

## THE RISE OF COMPLEX TERRORISM

*Foreign Policy*

January/February 2002

By Thomas Homer-Dixon

*Modern societies face a cruel paradox: Fast-paced technological and economic innovations may deliver unrivalled prosperity, but they also render rich nations vulnerable to crippling, unanticipated attacks. By relying on intricate networks and concentrating vital assets in small geographic clusters, advanced Western nations only amplify the destructive power of terrorists and the psychological and financial damage they can inflict.*

It's 4 a.m. on a sweltering summer night in July 2003. Across much of the United States, power plants are working full tilt to generate electricity for millions of air conditioners that are keeping a ferocious heat wave at bay. The electricity grid in California has repeatedly buckled under the strain, with rotating blackouts from San Diego to Santa Rosa.

In different parts of the state, half a dozen small groups of men and women gather. Each travels in a rented minivan to its prearranged destination—for some, a location outside one of the hundreds of electrical substations dotting the state; for others, a spot upwind from key, high-voltage transmission lines. The groups unload their equipment from the vans. Those outside the substations put together simple mortars made from materials bought at local hardware stores, while those near the transmission lines use helium to inflate weather balloons with long silvery tails. At a precisely coordinated moment, the homemade mortars are fired, sending showers of aluminum chaff over the substations. The balloons are released and drift into the transmission lines.

Simultaneously, other groups are doing the same thing along the Eastern Seaboard and in the South and Southwest. A national electrical system already under immense strain is massively short-circuited, causing a cascade of power failures across the country. Traffic lights shut off. Water and sewage systems are disabled. Communications systems break down. The financial system and national economy come screeching to a halt.

Sound far-fetched? Perhaps it would have before

September 11, 2001, but certainly not now. We've realized, belatedly, that our societies are wide-open targets for terrorists. We're easy prey because of two key trends: First, the growing technological capacity of small groups and individuals to destroy things and people; and, second, the increasing vulnerability of our economic and technological systems to carefully aimed attacks. While commentators have devoted considerable ink and airtime to the first of these trends, they've paid far less attention to the second, and they've virtually ignored their combined effect. Together, these two trends facilitate a new and sinister kind of mass violence—a "complex terrorism" that threatens modern, high-tech societies in the world's most developed nations.

Our fevered, Hollywood-conditioned imaginations encourage us to focus on the sensational possibility of nuclear or biological attacks—attacks that might kill tens of thousands of people in a single strike. These threats certainly deserve attention, but not to the neglect of the likelier and ultimately deadlier disruptions that could result from the clever exploitation by terrorists of our societies' new and growing complexities.

### Weapons of Mass Disruption

The steady increase in the destructive capacity of small groups and individuals is driven largely by three technological advances: more powerful weapons, the dramatic progress in communications and information processing, and more abundant opportunities to divert non-weapon technologies to destructive ends.

Consider first the advances in weapons technology. Over the last century, progress in materials engineering, the chemistry of explosives, and miniaturization of electronics has brought steady improvement in all key weapons characteristics, including accuracy, destructive power, range, portability, ruggedness, ease-of-use, and affordability. Improvements in light weapons are particularly relevant to trends in terrorism and violence by small groups, where the devices of choice include rocket-propelled grenade launchers, machine guns, light mortars, land mines, and cheap assault rifles such as the famed AK-47. The effects of improvements in these weapons are particularly noticeable in developing countries. A few decades ago, a small band of terrorists or insurgents attacking a rural village might have used bolt-action rifles, which take precious time to reload.

Today, cheap assault rifles multiply the possible casualties resulting from such an attack. As technological change makes it easier to kill, societies are more likely to become locked into perpetual cycles of attack and counterattack that render any normal trajectory of political and economic development impossible.

Meanwhile, new communications technologies—from satellite phones to the Internet—allow violent groups to marshal resources and coordinate activities around the planet. Transnational terrorist organizations can use the Internet to share information on weapons and recruiting tactics, arrange surreptitious fund transfers across borders, and plan attacks. These new technologies can also dramatically enhance the reach and power of age-old procedures. Take the ancient hawala system of moving money between countries, widely used in Middle Eastern and Asian societies. The system, which relies on brokers linked together by clan-based networks of trust, has become faster and more effective through the use of the Internet.

