BOMBS AND BANDWIDTH

THE EMERGING RELATIONSHIP BETWEEN INFORMATION TECHNOLOGY AND SECURITY

ROBERT LATHAM, EDITOR

PROJECT COORDINATED BY THE

SOCIAL SCIENCE RESEARCH COUNCIL. NEW YORK

THE NEW PRESS

NEW YORK
LONDON

CONTENTS

INTRODUCTION

ROBERT LATHAM

The relationship between information technology (IT) and security is as old as society itself. Ancient societies, like modern ones, sought information about the intentions and actions of real or imagined enemies (what we now call "intelligence"). Their technology was not the telegraph, radio, or satellite but the tower, smoke signal, and horse. In between the modern use of sophisticated electronic technologies and the ancient use of physical and mechanical technologies lies a long history of change in the relationship between IT and security.'

Our purpose here is not to trace that history but to focus on and critically assess contemporary changes. We believe we are in the midst of an important period of transformation. States, militias, firms, nongovernmental organizations (NGOs), social movements, and ethnic groups the world over are increasingly making advances in digital IT—associated with computers and networks such as the Internet—a central factor in their strategies of action and choices about how they organize themselves. Compared to the past these social entities are now far more self-conscious about IT as an instrument of action and means of organization. This heightened awareness does not stem simply from the high level of attention IT has received in mass media. Far more important is the ability of groups to be directly involved in designing and applying IT for their own uses, as desktop computers and local, organization-specific, digital networks (e.g., Ethernets) become increasingly widespread.

The transformation began before the attacks of September 11 (or "9/11"). But that event has galvanized and deepened attention to the relationship between IT and security, as many chapters in this volume show. Far more than earlier fears of large-scale computer failure associated with the year 2000 (Y2K), September 11 has prompted a host of questions that raise issues that extend beyond technology per se. Policy makers, journalists, activists, and citizenries around the world have become preoccupied with issues such as the development of worldwide systems of electronic surveillance; the effectiveness of such systems versus the cost in loss of privacy they may entail; the implications of terrorist organizations' use of electronic communications—from cell phones to the Internet—to coordinate their operations; the potential of the Internet to fan the embers of hatred and violence

or help the cause of peace; the perceived vulnerabilities of digitally dependent vital infrastructures of developed countries—from electric power systems to financial markets—not only to error but to purposeful electronic disruption; and the attempts of military forces to exploit innovations in IT.

These issues were probed prior to 9/11 but not with anything like the same urgency or interest, as any follower of news about the United States effort to build a system of Homeland Security can readily recognize. If the current period of transformation described above is based on changes in perceptions and strategies of action involving IT, then 9/11 must be counted as pivotal, as so many organizations, from militaries to NGOs to corporations, are treating it as an important occasion to redefine missions and approaches.

The chapters in this volume offer the reader an opportunity to develop an informed perspective from which to better understand the nature of and response to IT-related threats, the new structures of power emerging around IT, and the ethical-political implications of transformations in this area of human endeavor.

THE IMPORTANCE OF SOCIETY

These broad concerns suggest that when thinking about the relationship between IT and security it is not enough to focus on war and military organization: society is also important. It matters in four basic ways.[2] First, protecting the institutions (economic, political, and social) and resources (material and human) that make up a society has historically been understood by states to be one of the fundamental goals of security (the other, closely related goal being the survival of the state itself). For centuries, that meant protecting a society (its cities, population, national economy, form of life, and natural resources) from attack: armies could invade, ships could bomb, spies could sabotage. As contemporary developed societies increasingly rely on complex information and communication-based systems to operate, there emerges an entirely new layer of perceived vulnerability to invisible enemies attacking the systems from half a world away. Finance and commerce, electric power, health care, and city services are among the areas that depend on digital networks in the developed states and societies of the global North. If these networks are sabotaged by electronic intrusion—perhaps originating halfway around the world—it is assumed that the systems they manage would fail.

The very notion held by states that a society can be secured by strengthening national borders is challenged if entrance to its digital networks can be gained from anywhere, anytime. Concepts of national security and global security—bearing in mind that some systems like financial markets are global in scope—

are being rethought in nonterritorial, virtual terms, as the chapters by Bendrath, Denning, Gray, Libicki, and Yould suggest.

Society matters, in the second place, because social groups are the predominant users of IT and many of their applications have security implications. Most prominent today are the applications of IT by social groups that produce what are viewed as security threats. Groups associated with global terrorism, ethnic and nationalist violence, and transnational crime use IT for their own purposes: either communicating and distributing resources within their own networks (see Nordstrom and Rohozinski) or penetrating and disrupting the information systems in the developed world as just described above. (The identification of social, nonstate actors as producers of threats does not displace states as sources of threats via IT. As Bendrath points out, both types of actors are on the radar of the U.S. government)

Of course, societal groups of this sort have always managed to communicate—whether it be via ships or landline telephones—but digital IT offers a number of opportunities: utilizing, as the chapters by Nordstrom and Deibert and Stein point out, an increasing range of communication options (from Internet cafes to satellite phones); exploiting the large amount of information on the World Wide Web to carry out operations (attacks or smuggling can be coordinated via published information about systems of transportation); reaching out to new recruits or passive supporters (providing financial or other aid) around the world who might otherwise be difficult to contact; pursuing a form of "public relations" through websites that make an online case for a cause on one side of a violent conflict. While much attention is now given to international threats, such as Al Qaeda, any given society may, as the chapters by Nordstrom and Rohozinksi demonstrate, contain individuals or domestic groups dedicated to violence or crime that can exploit IT against their own social institutions and population.

