Chapter 38

Global Networks and Security: How Dark Is the Dark Side?

Martin C. Libicki

Networks span this country and go overseas. Although the United States has the choice to reject them, for the most part, it has greatly profited from their existence and operation. Our lives are generally richer from the increased prosperity, more opportunity, and greater variety that networks provide. Networks, on the whole, make the world safer; they are conduits through which other nations have adopted U.S.-promoted values such as freedom, democracy, rule of law, and individual initiative.

Networks do have their dark side. In growing dependent on them, the United States puts itself at risk from unexpected faults in their flows. Shocks to the system can arise if flows are expectedly small (for example, an oil cutoff) or too large (for example, drugs). The internationalization of computer networks creates at least a theoretical possibility that our enemies overseas could damage large parts of infrastructure and thus cripple our economy, without even the inconvenience of leaving home.

A network is but a set of conduits between nodes over which something flows. That something can be tangible items, such as people, goods, or germs. It also can be intangible—for example, money or memes (ideas that propagate from person to person) or control of information over computers and communications. Networks have always been part of human history, even if bit-hauling networks are new: in the United States they have existed only since 1844 (the telegraph), and globally they have existed only since 1866. In general, they have been steadily increasing their presence in the global economy and society. There is more flow, more types of flows, and the flows are faster.

This chapter aims to present a comprehensive and empirical perspective on international networks. It addresses the Internet and other information systems but also covers a broader set of networks, seeing their operations as composed of several parts whose impact is assessed as a whole. It also offers a framework for examining the risks to U.S. national security from international networks. A complex system of international networks is rapidly becoming a powerful variable in global security affairs. It may encourage peace but may also exacerbate discord; it may even tip the scales toward war. It can, as well, affect how wars are carried out by the United States and other countries. Thus,

---

Martin C. Libicki is a senior policy analyst at RAND. Formerly he was a senior fellow in the Institute for National Strategic Studies at the National Defense University. Dr. Libicki is the author of Scaffolding the New Web, Illuminating Tomorrow's War, The Mesh and the Net, *and* Defending Cyberspace and Other Metaphors.

this chapter is less optimistic than is much of the other literature on international networks, but it also casts less gloom than do other forecasts of unmitigated and imminent disaster. Such networks bring with them sunshine, clouds, and the occasional storm. All three aspects need to be understood.

In this treatment, a brief conceptual overview is followed by a discussion of three types of flows: tangible goods, intangibles, and network control information. Most of the emphasis will be on the last category. As the newest type of network, it is the one about which the least has been written (despite heroic efforts of late to bridge the gap). Also, information network attack has been increasingly theorized to be the preferred mode of 21st-century warfare.

For the purposes of this chapter, *national security* is defined broadly. It is the ability to keep the American people shielded from the substantial negative consequences of actors or forces coming from overseas. Why so broad a definition? Limiting national security to the ability of foreign entities to control the country per se would limit network risks to a paralyzing but highly implausible computer attack on the Nation's nuclear command-and-control system. Thus, only a broad definition can give the subject analytical traction.

The ultimate point presented in this chapter is thus to establish a mode of discourse through which policies that garner the benefits can be discussed and ways to manage the risks of international networks can be found and validated.

General Principles

Risks from existing international networks to the United States or any other country can be ascribed to one or another fault in the flows along the conduit. Such faults can be divided into three categories: disruption, eruption, and corruption.

Disruption is the unexpected decline of a flow on which economic or well-being has been predicated: the Arab Oil embargo (1973–1974) is an example (albeit one that was deliberately engineered for that purpose). Wars, strikes, accidents, and natural disasters can also create disruption: in the last quarter of 1999, the world suffered a shortage of computer memory chips because of an earthquake in Taiwan.

Eruption is too much flow. Examples include the hot money that made Southeast Asian currencies so unstable in the 1990s, the surge of refugees from Cuba in 1980, the waves of cocaine washing over American cities, or computer attacks that come from unleashing a flood of unwanted email.

Corruption may be defined as a flow rendered dangerous because of unexpected changes in its makeup. Several years ago, for instance, a few imported table grapes were found laced with cyanide. No one was hurt, but a pall was put over the imported-grape industry for several months. This incident illustrates an oft-repeated link between networks and globalization: people are quick to blame foreigners for faults of undetermined origin. The grapes were Chilean, and it was therefore immediately assumed that the cyanide was placed in that country (perhaps as protest against the military government). Only later did food scientists conclude that the cyanide would not have survived the long boat trip from Chile. More recently, Islamic fundamentalists were thought responsible for the Oklahoma City bombing until an arrest was made.