Information-processing technologies have also boosted the power of terrorists by allowing them to hide or encrypt their messages. The power of a modern laptop computer today is comparable to the computational power available in the entire U.S. Defense Department in the mid-1960s. Terrorists can use this power to run widely available state-of-the-art encryption software. Sometimes less advanced computer technologies are just as effective. For instance, individuals can use a method called steganography ("hidden writing") to embed messages into digital photographs or music clips. Posted on publicly available Web sites, the photos or clips are downloaded by collaborators as necessary. (This technique was reportedly used by recently arrested terrorists when they planned to blow up the U.S. Embassy in Paris.) At latest count, 140 easy-to-use steganography tools were available on the Internet. Many other off-the-shelf technologies—such as "spread-spectrum" radios that randomly switch their broadcasting and receiving signals—allow terrorists to obscure their messages and make themselves invisible.

The Web also provides access to critical information. The September 11 terrorists could have found there all the details they needed about the floor plans and design characteristics of the World Trade Center and about how demolition experts use progressive collapse to destroy large buildings. The Web also makes available sets of instructions—or "technical ingenuity"—needed to combine readily available materials in destructive ways. Practically anything an extremist wants to know about kidnapping, bomb making, and assassination is now available online. One somewhat

facetious example: It's possible to convert everyday materials into potentially destructive devices like the "potato cannon." With a barrel and combustion chamber fashioned from common plastic pipe, and with propane as an explosive propellant, a well-made cannon can hurl a homely spud hundreds of meters—or throw chaff onto electrical substations. A quick search of the Web reveals dozens of sites giving instructions on how to make one.

Finally, modern, high-tech societies are filled with supercharged devices packed with energy, combustibles, and poisons, giving terrorists ample opportunities to divert such non-weapon technologies to destructive ends. To cause horrendous damage, all terrorists must do is figure out how to release this power and let it run wild or, as they did on September 11, take control of this power and retarget it. Indeed, the assaults on New York City and the Pentagon were not low-tech affairs, as is often argued. True, the terrorists used simple box cutters to hijack the planes, but the box cutters were no more than the "keys" that allowed the terrorists to convert a high-tech means of transport into a high-tech weapon of mass destruction. Once the hijackers had used these keys to access and turn on their weapon, they were able to deliver a kiloton of explosive power into the World Trade Center with deadly accuracy.

### **High-Tech Hubris**

The vulnerability of advanced nations stems not only from the greater destructive capacities of terrorists, but also from the increased vulnerability of the West's economic and technological systems. This additional vulnerability is the product of two key social and technological developments: first, the growing complexity and interconnectedness of our modern societies; and second, the increasing geographic concentration of wealth, human capital, knowledge, and communication links.

Consider the first of these developments. All human societies encompass a multitude of economic and technological systems. We can think of these systems as networks—that is, as sets of nodes and links among those nodes. The U.S. economy consists of numerous nodes, including corporations, factories, and urban centers; it also consists of links among these nodes, such as highways, rail lines, electrical grids, and fiber-optic cables. As societies modernize and become richer, their networks become more complex and interconnected. The number of nodes increases, as does the density of links among the nodes and the speed at

which materials, energy, and information are pushed along these links. Moreover, the nodes themselves become more complex as the people who create, operate, and manage them strive for better performance. (For instance, a manufacturing company might improve efficiency by adopting more intricate inventory-control methods.)

Complex and interconnected networks sometimes have features that make their behavior unstable and unpredictable. In particular, they can have feedback loops that produce vicious cycles. A good example is a stock market crash, in which selling drives down prices, which begets more selling. Networks can also be tightly coupled, which means that links among the nodes are short, therefore making it more likely that problems with one node will spread to others. When drivers tailgate at high speeds on freeways, they create a tightly coupled system: A mistake by one driver, or a sudden shock coming from outside the system, such as a deer running across the road, can cause a chain reaction of cars piling onto each other. We've seen such knock-on effects in the U.S. electrical, telephone, and air traffic systems, when a failure in one part of the network has sometimes produced a cascade of failures across the country. Finally, in part because of feedbacks and tight coupling, networks often exhibit nonlinear behavior, meaning that a small shock or perturbation to the network produces a disproportionately large disruption.