At the same time, it is important not to overemphasize threats as the only form of IT use relevant to security. As opposed to applications that produce threats, there are also applications that are associated with the reduction of violence and the possibility of greater peace. Relevant are the exchanges online (sometimes in chat rooms) between individuals from across lines of conflict, which might otherwise never take place (see the Kadende-Kaiser chapter on Burundi). Also relevant are the attempts of activist organizations and NGOs to bring to the fore questions about the human dimensions of conflicts such as the status of refugees or the basic human rights of women (see the Dartnell chapter on Afghanistan). Although many claims over the last decade have been made about the Internet as a force for peace and human development, the chapters by

Dartnell, Kadende-Kaiser, and Rohozinski show that there is no obvious or automatic relationship between IT, peace, and development,

A third way that society matters is as a realm of IT-related innovations that can be applied in the pursuit of security, especially by states and their militaries. Perhaps the most well known form of innovation is in the realm of organizational style and strategy. For over a decade, transnational corporations have been organizing themselves into multi-firm networks linking their production and marketing resources worldwide. IT has been central to these networks in that it allows firms to share up-to-the-minute information as well as knowledge about markets and production.[3] Such applications and innovations have inspired the U.S. military to attempt to organize itself into networks across and within various units (a part of what is called the Revolution in Military Affairs, discussed in the chapter by Gray). In such networks military resources, from individual soldiers and tanks to miniature surveillance robots, are linked, communicating and sharing access to data such as live action images of enemy positions. While such military networks can operate in large-scale wars, they also can be applied against threats from flexible, diffusely organized terrorist networks—striking anywhere, anytime (see the chapter by Deibert and Stein).

The application of IT-related innovations to security does not rest solely on borrowing organizational strategies from the private sector. It can also involve long-term partnerships between industry and the military. During the Cold War the U.S. government was the main force stimulating IT innovations. Sometimes the government directly undertook research and development (R & D), as in the case of the Internet (developed through the Defense Advanced Research Projects Agency [DARPA] and National Science Foundation);[4] other times it just sponsored R & D in corporations and universities, as in the case of the mainframe computer.[5] Over the last decade, the boom in private-sector IT development has shifted the balance of innovation closer to industry. This has opened up an opportunity for U.S. security agencies (from the military to intelligence) to exploit private-sector innovation, as well as continue to sponsor R & D itself. It has also led to new forms of public-private partnership reminiscent of the Cold War military-industrial complex, which allowed firms such as General Dynamics to cater to military-industrial needs for warplanes, tanks, and ships. The chapter by Lenoir documents how both the military and the entertainment industry are collaborating to generate innovations in one particularly interesting area: electronic simulations of battle—"wargames"—used by the military for training and strategic development and by the industry for the production of game products for mass entertainment. Intricate partnerships between the entertainment industry and the military in this area are developing rapidly and suggest that the

relationship between society, security, and IT will continue to evolve in unanticipated—and often disturbing—ways in the near future.

A fourth way that society matters is as a source of ethical and political considerations that raise questions about the purpose of security. To gain the hypothesized protections that greater surveillance affords—learning of planned crimes or terror attacks, for example—how much privacy are citizens willing to surrender? How closed are societies willing to be as they attempt to strengthen their borders to keep out groups and individuals viewed as potential threats? How much global spying are foreign states and societies willing to tolerate as they contemplate violations of their national sovereignty? The chapter by Rotenberg reviews what is at stake for privacy in the United States in recent changes in surveillance practices and regulations, as symbolized by the USA PATRIOT Act passed after 9/11. Libicki's chapter deals with the various logics and possibilities for tightening the U.S. border, especially through various forms of IT. And in her chapter, Landau provides an overview of the infrastructure and institutions, anchored in the United States, that are available to carry out surveillance on a global basis. All three chapters should prompt readers to weigh more accurately the balance between surveillance, human rights, and sovereignty.

WHOSE SECURITY?

The above discussion of the ways that society matters opens up two questions. One question is: what is the perspective from which we are making claims about security? Whose security is at stake (that of the U.S. state, that of an ethnic enclave's, or that of the worldwide community of states and societies)? And are we talking about policies (on the part of the U.S. military, the United Nations, or the European Union) or conditions of security (war, conflict, attack, threat, peace)? This volume starts from the assumption that the U.S. state is a central force in shaping global security, particularly as it relates to IT. And that the U.S. state pursues security not only to make itself as a state and its society secure, but also to make secure the entire international system, a system within which the United States has tremendous stakes as the largest economy and as the most powerful actor. The uses of IT by the United States to organize its globe-ranging military forces (see the chapter by Gray); to construct capacities for global surveillance (see Landau); and to strengthen national borders (see Libicki) are among the crucial factors that shape the overall structures of global security. The point is that while the United States is not the only state pursuing information-warfare capabilities (China and Russia are also doing so quite vigorously), the U.S. effort is likely to have the broadest effects by virtue of its global military system.

