cybernetics, or Control and Communication in the Animal and the Machine (2nd. ed. 1961), p 166.
[43] Viktor Mayer-Schönberger and Deborah Hurley, Globalization of Communication, in Joseph S. Nye and John D. Donahue, Governance in a Globalizing World, Brookings, 2000, pp. 135-151.
[44] This is the title of the best-selling Being Digital, by Nicholas Negroponte, Knopf (1995), pp. 11-20.
[45] Tim Jordan, Cyberpower – The Culture and Politics of Cyberspace and the Internet, Routledge 1999.
[46] For an excellent overview of remote sensing see the NASA tutorial at http://rst.gsfc.nasa.gov/Front/overview.html.
[47] See, for example, Jeffrey T. Richelson, America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program, Harper & Row, 1990; William E. Burrows, Deep Black: Space Espionage and National Security, Berkley Books, 1986;, Dwayne A. Day et al. (eds.), Eye in the Sky: The Story of the Corona Spy Satellites, Smithsonian 1998; see also the overview by the Federation of American Scientists (FAS) at http://www.fas.org/spp/military/program/imint/index.html.
[48] With the end of the Cold War, Russia entered the commercial market. The first images of 2m resolution were made available in 1992, but the fact that the Russian government seemed to release images on a case-by-case basis made them commercially unattractive. This changed with a joint venture between a U.S. company and the responsible Russian agency, which are now marketing these images on the Internet under the SPIN-2 trademark.
[49] IKONOS is just the first one in a series of high-resolution commercial satellites. Other planned launches include Orbimage's Orbview-3 and 4, Earthwatch's Quickbirds, and several satellites by West Indian Space. SpaceImaging, in the meantime, has received a license for 0.5m resolution (see http://www.spaceimaging.com/newsroom/releases/2001/halfmeter_license.htm).
[50] The Next Wave. WIRED April 2001 available at http://www.wired.com/wired/archive/9.04/sealaunch.html.
[51] For an overview of various small satellite projects, see http://www.ee.surrey.ac.uk/SSC/SSHP/.
[52] See Fact Sheet: Foreign Access to Remote Sensing Space Capabilities.
[53] For a good overview of the policy implications of high-resolution imagery, see Yahya Deqanzada and Ann Florini, Secrets for Sale: How Commercial Satellite Imagery Will Change the World, Carnegie Endowment for International Peace, 2000.
[54] FAS also provided some analysis of the images, calling the facilities "underwhelming" and the whole scenario "a mouse that roared." This assessment pointed to the disproportionality of American reactions to the North Korean threat and allowed public opinion to form its own views.
[55] Viktor Mayer-Schönberger, Generational Development of Data Protection in Europe, in: Philip E. Agre and Marc Rotenberg (eds.), Technology and Privacy: The New Landscape, MIT Press 1997, pp.219-241.
[56] For an overview see http://www3.shore.net/~kht/text/dmwhite/dmwhite.htm.
[57] The surveillance society, The Economist, 29 April 1999.

[58] For the text, see http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.
[59] See Kevin Davies, Cracking the Genome – Inside the Race to Unlock Human DNA, Free Press, 2001.
[60] http://news.bbc.co.uk/hi/english/sci/tech/newsid_805000/805803.stm.
[61] Drug-induced Dilemma. The Economist, 19 April 2000.
[62] See Scott McCartney, ENIAC – The Triumphs and Tragedies of the World's First Computer, Walker Publishing New York, 1999.
[63] Ceruzzi attributes this to computer pioneer Howard Aiken, although this is doubtful. Paul E. Ceruzzi, A History of Modern Computing, MIT Press 1998, p. 13.Paul Cerruzzi, "An Unforeseen Revolution: Computers and Expectations, 1935-1985." [160-174]
[64] Paul N. Edwards, The Closed World – Computers and the Politics of Discourse in Cold War America, MIT Press 1996, p. 103.
[65] See Colin Bennett, Regulating Privacy, Cornell University Press 1992, pp. 46-49; Arthur R. Miller, The Assault on Privacy, University of Michigan Press 1971, pp. 71-82.
[66] Of course, Xerox PARC benefited substantially from the human capital of researchers previously employed by the government or paid through government research grants. See Michael Hiltzik, Dealers of Lightning – XEROX PARC and the Dawn of the Computer Age, Harper, 1999.
[67] Gordon E. Moore, Moore's Law, in Richard Rhodes (ed.), Visions of Technology, Simon & Schuster (1999), pp. 243-244.
[68] In 2000, Microsoft spent U.S. $3.775 billion (vs. $2.970 in 1999) on R&D; see Microsoft Annual report 2000, http://www.microsoft.com/msft/ar.html. The Department of Defense 2000 Budget allocated U.S. $1.951 billion to DARPA, the Department's research arm who originally funded the Internet. Of this, U.S. $377 million were allocated to Computing and Communication Systems, and a mere U.S. $15 million to research on the "next Internet"; see Department of Defense 2000 Budget at http://www.dtic.mil/comptroller/fy2001budget/fy2001r1.pdf.