Terrorists and other malicious individuals can magnify their own disruptive power by exploiting these features of complex and interconnected networks. Consider the archetypal lone, nerdy high-school kid hacking away at his computer in his parents' basement who can create a computer virus that produces chaos in global communications and data systems. But there's much more to worry about than just the proliferation of computer viruses. A special investigative commission set up in 1997 by then U.S. President Bill Clinton reported that "growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage." The commission continued: "We are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs [of launching an attack] continue to drop."

Terrorists must be clever to exploit these weaknesses. They must attack the right nodes in the right networks. If they don't, the damage will remain isolated and the overall network will be resilient. Much depends upon the network's level of redundancy—that is, on the

degree to which the damaged node's functions can be offloaded to undamaged nodes. As terrorists come to recognize the importance of redundancy, their ability to disable complex networks will improve. Langdon Winner, a theorist of politics and technology, provides the first rule of modern terrorism: "Find the critical but nonredundant parts of the system and sabotage ... them according to your purposes." Winner concludes that "the science of complexity awaits a Machiavelli or Clausewitz to make the full range of possibilities clear."

The range of possible terrorist attacks has expanded due to a second source of organizational vulnerability in modern economies—the rising concentration of high-value assets in geographically small locations. Advanced societies concentrate valuable things and people in order to achieve economies of scale. Companies in capital-intensive industries can usually reduce the per-unit cost of their goods by building larger production facilities. Moreover, placing expensive equipment and highly skilled people in a single location provides easier access, more efficiencies, and synergies that constitute an important source of wealth. That is why we build places like the World Trade Center.

In so doing, however, we also create extraordinarily attractive targets for terrorists, who realize they can cause a huge amount of damage in a single strike. On September 11, a building complex that took seven years to construct collapsed in 90 minutes, obliterating 10 million square feet of office space and exacting at least \$30 billion in direct costs. A major telephone switching office was destroyed, another heavily damaged, and important cellular antennas on top of the towers were lost. Key transit lines through southern Manhattan were buried under rubble. Ironically, even a secret office of the U.S. Central Intelligence Agency was destroyed in the attack, temporarily disrupting normal intelligence operations.

Yet despite the horrific damage to the area's infrastructure and New York City's economy, the attack did not cause catastrophic failures in U.S. financial, economic, or communications networks. As it turned out, the World Trade Center was not a critical, nonredundant node. At least it wasn't critical in the way most people (including, probably, the terrorists) would have thought. Many of the financial firms in the destroyed buildings had made contingency plans for disaster by setting up alternate facilities for data, information, and computer equipment in remote locations. Though the NASDAQ headquarters was demolished, for instance, the exchange's data centers in Connecticut and Maryland remained linked to trading companies

through two separate connections that passed through 20 switching centers. NASDAQ officials later claimed that their system was so robust that they could have restarted trading only a few hours after the attack. Some World Trade Center firms had made advanced arrangements with companies specializing in providing emergency relocation facilities in New Jersey and elsewhere. Because of all this proactive planning—and the network redundancy it produced—the September 11 attacks caused remarkably little direct disruption to the U.S. financial system (despite the unprecedented closure of the stock market for several days).

But when we look back years from now, we may recognize that the attacks had a critical effect on another kind of network that we've created among ourselves: a tightly coupled, very unstable, and highly nonlinear psychological network. We're all nodes in this particular network, and the links among us consist of Internet connections, satellite signals, fiber-optic cables, talk radio, and 24-hour television news. In the minutes following the attack, coverage of the story flashed across this network. People then stayed in front of their televisions for hours on end; they viewed and reviewed the awful video clips on the CNN Web site; they plugged phone lines checking on friends and relatives; and they sent each other millions upon millions of e-mail messages—so many, in fact, that the Internet was noticeably slower for days afterwards.