We can see U.S. policy and practice as one critical window into understanding

this important period of transformation in this area, but not only as it applies to the international realm. Policies bearing on the domestic realm are also relevant because the reach of IT-based domestic security policies extends beyond U.S. national territory. Homeland Defense is, as the chapter by Yould shows, at its core about the interaction of the international and domestic realms, driven by the fear that internationally networked threats are present and operating domestically. It also remains to be seen to what extent U.S. policies regarding IT are becoming models for the policies and practices of other states around the world.

This volume also assumes that policies and conditions of security are deeply intertwined, as the forces put in place by policy makers to achieve security (the deployment of mobile, electronically networked military units, for example) help determine the conditions of security, contributing to the nature of war, threats, and even peace.

But no matter how important U.S. policy is to this area, it is not the only factor shaping conditions of security. The actions and policies of groups outside the United States are also important: whether that means the policies of developing world states, the pursuits of NGOs (see Dartnell) or the actions of ethnic groups in local conflicts (see Kadende-Kaiser and Rohozinski). And when it comes to considering who or what is to be made secure, the focus should be not only on the United States but on all the countries and communities around the world. Thus, we use the term "global security" to refer not just to the global structures of security and the national policies that bear on them. We also use the term to refer to the many contexts (local, national, or regional) around the world where security is a major issue due to war and long-standing conflict.

IS SECURITY CHANGING?

The second question suggested by the discussion on why society matters is whether and how security is changing. As implied in the above discussion, there is nothing new per se about the protection of society, socially generated threats, private and public technological innovation, or ethical implications to security policies. These factors obviously take a different form in the twenty-first century, as indicated by the chapters in this volume that discuss new policies, new practices, and even new types of threats. The question is, do these changes and their twenty-first-century context point to any overall transformation in security?

This question offers no easy answer and requires a more lengthy consideration. Security has—at least since the beginning of World War II—been a complex affair, pursued across three basic dimensions: physical space (territory, atmo-

sphere, ocean), infrastructure (networks and systems that determine how societies are organized), and ideas (norms and perceptions that shape social action). If security is transforming, then we would expect to see changes in the way states and societies are organized to achieve security through space, infrastructure, and ideas.

PHYSICAL SPACE

The dimension we most closely associate with security is physical space: that is, land, sea, and atmosphere. Physical space is generally organized into territory. Territory is an expanse of land (or geographical area)—and often the abutting waters—that is under the jurisdiction of a political power. Today the political power of relevance is the state. Throughout history, armies have been deployed across territories and bodies of water—whether they were provinces, kingdoms, countries, or whole empires—in order to defend their own land or lay claim to other lands (in the name of security or national aggrandizement). Territory remains important to security because people, places (such as cities), and resources (such as oil, factories, or even computer networks) exist in physical space. As societies are organized today, cyberspace and cyber threats ultimately matter because they have implications for life that occurs in physical space. A cyberattack on a computerized electrical system matters in security terms because it may disrupt life in a city by threatening social order, economic life, or basic human services.

Land is not the only real, spatial dimension relevant to security: atmosphere is as well. Sovereign control over territorial airspace goes along with the control of territory and is sanctioned by international law. The stakes of control are significant. Ever since World War II the dominance and use of airspace has been critical to military conflict. (The recent armed interventions in Bosnia, the Persian Gulf, and Afghanistan reinforced the importance of control of the air, as large-scale air campaigns were central to the Allied effort.) In addition, the capacity of radio and television broadcasters to send signals into a territory across its airspace limits the state's control of the information circulating in its society.

But the airspace abutting territory is not the only aspect of the atmosphere that is relevant: "outer space," lying at and beyond the boundary of the atmosphere is important as well. This is where satellites circle in orbits above the earth, outside its atmosphere, receiving and sending signals (data, pictures, voice) for telephone systems and data networks around the world. Outer space has had an important place in security affairs ever since the first satellites began to be launched in the late 1950s and early 1960s. Developed countries' militaries—

especially that of the United States—use satellites for their own communications and to spy via long-range cameras and listening mechanisms (see the overview provided by Landau).

Similarly, the sea is a space that has always had a close connection to security. Like the atmosphere, it can be separated into its territorial form (i.e., the waters that lie within twelve miles of national territory, to which states can lay sovereign claim) and its nonterritorial form, the oceans and seas beyond the twelve-mile territorial water limits that are a sort of global commons. Oceans allow vessels to move about and deploy themselves in faraway places. They thus represent a space from which threats can emerge as forces, large and small (e.g., terrorists), might use waterways to attack or infiltrate a society. It is also the space from which cyber-threats are likely to emerge because submarine cables are a major conduit not just of telephone traffic but of Internet traffic. Access to the depths of the oceans to disrupt cables or tap them for surveillance purposes—something the United States has more or less monopolized—will remain crucial to security for years to come.

As long as humans remain corporeal beings, spatially based transformations in security—whether IT-related or not—will be of great importance. We are deeply anchored in space, and physical threats to our bodies, homes, communities, and "nations" understandably continue to preoccupy us. Perhaps the best-known hypothesis about a transformation under way suggests that—at least for the most developed societies—the capture of territory is no longer a motive for war, since today, wealth increasingly depends on knowledge-based businesses (from software development and data management to high finance) rather than land-based agriculture or heavy industry (such as steel production).[6] The growing prevalence of information networks (such as the Internet) as a means to conduct business only reinforces that view, as transactions occur on computer screens and data are transmitted in cyberspace.