[69] In 2000, Intel had an R&D budget of U.S. $3.897 billion and employed more than 6,000 researchers in 80 laboratories worldwide; see http://www.intel.com/labs/; Cisco spent U.S. $2.704 billion on R&D in 2000; see http://www.cisco.com/warp/public/749/ar2000/low/financials/consolidated_state.html.
[70]
[71] For a general account of the art of cryptography, see David Kahn, The Codebreakers – The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner 2nd ed 1996; Bruce Schneier, Applied Cryptography, Wiley 2nd ed. 1995.
[72] For example, an implementation of the strong RSA encryption algorithm is available as a freeware software program called PGP (for "pretty good privacy"); see http://www.pgp.com. See also generally Simson Garfinkel, Pretty Good Privacy, O'Reilly 1996).
[73] Celera's data center network consists of 10,000 individual processors and computes 1.3 trillion floating point operations per second (teraflops); see David Pescovitz, Monsters in a Box, WIRED December 2000, pp. 341-347; the largest government supercomputer, an IBM ASCI White operated by Lawrence Livermore Laboratories, sports "only" 8,192 processors, although it still outpaces Celera slightly with a performance of 4.9 teraflops; for a current chart of supercomputing power, see http://www.top500.org.
[74] http://setiathome.berkeley.edu utilizes an average of 100,000 networks processors, and a sustained computing power of 100 teraflops, about 20 times more than the fastest physical supercomputer.
[75] See Whitfield Diffie and Susan Landau, Privacy on the Line – The Politics of Wiretapping and Encryption, MIT Press 1998, p. 56.
[76] R. Rivest, A. Shamir, L. Adleman, A Method of Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM Vol 21 (2), pp. 120-126.
[77] For a detailed description, see Whitfield Diffie and Susan Landau, Privacy on the Line – The Politics of Wiretapping and Encryption, MIT Press 1998; Steven Levy, Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age, Viking 2001.
[78] A major liberalization in January 2000 (see http://www.epic.org/crypto/export_controls/finalregs.pdf for the full text) was followed by another liberalization in October 2000 as a revision to the Export Administration Requirements (EAR), issued in direct response to a drastic EU liberalization by the U.S. Department of Commerce Bureau of Export Administration (BXA) (see http://www.bxa.doc.gov/Encryption/pdfs/EncryptionRuleOct2K.pdf).
[79] For detailed data see Mark Balnaves / James Donald / Stephanie Hemelryk Donald, The Penguin Atlas of Media and Information - Key Issues and Global Trends (2001).

[80] On a European level, see only the Judgement of the European Court of Human Rights in Informationsverein Lentia and Others v. Austria, November 24, 1993, A276.
[81] ITU, World Telecommunication Indicators Database, 4th edition.
[82] Digital DTH Subscribers to Outnumber Digital Cable Subscribers through 2003, Business Wire, October 19, 1999.
[83] See, for example, Piers Robinson, 'The CNN Effect: Can the News Media Drive Foreign Policy?', Review of International Studies, Vol. 25, No. 1 (1999); Don M. Flournoy and Robert K. Stewart, CNN: Making News in the Global Market, University of Luton Press 1997; Steven Livingston and Todd Eachus, "Humanitarian Crises and U.S. Foreign Policy: Somalia and the CNN Effect Reconsidered," Political Communication, Vol. 12 (1995); Nicholas Hopkinson, The Impact of New Technology on the International Media and Foreign Policy, Wilton Park Paper 97, London: HMSO (1995); Center for Defense Information, The CNN Effect, available at http://www.cdi.org/adm/834/.
[84] For more details about these regulations and their effectiveness see Lin Neumann, The Great Firewall, available at http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html, and the Human Rights Watch Backgrounder on Freedom of Expression and the Internet in China, available at http://www.hrw.org/backgrounder/asia/china-bck-0701.htm.
[85] see Neumann, supra.
[86] This is often called Gilder's law; see George Gilder, Telecosm: How Infinite Bandwidth Will Revolutionize Our World, Free Press, 2000.
[87] See, for example, 4 Firms Control Half of Net Usage, The Industry Standard, June 5 2001, http://www.thestandard.com/article/0,1902,26904,00.html.
[88] See http://www.icann.org.
[89] David Ronfeldt, John Arquilla, Graham E. Fuller, and Melissa Fuller, The Zapatista Social Netwar in Mexico, RAND, 1998.
[90] The authors have conducted interviews with B92 members; for published accounts see Pantic, B92 of Belgrade, Media Studies Journal, New York, Fall 1999, Vol. 13, Issue 3, pp. 176-181; Matic/Pantic, War of words: When the Bombs Came, Serbia's B92 Hit the Net, The Nation, November 29, 1999; issue 18, pp. 34-35.