Along these links, from TV and radio stations to their audiences, and especially from person to person through the Internet, flowed raw emotion: grief, anger, horror, disbelief, fear, and hatred. It was as if we'd all been wired into one immense, convulsing, and reverberating neural network. Indeed, the biggest impact of the September 11 attacks wasn't the direct disruption of financial, economic, communications, or transportation networks—physical stuff, all. Rather, by working through the network we've created within and among our heads, the attacks had their biggest impact on our collective psychology and our subjective feelings of security and safety. This network acts like a huge megaphone, vastly amplifying the emotional impact of terrorism.

To maximize this impact, the perpetrators of complex terrorism will carry out their attacks in audacious, unexpected, and even bizarre manners—using methods that are, ideally, unimaginably cruel. By so doing, they will create the impression that anything is possible, which further magnifies fear. From this perspective, the World Trade Center represented an ideal target, because the Twin Towers were an icon of the mag-

nificence and boldness of American capitalism. When they collapsed like a house of cards, in about 15 seconds each, it suggested that American capitalism was a house of cards, too. How could anything so solid and powerful and so much a part of American identity vanish so quickly? And the use of passenger airplanes made matters worse by exploiting our worst fears of flying.

Unfortunately, this emotional response has had huge, real-world consequences. Scared, insecure, grief-stricken people aren't ebullient consumers. They behave cautiously and save more. Consumer demand drops, corporate investment falls, and economic growth slows. In the end, via the multiplier effect of our technology-amplified emotional response, the September 11 terrorists may have achieved an economic impact far greater than they ever dreamed possible. The total cost of lost economic growth and decreased equity value around the world could exceed a trillion dollars. Since the cost of carrying out the attack itself was probably only a few hundred thousand dollars, we're looking at an economic multiplier of over a millionfold.

### **The Weakest Links**

Complex terrorism operates like jujitsu—it redirects the energies of our intricate societies against us. Once the basic logic of complex terrorism is understood (and the events of September 11 prove that terrorists are beginning to understand it), we can quickly identify dozens of relatively simple ways to bring modern, high-tech societies to their knees.

How would a Clausewitz of terrorism proceed? He would pinpoint the critical complex networks upon which modern societies depend. They include networks for producing and distributing energy, information, water, and food; the highways, railways, and airports that make up our transportation grid; and our healthcare system. Of these, the vulnerability of the food system is particularly alarming. However, terrorism experts have paid the most attention to the energy and information networks, mainly because they so clearly underpin the vitality of modern economies.

The energy system—which comprises everything from the national network of gas pipelines to the electricity grid—is replete with high-value nodes like oil refineries, tank farms, and electrical substations. At times of peak energy demand, this network (and in particular, the electricity grid) is very tightly coupled. The loss of one link in the grid means that the electricity it carries must be offloaded to other links. If other links are already operating near capacity, the additional load can

cause them to fail, too, thus displacing their energy to yet other links. We saw this kind of breakdown in August 1996, when the failure of the Big Eddy transmission line in northern Oregon caused overloading on a string of transmission lines down the West Coast of the United States, triggering blackouts that affected 4 million people in nine states.

Substations are clear targets because they represent key nodes linked to many other parts of the electrical network. Substations and high-voltage transmission lines are also "soft" targets, since they can be fairly easily disabled or destroyed. Tens of thousands of miles of transmission lines are strung across North America, often in locations so remote that the lines are almost impossible to protect, but they are nonetheless accessible by four-wheel drive. Transmission towers can be brought down with well-placed explosive charges. Imagine a carefully planned sequence of attacks on these lines, with emergency crews and investigators dashing from one remote attack site to another, constantly off-balance and unable to regain control. Detailed maps of locations of substations and transmission lines for much of North America are easily available on the Web. Not even all the police and military personnel in the United States would suffice to provide even rudimentary protection to this immense network.

The energy system also provides countless opportunities for turning supposedly benign technology to destructive ends. For instance, large gas pipelines, many of which run near or even through urban areas, have huge explosive potential; attacks on them could have the twin effect of producing great local damage and wider disruptions in energy supply. And the radioactive waste pools associated with most nuclear reactors are perhaps the most lethal targets in the national energy-supply system. If the waste in these facilities were dispersed into the environment, the results could be catastrophic. Fortunately, such attacks would be technically difficult.