Whether or not land as a reason to go to war is less relevant, states—even in the developed world—are still organized to fight wars across territory and to seize and hold it if necessary (if not in the name of permanent gain—such as a colony—then in the name of less permanent security—such as a temporary occupation or no-fly zone). We also cannot discount the prospect that states may be willing to go to war to defend global or national infrastructure (that is not simply cyber-attacked but physically attacked). On one level the current U.S. military intervention in Afghanistan is exactly this: a response to an attack on infrastructure of government, finance, and aviation.

Since militaries have not shifted significantly away from territory-based war yet, looking for space-related transformations by focusing on war motives may

miss some important changes afoot in how states and societies—especially the United States—are organized for security. In particular, it would miss transformations associated with the way that states pursuing security perceive and represent physical space through digital forms of IT.

In the past, physical space was known through physical survey (through scouts and surveyors) on the ground and later in the air, and as represented through drawn maps or photographs. The emergence of detailed scale-drawn maps was important to three major transformations bearing on security; they enabled a) political powers to fix sovereign borders and identify how they might be violated; b) military forces to move about and conduct battle in a more organized and precise way (also allowing for the identification of enemy forces); and c) explorers to chart voyages around the world and change the face of history through empire for the rest of the millennium. With the advent of the scale map, forces large and small, on land or sea, could be fielded and coordinated across time and space.

While two-dimensional scale maps are still in use, today there is a new form of

representation and knowledge about physical space that is emerging around IT. It is actively being pursued by the U.S. military as well as civilian organizations, ranging from high-tech land surveyors offering their services to businesses, such as surface mining firms, to environmental NGOs tracking the loss of forests and other natural habitats. This new form of representation is based on satellite imagery (high-resolution images of the earth's surface), a global satellite navigation system that allows those who access it to discern their exact position or the position of others being tracked (called the global positioning system or GPS); and on computer systems that put all geographical data together to produce in-depth digital maps of terrains and that can portray the life that exists on such terrains, such as cities and even specific buildings (called geographic information systems or GIS). In the military sphere three other elements can be added: a) the simulations (see Lenoir's chapter) mentioned above that create digital renditions of real spaces, based in part on GIS, within which actors or players can move about and make strategic choices; b) the correlation of intelligence data from global surveillance (see Landau's chapter) with GIS to produce socio-geographic portraits of places; and c) the formation of digital infospheres equipped with consoles, keyboards, and other interfaces in zones of conflict and military deployment (that is, "battlespaces") through an array of flying drones, satellites, and sensors, for use by combatants.

From a skeptical view, this emerging assemblage of digital mapping might be seen as simply providing a wider and more complete range of information, more easily organized and aggregated. Once the revolutionary transition to scale maps

occurred from the seventeenth century onward, everything else can be seen merely as improvements or embellishments.

But this view fails to consider the question of whether or not these new forms of information and representation of physical space, when taken together, constitute an emerging "global information grid" (GIG), and whether such a grid would transform the pursuit of security. A GIG is, essentially, the sum of information—digitally stored and distributed in pictures and text (words and numbers)—about targets, groups, locales, countries, regions, etc. It is produced and accessed by the actors most engaged in the pursuit of security (military and intelligence), who increasingly rely on it to identify, evaluate, and implement security policies and plans. The attempt to organize the global information grid into an integrated, accessible system of information is already under way (the phrase itself is a U.S. military term). And a few years ago the U.S. Defense Intelligence Agency recognized the value of joining security-relevant images, data, and analysis into a single, easily accessible intelligence information system that could facilitate collaboration—called the Joint Intelligence Virtual Architecture or JIVA—among security actors ranging from National Security Agency (NSA) analysts to military forces in the field.[7]

How might the emergence of a GIG as the twenty-first-century map of the world transform how states and societies—in this case the United States—organize for and pursue security? For centuries, the pursuit of security has been focused on threats to territory (and its human and material resources) or to things identified as vital interests in the international realm (such as important allies, oil fields, or communication lines). Two-dimensional scale maps have served well to delineate borders, mark where one's own and one's enemy's forces are located, and where such forces could maneuver vis-a-vis territory and interests. However, such maps are static (distinguishing between one country and another, enemy and foe). And they can impart only a limited amount of information, mostly in the form of geographical representation (terrains, distances, longitude and latitude). The most appropriate perspective for organizing for security on this basis is to focus on lines—at borders, on fronts between enemy forces, and as the best route between two points on land or at sea. Among the famous fronts in recent history was the one between Eastern and Western Europe during the Cold War. In contrast, the GIG is a dynamic information system that is constantly revising and adding new information based on perceived and recorded changes (whether these are enemy movements or new political conditions). Threats can emerge from anywhere, anytime, within the global grid,[8] which ultimately is composed of various "spaces" that are geographical (e.g., the Middle East or Latin America) and functional (battlespace, economic space, political space, and

outer space). In this case, the most appropriate perspective for organizing security is not lines in two dimensions but spaces in five dimensions (length, width, height, time, and data).