Even beyond energy networks, opportunities to release the destructive power of benign technologies abound. Chemical plants are especially tempting targets, because they are packed with toxins and flammable, even explosive, materials. Security at such facilities is often lax: An April 1999 study of chemical plants in Nevada and West Virginia by the U.S. Agency for Toxic Substances and Disease Registry concluded that security ranged from "fair to very poor" and that oversights were linked to "complacency and lack of awareness of the threat." And every day, trains carrying tens of thousands of tons of toxic material course along transport

corridors throughout the United States. All a terrorist needs is inside knowledge that a chemical-laden train is traveling through an urban area at a specific time, and a well-placed object (like a piece of rail) on the track could cause a wreck, a chemical release, and a mass evacuation. A derailment of such a train at a nonredundant link in the transport system—such as an important tunnel or bridge—could be particularly potent. (In fact, when the U.S. bombing campaign in Afghanistan began on October 7, 2001, the U.S. railroad industry declared a three-day moratorium on transporting dangerous chemicals.) Recent accidents in Switzerland and Baltimore, Maryland, make clear that rail and highway tunnels are vulnerable because they are choke points for transportation networks and because it's extraordinarily hard to extinguish explosions and fires inside them.

Modern communications networks also are susceptible to terrorist attacks. Although the Internet was originally designed to keep working even if large chunks of the network were lost (as might happen in a nuclear war, for instance), today's Internet displays some striking vulnerabilities. One of the most significant is the system of computers—called "routers" and "root servers"—that directs traffic around the Net. Routers represent critical nodes in the network and depend on each other for details on where to send packets of information. A software error in one router, or its malicious reprogramming by a hacker, can lead to errors throughout the Internet. Hackers could also exploit new peer-to-peer software (such as the information-transfer tool Gnutella) to distribute throughout the Internet millions of "sleeper" viruses programmed to attack specific machines or the network itself at a predetermined date.

The U.S. government is aware of many of these threats and of the specific vulnerability of complex networks, especially information networks. President George W. Bush has appointed Richard Clarke, a career civil servant and senior advisor to the National Security Council on counterterrorism, as his cyberspace security czar, reporting both to Director of Homeland Security Tom Ridge and National Security Advisor Condoleezza Rice. In addition, the U.S. Senate recently considered new legislation (the Critical Infrastructure Information Security Act) addressing a major obstacle to improved security of critical networks: the understandable reluctance of firms to share proprietary information about networks they have built or manage. The act would enable the sharing of sensitive infrastructure information between the federal government and private sector and within the private sector itself. In his opening remarks to introduce the act on September 25, 2001, Republican Sen. Bob Bennett of Utah clearly recognized

that we face a new kind of threat. "The American economy is a highly interdependent system of systems, with physical and cyber components," he declared. "Security in a networked world must be a shared responsibility."

### **Preparing for the Unknown**

Shortly following the September 11 attacks, the U.S. Army enlisted the help of some of Hollywood's top action screenwriters and directors—including the writers of *Die Hard* and *McGyver*—to conjure up possible scenarios for future terrorist attacks. Yet no one can possibly imagine in advance all the novel opportunities for terrorism provided by our technological and economic systems. We've made these critical systems so complex that they are replete with vulnerabilities that are very hard to anticipate, because we don't even know how to ask the right questions. We can think of these possibilities as "exploitable unknown unknowns." Terrorists can make connections between components of complex systems—such as between passenger airliners and skyscrapers—that few, if any, people have anticipated. Complex terrorism is particularly effective if its goal is not a specific strategic or political end, but simply the creation of widespread fear, panic, and economic disruption. This more general objective grants terrorists much more latitude in their choice of targets. More likely than not, the next major attack will come in a form as unexpected as we witnessed on September 11.

What should we do to lessen the risk of complex terrorism, beyond the conventional counterterrorism strategies already being implemented by the United States and other nations? First, we must acknowledge our own limitations. Little can be done, for instance, about terrorists' inexorably rising capacity for violence. This trend results from deep technological forces that can't be stopped without producing major disruptions elsewhere in our economies and societies. However, we can take steps to reduce the vulnerabilities related to our complex economies and technologies. We can do so by loosening the couplings in our economic and technological networks, building into these networks various buffering capacities, introducing "circuit breakers" that interrupt dangerous feedbacks, and dispersing high-value assets so that they are less concentrated and thus less inviting targets.