What this means in terms of the pursuit of security is that an increasing range of geographic and functional spaces within which people carry out their lives (such as cities, communities, and financial markets) can be subject to surveillance and possible intervention in order to identify, destabilize, or eradicate threats. Whereas total war drew the economic, social, ideological, and political dimensions of a nation into organizing for war, what can be labeled *total security* draws these dimensions, not simply on a national but a global scale, into a digital grid of omnipresent vigilance. The chapters by Landau, Libicki, Rotenberg, and Yould indicate that the division between internal national territory and external international realms is becoming increasingly blurred as total security is pursued across the international/domestic divide.[9] As mentioned above, a concept like "homeland" becomes fuzzy when threats, such as those coming from an organized crime network, can stretch across multiple borders and U.S. trade and investment are anchored in overlapping relations around the world.

No organizational form better expresses the changes associated with the rise of total security than networks (see the chapter by Deibert and Stein). The purview of total security favors a focus on networks as a threat and a mode of pursuing security, because networks are composed of nodes that can operate in a mobile fashion locally and across vast geographical expanses. Such nodes^for example, a terrorist cell in a wider terrorist network organization—can surface and disappear across various spaces, connecting to economic institutions such as banks (to move financial resources) or government organizations, such as intelligence agencies (to utilize expertise). Networks can emerge to fight in cities, jungles, or on mountaintops. As the U.S. military draws closer to this organizational form, U.S. society will have to ask whether there will be space for democratic evaluation of preemptive and reactive military actions in a world where total security actually requires a form of permanent engagement across the grid. Since total security can never actually be achieved but only sought, it will likely remain an ongoing project expanding and deepening its reach into various social spaces across the planet. (See the discussion of this in the chapter by Gray.)

Readers should note that the developments tied to total security—an increasingly global view and an emphasis on networks—were not caused by the emergence of the GIG. If we go back to the example of the scale map, it is obvious that the desire to field and coordinate large armies and colonize lands across large ocean expanses was not produced directly by maps per se. Maps, which developed over decades and centuries, opened up options and suggested the possibil-

ity of pursuing war and imperial expansion differently. And the investment in improving maps was sometimes driven by the desire of states to put them to use in war and conquest. Likewise, the GIG evolved as satellites, surveillance systems, intelligence databases, and military-information networks emerged across the post-World War II period. The United States' commitment to a global military system, its role as the ultimate guarantor of international security, and its planetary competition with the USSR were important incentives for putting in place the pieces (such as satellite networks) that ultimately led to the GIG. As the pieces of the GIG fell into place over the decades, it opened up the possibility for pursuing total security.

This back and forth between the means of security (GIG) and the organizational approaches to security (total security) is likely to continue into the future as there emerge new IT applications, new security doctrines, and new understandings of threat. An increasing reliance on a GIG for pursuing security should have two main consequences: One is that global security becomes even more dependent than in the past on assumptions about how security works (such as who and what is a potential threat, what is a relevant piece of intelligence, how elements of the grid connect), which are built into the GIG. To make the grid, hundreds of thousands of big and small choices have to be made about constructing databases and what counts as information, where to place or aim sensors, and which models to employ for analyzing information in real time. Will small choices lead to mistakes, big and small, ranging from a wrong bombing target—such as the Chinese embassy in Belgrade during the Kosovo campaign—to misinterpreted communications that fail to uncover potentially lethal attacks? In the context of large-scale war, will small missteps cause catastrophe?

In her chapter, Landau points to the difficulties intelligence systems have in piecing together data that signal threats. She indicates that this was a large part of the problem with anticipating the Pearl Harbor and 9/11 attacks. This type of difficulty is yet another aspect of the problem of choice in constructing and maintaining the grid: either a computer program has to be in place to anticipate potentially meaningful threat-relevant combinations of data, or intelligence analysts have to know when to rely on their own judgment and analysis to figure out such combinations. In the case of the computer program it is hardly clear that those responsible for creating the program can anticipate all the possible combinations and what they imply. In the case of human intelligence analysis, there is the problem of how to determine when developments and potential combinations warrant close human inspection and analysis. That determination itself requires effective software to signal that attention is required. Considering that there is an incredible amount of communication traffic across the air and wires

and millions of square miles to survey and keep track of, this is a great deal to ask of any program.

That is exactly the dilemma total security poses: you dig deeper and deeper to find more data to confront potential threats and perhaps overcome shortfalls in analysis, but that creates even more need for analytical tools that can sift effectively through even more data.

Whether or not such a cycle emerges, a growing reliance on the global information grid has a second consequence: the rise of the GIG as a new realm of vulnerability. That is, the GIG itself is understood to be a resource that needs to be secured against threats to it—cyber intrusion (hacking) and physical disruption such as sabotage of cables or satellites. Recognizing the GIG as the new nervous system of the global military network, the U.S. military has leaked information about secret exercises undertaken to verify the extent of vulnerability and has taken steps to decrease it.[10] Whether or not these exercises were productive, the very attempt to achieve greater security for the GIG has two implications. It further deepens the grid as greater amounts of information about potential cyber-threats around the world are sought after. But the attempt to anticipate attack—and to know potential attackers—assumes that the nature of attacks, as well as the identities of those who might undertake them, can be anticipated. But that is unreasonable, given what was just claimed about how the operation of the grid is only as good as the myriad choices composing it. A second implication is that organizing to secure the grid might produce new vulnerabilities in that efforts to centralize data in protected digital vaults conveniently gather together valuable information for intruders to access.[11] The chapters by Bendrath, Denning, and Yould probe these and other implications of securing grid-related infrastructure.