These prescriptions will mean different things for different networks. In the energy sector, loosening coupling might mean greater use of decentralized, local energy production and alternative energy sources (like small-scale solar power) that make individual users

more independent of the electricity grid. Similarly, in food production, loosening coupling could entail increased autonomy of local and regional food-production networks so that when one network is attacked the damage doesn't cascade into others. In many industries, increasing buffering would involve moving away from just-in-time production processes. Firms would need to increase inventories of feedstocks and parts so production can continue even when the supply of these essential inputs is interrupted. Clearly this policy would reduce economic efficiency, but the extra security of more stable and resilient production networks could far outweigh this cost.

Circuit breakers would prove particularly useful in situations where crowd behavior and panic can get out of control. They have already been implemented on the New York Stock Exchange: Trading halts if the market plunges more than a certain percentage in a particular period of time. In the case of terrorism, one of the factors heightening public anxiety is the incessant barrage of sensational reporting and commentary by 24-hour news TV. As is true for the stock exchange, there might be a role for an independent, industry-based monitoring body here, a body that could intervene with broadcasters at critical moments, or at least provide vital counsel, to manage the flow and content of information. In an emergency, for instance, all broadcasters might present exactly the same information (vetted by the monitoring body and stated deliberately and calmly) so that competition among broadcasters doesn't encourage sensationalized treatment. If the monitoring body were under the strict authority of the broadcasters themselves, the broadcasters would—collectively—retain complete control over the content of the message, and the procedure would not involve government encroachment on freedom of speech.

If terrorist attacks continue, economic forces alone will likely encourage the dispersal of high-value assets. Insurance costs could become unworkable for businesses and industries located in vulnerable zones. In 20 to 30 years, we may be astonished at the folly of housing so much value in the exquisitely fragile buildings of the World Trade Center. Again, dispersal may entail substantial economic costs, because we'll lose economies of scale and opportunities for synergy.

Yet we have to recognize that we face new circumstances. Past policies are inadequate. The advantage in this war has shifted toward terrorists. Our increased vulnerability—and our newfound recognition of that vulnerability—makes us more risk-averse, while terrorists have become more powerful and more tolerant of risk. (The September 11 attackers, for instance, had an

extremely high tolerance for risk, because they were ready and willing to die.) As a result, terrorists have significant leverage to hurt us. Their capacity to exploit this leverage depends on their ability to understand the complex systems that we depend on so critically. Our capacity to defend ourselves depends on that same understanding.

### **Sidebar: Feeding Frenzies**

Shorting out electrical grids or causing train derailments would be small-scale sabotage compared with terrorist attacks that intentionally exploit psychological vulnerabilities. One key vulnerability is our fear for our health—an attack that exploits this fear would foster widespread panic. Probably the easiest way to strike at the health of an industrialized nation is through its food-supply system.

Modern food-supply systems display many key features that a prospective terrorist would seek in a complex network and are thus highly vulnerable to attack. Such systems are tightly coupled, and they have many nodes—including huge factory farms and food-processing plants—with multiple connections to other nodes.

The recent foot-and-mouth disease crisis in the United Kingdom provided dramatic evidence of these characteristics. By the time veterinarians found the disease, it had already spread throughout Great Britain. As in the United States, the drive for economic efficiencies in the British farming sector has produced a highly integrated system in which foods move briskly from farm to table. It has also led to economic concentration, with a few immense abattoirs scattered across the land replacing the country's many small slaughterhouses. Foot-and-mouth disease spread rapidly in large part because infected animals were shipped from farms to these distant abattoirs.

Given these characteristics, foot-and-mouth disease seems a useful vector for a terrorist attack. The virus is endemic in much of the world and thus easy to obtain. Terrorists could contaminate 20 or 30 large livestock farms or ranches across the United States, allowing the disease to spread through the network, as it did in Great Britain. Such an attack would probably bring the U.S. cattle, sheep, and pig industries to a halt in a matter of weeks, costing the economy tens of billions of dollars.