INFRASTRUCTURE

Infrastructure has been central to security since the beginning of organized war. Transport, communications, and fortification have been among the infrastructures of key concern to military leaderships even before the time of the Roman Empire. The pursuit of total war in the twentieth century carried the mobilization of infrastructure (especially civil infrastructure) to an extreme, as trains, factories, schools, hospitals, and media were dedicated to supporting military mobilization.

Since infrastructures are so valuable to war-making and, more generally, to the well-being of a society, direct attacks on enemy infrastructures became an important aspect of strategy. Such attacks are not a new development. During the U.S. Civil War telegraph lines were cut to sabotage communications. But with

the Second World War the waging of war against infrastructure came into its own as extensive aerial bombing campaigns could target bridges, railroads, factories, and government offices.

For forty years after the Second World War, it was taken as a core assumption of U.S. policy makers and the informed public that weapons of mass destruction "not only can nullify any nation's military effort, but can also demolish its economic and social structures and prevent their reestablishment for long periods of time."[12] Yet, just over a decade after the end of the Cold War, most policy makers and the public seemed to be taken by surprise when on September 11 a structure as basic as the aviation system could be not only shut down (temporarily) but also transformed into a destructive weapon itself. The pervasiveness and importance of infrastructures within a social system mean the stakes of their fate are high. (Not only do so many activities depend on such structures but, when weaponized, their prevalence puts large numbers of people at risk.)

Today IT has a privileged place regarding infrastructure. According to the U.S. Critical Infrastructures Assurance Office, developed countries have "become dependent upon computer networks for many essential services" including "water, electricity, gas, voice and data communications, rail and aviation."[13] In this respect, IT is not like other technological developments (such as materials or standards) because it is applied directly as an infrastructure in its own right (i.e., the Internet) and is central to the governance of infrastructure systems (from electric power to finance). In effect, IT becomes the brains and nervous system of the infrastructure overall and thus the "infrastructure of the infrastructure" or what we can call a "core infrastructure."

Infrastructures, and especially core infrastructures, are supposed to be metaphorically invisible. Working beneath (hence, "infra"), smoothly, the quotidian activities of societies. Even so visible an infrastructure as a highway is operational to the extent that it is taken for granted, assumed, unproblematic. On September 11, the aviation infrastructure rose to the surface as visibly problematic. Making the infrastructure operational again is not merely a matter of starting it up again. The problem—insecurity due to terrorism—requires that the infrastructure be redesigned. But what principles, theories, goals, norms, and precedents do we possess to guide such redesign? What knowledge is available, and how have we thought about the relationship between infrastructure and security? The issues of civil liberties discussed by Rotenberg show that we have no clear road map for navigating between rights and security in relation to infrastructure.

What sort of transformation in the way societies are organized for security can we detect in the infrastructure dimension? The range of movement and com-

munications now subject to scrutiny inside and across national boundaries a) bear on an increasing array of infrastructures from roads and airports to media systems; and b) expand the scope of the global information grid discussed above. Moreover, new sorts of infrastructures of surveillance are being put in place for security purposes, relying especially on biometric technologies (from face recognition and iris scanning to hand geometry and brain fingerprinting). These changes will probably reshape the character of social life in the United States and elsewhere around the world, especially as new infrastructures change daily interactions in buildings, on sidewalks, and across the information highway. Outside of what fiction such as 7984 suggests to us, we really have little idea of what that might mean for how security is pursued and the relationship between states and their societies.[14]

The ultimate direction of this transformation will depend on the mix of values attached to infrastructures. Infrastructure has typically been thought of in regard to its economic value, and there is thus a good deal of knowledge in this area. Roads and electricity facilitate national markets and mechanized industry. Even Cold War concern with infrastructure was often treated as a matter—indicated by the quote above—of either protecting "economic and social structures" or attacking those of the enemy. Despite the dominance of economic value in thinking about infrastructure, it has in practice often been double coded—according to both economic and security values. Cities and towns have historically been the most pointed sites for the intersection of infrastructure, security, and economy Premodern cities and towns were double coded, as castles and city walls did double duty as a means of defense and economic control (policing markets, for example). The way this double coding occurred in modern cities was through the internal organization of cities, especially in transportation systems. Baron Haussmann's redesign of Paris into broad boulevards not only allowed easy access for security forces to suppress popular uprisings (along spokelike roads not easily defended by such populations) but also allowed for smoother economic transactions across the city.

The same sort of duality was also played out in state-formation processes, as railroads, roads, and telegraphs extended military and administrative reach across wide swaths of territory, and at the same time made national economic life a possibility.[15]

In more recent history, the U.S. highway program associated with President Eisenhower ("National System of Interstate and Defense Highways") followed the same dualist strategy (highways to move men and weapons and emergency forces as well as to undergird the trucking and the automotive economy). The highway system furthered the dynamics of this duality, as roadways helped sub-

urbs emerge, which in turn built infrastructures of local security in closed communities (via restricted-access roads and systems of surveillance and the policing of movement). The same suburbs were expected to be the only survivors in the event of nuclear war (unlike the cities).

Sometimes infrastructure is valued differently in different periods. A pointed example is the wartime economy when what had been exclusively economic-directed infrastructures (electricity and railroads) were redesigned for the needs of war-making. During World War I, for example, the U.S. state prompted the interconnection of previously disparate electric utilities, which opened up a post-war option of power sharing (the war also led to the design of the mega-power plant in both the United States and Germany).

The point is that IT-based infrastructures have been deeply double coded. The computer was developed as a crucial tool for security infrastructure (especially air-intrusion detection systems such as the U.S. Air Force's system called the Semi-Automatic Ground Environment or SAGE). The Internet was hatched out of the Department of Defense and often associated with logics of security (the survivability of communication systems).

Nonetheless, the Internet has been commercialized rather rapidly in fundamental ways, from software applications and online commerce to the very provision of the backbone that makes the Internet possible—upon which even the U.S. military relies for its communications. But looking back on the 1990s, we might well detect a whiff of naivete in our assumptions of an open and exclusively market-driven Internet. While the Internet per se moved out of the Department of Defense's hands into the private and public sectors, this does not mean U.S. security agencies stepped out of the internetworking business. After all, there is the development of the global information grid, which commenced prior to 9/11, and which has only intensified after 9/11 through the infrastructure transformations described above. The question is how the security values of the grid will interact with values associated with other systems in place or being put in place around the world. Will economic and social development agendas be overtaken by security agendas as networks are established or expanded, a process that, according to Rohozinski, is already under way?

IDEAS

Whether or not the realm of ideas has been as central as physical space and infrastructure, it has to be counted as a basic dimension of security. Bendrath's chapter shows that at the most fundamental level, perceptions of security and insecurity rest on beliefs among elites, average citizens, and military forces about what a threat is and what one's vulnerabilities to threats are. Perceptions are also

shaped by theories about how to respond to threats and vulnerabilities. One such theory held by U.S. policy makers is that the vulnerabilities exposed by 9/11 require in response a War Against Terrorism and a Homeland Defense.

War and conflict have for a long time been tied up with ideas. Citizens are mobilized to fight in the name of ideals such as freedom, the homeland, or the nation. Recognizing the importance of ideals, warring states in the twentieth century have often launched considerable propaganda campaigns to demoralize their enemies. In World War I the Allies concentrated their effort on the German army to create—through media such as pamphlets and flyers—a sense that continued fighting was hopeless. Belligerents in World War II took advantage of mass media (radio and film) to attack the will of citizens on the home front to go on supporting the war. It should also be recalled that global Cold War conflict was not just a competition between two superstates but a contest between those who sought to organize societies along either socialist or capitalist lines. In the 1990s that contest faded as conflicts mobilizing beliefs about ethnic identity as a basis for violence came to the fore.

These examples indicate that the modern state, which is the primary organizational form responsible for security and order, has had a long history of undertaking ideational campaigns. The U.S. state began such a campaign as early as 1802, when it sent agents among the Native Americans to teach "the Arts of husbandry, and domestic manufactures, as a means of producing, and diffusing, the blessings attached to a well regulated civil society."[16] Programs to pacify populations by convincing them of the advantages of American life were applied not just within U.S. territory but also without it, notably in the Philippines around 1900.

With the Cold War, a whole complex of programs was initiated in the "psychological warfare" category, as misinformation and misperception were deliberately sown to confuse enemies and create conditions of disorder. During the very early stages of U.S. intervention in Vietnam, for example, CIA operatives spread leaflets around Hanoi scaring targeted groups into migrating southward in order to foster chaotic conditions that would slow down enemy force movements.

Besides these more clandestine ideational programs, the United States invested heavily in bringing the opinion of foreign publics in Europe and the developing world toward a pro-United States and anti-Soviet stance. Programs relied on publications, films, radio, and, most important, partnerships with and sponsorships of foreign media. Most famous of all is the Voice of America, which broadcast radio programs featuring aspects of American life. In the 1980s the National Endowment for Democracy became very active promoting American-style democracy.

States have targeted their own citizens for various forms of "education" and "public relations." In the name of civil defense and loyalty at home, hundreds of millions of pamphlets, bulletins, posters, films, and training manuals were produced by U.S. security agencies to show how nuclear attack could be a survivable event.[17] In the name of domestic support for foreign policy, the U.S. state has not only produced its own media materials, but much more importantly it has sought to generate backing for its policies through the information disseminated by mass media (especially television and newspapers). Strategies changed across the years. During the Vietnam War, journalists were given relatively free access to the battlefield in order to create sympathy for U.S. GIs. The failure of this approach—as horrific war footage flooded nightly news programs—was not lost on public-affairs strategists planning for the first Gulf War, who sought tight control over information and access, containing journalists in "News Media Pools."

It should not be surprising that the advances in IT of the past decade prompted U.S. policy makers and observers to identify the potential for a new era in diplomatic communication based on "public diplomacy."[18] In such an era, satellites can more easily distribute news-style programs and documentaries explaining UN-sanctioned interventions directly to people's satellite dishes in the developing world, and the NATO website can present a case for NATO expansion. However, against the historical background, the relatively recent surge of U.S. interest in public diplomacy should be seen as only the latest in a long line of commitments to ideational strategies. The application of new technologies in themselves do not constitute a transformation of the ways states and societies are organized to pursue security. Rather, it confirms the longer-term trend in state-sponsored publicity.