Despite the potential economic impact of such an attack, however, it wouldn't have the huge psychological effect that terrorists value, because foot-and-mouth

disease rarely affects humans. Far more dramatic would be the poisoning of our food supply. Here the possibilities are legion. For instance, grain storage and transportation networks in the United States are easily accessible; unprotected grain silos dot the countryside and railway cars filled with grain often sit for long periods on railway sidings. Attackers could break into these silos and grain cars to deposit small amounts of contaminants, which would then diffuse through the food system.

Polychlorinated biphenyls (PCB)—easily found in the oil in old electrical transformers—are a particularly potent group of contaminants, in part because they contain trace amounts of dioxins. These chemicals are both carcinogenic and neurotoxic; they also disrupt the human endocrine system. Children in particular are vulnerable. Imagine the public hysteria if, several weeks after grain silos and railway cars had been laced with PCBs and the poison had spread throughout the food network, terrorists publicly suggested that health authorities test food products for PCB contamination. (U.S. federal food inspectors might detect the PCBs on their own, but the inspection system is stretched very thin and contamination could easily be missed.) At that point, millions of people could have already eaten the products.

Such a contamination scenario is not in the realm of science fiction or conspiracy theories. In January 1999, 500 tons of animal feed in Belgium were accidentally contaminated with approximately 50 kilograms of PCBs from transformer oil. Some 10 million people in Belgium, the Netherlands, France, and Germany subsequently ate the contaminated food products. This single incident may in time cause up to 8,000 cases of cancer.

### **Further Reading**

Many of the ideas introduced in this article are discussed further in Thomas Homer-Dixon's *The Ingenuity Gap: How Can We Solve the Problems of the Future?* (New York: Alfred A. Knopf, 2000). See especially Chapter 4, which examines the nature and sources of complexity in our societies and technologies, as well as the discussion of the instabilities of complex technological systems and networks in Chapter 7 and of terrorism in Chapter 13.

A comprehensive technical treatment of complexity theory can be found in *Dynamics of Complex Systems* (Reading: Addison-Wesley, 1997) by Yaneer Bar-Yam. This book is not for the faint-hearted, and some knowl-

edge of mathematics is helpful, but Bar-Yam is quite daring in his treatment of the social, political, and security implications of complexity. A truly groundbreaking discussion of the sources of complexity in biological, technological, and social systems is W. Brian Arthur's "On the Evolution of Complexity" in *Complexity: Metaphors, Models, and Reality*, edited by G. Cowan, D. Pines, and D. Meltzer (Reading: Addison-Wesley, 1994).

Countless writings examine the implications of rising complexity in our world, but four are particularly stimulating. The seminal discussion of the perils of complex technological systems is Charles Perrow's *Normal Accidents: Living With High-Risk Technologies* (New York: Basic Books, 1984). Gene Rochlin examines the unexpected outcomes of the information revolution in *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton: Princeton University Press, 1997). Langdon Winner's wonderful article "Complexity and the Limits of Human Understanding" is rich with insights on the social and cognitive challenges posed by rising complexity. It can be found in a book that is worth reading in its entirety: *Organized Social Complexity: Challenge to Politics and Policy* (Princeton: Princeton University Press, 1975), edited by Todd La Porte. For a far more apocalyptic but tremendously provocative study of the risks of greater social complexity, see Joseph Tainter's *The Collapse of Complex Societies* (Cambridge: Cambridge University Press, 1988).

On the vulnerabilities of modern infrastructure, see *Critical Foundations: Protecting America's Infrastructures* (Washington: President's Commission on Critical Infrastructure Protection, 1997) and Massoud Amin's "National Infrastructures as Complex Interactive Networks" in Tariq Samad and John Weyrauch, eds., *Automation, Control, and Complexity: An Integrated Approach* (Chichester: John Wiley & Sons, 2000). For a journalistic account of how New York financial firms protected their critical infrastructure in the aftermath of the September 11 attacks, see Tom Foremski's "How Business Could Survive" (*Financial Times*, October 10, 2001).