To find significant transformation, we have to look beyond the state itself to the realm of nonstate actors and groups, populated by corporations, local communities, ethnic groups, diasporas, militias, grassroots activists, and NGOs. Of course, states never exercised a monopoly over international communications—international wire services such as Reuters have been in operation since the nineteenth century. And rarely have states in the capitalist world controlled all communications inside their own borders (authoritarian states have typically had to face the presses and pamphlets of groups, operating inside and outside national borders, who oppose their rule). What is changing is that the communication activities of civil society groups—from independent community radio programming to website development—are changing the information environment within which states operate. It is simply far more diverse.

In this new environment, states have to compete to get their own messages

across. Perhaps the most noted point of competition to US, public diplomacy has been the privately owned Al-Jazeera TV satellite-based network operating in the Middle East, which has broadcast anti-United States programming and pictures of Iraqi civilian casualties in the second Gulf War. Even a Western-based global network like CNN can undermine state public relations, as the United States learned when pictures of a U.S. soldier being dragged through the streets in Somalia created a general perception that the UN intervention in that country was a failure. But one need not go to as grand a scale as a regional or global network. On a far more modest scale are the independent, community-based radio stations in the developing world that provide news written from the perspective of people in those communities rather than editors in Washington, New York, London, or Paris,

To grasp the transformation under way, one has to shift the focus of security from states to societies. That is, civil society groups are able to pursue their own security in new ways. Sometimes that means drawing in international support to their cause through global networking on the Internet via websites and e-mail communication.[19] Other times it means influencing world opinion about a situation such as a conflict by providing information about it that would otherwise not be available. Of course, groups have always tried to build international networks of support around causes and to inform world opinion using letters, pamphlets, and posters. What is different about today is the depth and breadth of information a group can provide in real time, including pictures, histories, facts, data, and commentary. Dartnell's chapter looks at one group, the Revolutionary Association of the Women of Afghanistan (RAWA). Their website allowed them to leapfrog the poor communication capabilities of communities in Afghanistan to reach the world with a powerful array of information about the plight of women in that country. Their effectiveness was not just a function of providing more information. Rather, they also were able to quickly communicate their views on new developments and events to counter the positioning of the Taliban.

Another way that security can be pursued by nonstate groups is to use communications to help avoid the further deepening of conflicts and exchange strategies for the resolution of violent conflicts. Kadende-Kaiser's chapter on Burundi shows how well-designed and carefully managed electronic bulletin boards and discussion groups on the Internet can become "coffeehouses'* or "meeting places" for individuals to exchange ideas across different sides of a conflict. In such relatively anonymous spaces she finds that individuals are more likely to speak their minds and propose strategies for moving forward positively toward peace. While the Internet may be accessible to only a tiny percentage of

Burundians—especially those living outside the country in the diaspora—Kadende-Kaiser underscores how important it is to have a space to devise strategies for conflict resolution, especially when that space is likely to be populated by young elites and future leaders.

As Rohozinski shows, interaction on the Internet more often than not can deepen divisions between sides of a conflict. It can be used to strengthen support for a belligerent side in a conflict and increase animosity between groups. Even a quick survey of websites of groups involved in violent conflicts, from Palestine (www.hizbollah.org) and Sri Lanka (www.eelam.com) to Colombia (www.farc.org), makes this obvious. Many of these sites are for the benefit of diaspora populations. Diasporas can be critical to the life of a conflict because they can provide financial resources to belligerents, lobby political leaders in the West, and take hard-line positions. This is why it is crucial to pay attention to the developments traced by Kadende-Kaiser that point toward the peace-generating endeavors of diasporas.

Those observers looking for overall trends in the relationship between IT, security, and the realm of ideas are likely to be disappointed. A communication system like the Internet is not a tool for peace or war in itself: it depends on the uses to which it is put by various groups that employ it. The transformation under way in the number and type of groups employing IT directly to disseminate information and facilitate worldwide communication implies that those uses will be diverse and often contradictory.

CONCLUSION

At its broadest, the relationship between IT and security discussed in this volume is shaped by a tension between two worlds. One world is organized as an "order of universal security," where the social life of the planet is made legible in state-sanctioned bodies and flows of information. On the one hand, this order facilitates communication within and across the states and societies participating in the various realms of modern capitalism, from trade and international law to global cultural exchange. On the other hand, it requires the policing of borders, the anticipation of new vulnerabilities, the identification of forces of disruption, and the thwarting of threats.

A second world is composed of innumerable social, economic, and political networks—global in reach—that seek to operate, hidden and illegibly, outside the purview of governments and global surveillance efforts. These networks are hardly homogeneous. They include the illicit business and crime networks discussed below by Nordstrom; the terrorist networks discussed by Deibert and

Stein; the hacker networks discussed by Denning; and the conflict networks discussed by Rohozinski.

The boundaries between these two worlds are murky, and we should not assume that only criminals and the mischievous populate the illegible one. We might easily include clandestine efforts of the U.S. security and intelligence agencies to police borders and threats as part of the second, illegible world. Likewise, we might count the billions of communications between individuals who treasure privacy and assume their interactions are lost in the ether. As Rotenberg implies in his chapter, important political questions about the nature of privacy, open societies, and transparent government lie ahead. The ways that society matters to IT and security will continue to evolve. This volume seeks to show that the relationship between IT and security will be shaped not only by transformations in how societies organize to pursue security, but more fundamentally by how societies try to answer these questions in law and in practice.