Which is the worst threat: disruption, eruption, or corruption? Of the three, only disruption requires that one go to, or at least affect, the source if it is to be straightened out. Eruptions and corruptions can, in theory, be managed, either through border controls (in the case of eruptions) or border filters (in the case of corruptions), although neither is necessarily simple to do. By another measure, corruption is the most difficult problem. It is hard to determine whether it *has* taken place, much less *is* taking place. Disruption and eruption have less ambiguous metrics, although it can be hard to actually measure them (for example, to determine the amount of narcotics crossing the border). Table 1 sketches six categories of flows plus contraband (that is, bad goods) and the three types of network faults. It illustrates where each fault applies to which flow. The squares are filled with examples or effects.

Table 1. Samples of Network Faults for Specific Flow Categories

	Network Fault		
Flow	*Disruption*	*Eruption*	*Corruption*
Tangibles			
Goods	Oil embargoes	Dumping	Hazardous material
Contraband	"Cold turkey"	Drug infestation	Possible health effects
People	Skill shortages	Aliens, refugees	Criminals, terrorists
Germs	N/A	Epidemics	New disease strains
Intangibles			
Money	Asset deflation	Speculation, inflation	Business, political corruption
Memes	N/A*	N/A*	Manias, panics
Network Data			
Bits	Loss of e-commerce	Some denial-of-service attacks, spamming	Illicit access, spoofing

*The quantity of memes is meaningless.

This table suggests that disruptions largely affect the flow of goods and money—that is, trade. Disruption is less important for the other categories than it is for goods and money. Eruptions affect all categories except memes. Corruption affects all categories, but perhaps goods least. Also, corruption is defined to affect money insofar as money is seen as corrupting as well as corrupted (such as counterfeit currency).

Perhaps the broader issue is less one of which fault is at work and more of the phenomenon of overall stability in the network. A flood of bits in a denial-of-service attack may squeeze legitimate traffic to e-commerce sites to a trickle. An eruption of refugees may be correlated with the reduced ability to weed out criminals from that mix (for ex-

ample, the 1980 influx from Cuba). Trade embargoes are often associated with a rise in black marketeering.

Some propagation phenomena are well modeled. Quantity faults such as disruption or eruption are measured by their size and speed. The latter is a function of link speed, network clumpiness (the "six degrees of separation" phenomenon does not work well if everyone lives in isolated villages), and the size of buffers available to smooth out flows.

Networks of Tangibles

Flows of goods, people, and disease said to define networks can be physical (for example, roads, pipelines) or implied (for example, airways), and points of entry can be both limited (for example, international airports) and unlimited (for example, anywhere a border can be crossed by foot). Some networks, such as those along which oil is traded, are defined by formal contractual arrangements; others, such as the Underground Railroad of the 19th century, are built on informal arrangements.

How are faults along such networks best characterized? How does the globalization of such networks affect the nature and distribution of such threats?

Goods

Over time, the global economy has grown more sensitive to possible disruptions in the flow of goods, thanks to three factors: rising shares of world (and U.S.) gross domestic product originating in exports and imports, the shift of such exports from commodities to intermediate components of complex manufactures, and steady reductions in work-in-process inventories arising from just-in-time production philosophies. As a partial offset, globalization permits a wider range of suppliers than simply those at home and thus some alternatives to problems with any one of them.

An unanticipated cutoff in the supply of components to a manufacturing process can now stop production lines all over the world. The key word is "unanticipated." Parts sourced from regions where shipping schedules are unstable are more likely to be kept in reserve against such contingencies, just as coal mountains were used to buffer electric utilities against the threat of strikes. A similar sensitivity to disruption characterizes aircraft and air freight networks. Very few goods, nevertheless, are of such importance that disruptions in their flow rise to the level of national security concerns.

Except, of course, oil. The Arab oil embargo came close to being a *casus belli*. In 1956–1957, the American embargo on oil exports to the United Kingdom and France helped persuade these countries to abandon their seizure of the Suez Canal, a goal to which they committed military forces. The global oil threat has not disappeared. The United States and its allies are no less dependent on imported oil today than they were in 1973 and 1979. Nonetheless, petroleum is one of those exceptions that do prove the rule. Its sheer weight in the global economy, as well as its unbalanced distribution (most of the world's oil crosses national borders between extraction and consumption), are characteristics possessed by no other commodity (most grains do not cross borders in their life cycle; no single metallic ore carries that much weight in industrial societies). Thus, the disruption of any other goods does not come close to having even a fraction of oil's

economic effect and thus an effect on national security of any country when broadly defined. Oil was a globalized commodity throughout the 20th century, but its eventual displacement in the 21st century by natural gas, and perhaps hydrogen/electricity networks, may result in *less* globalization of the world's energy economy.

An unanticipated disruption in the flow of components for U.S. weapons systems was of desultory national security concern in the 1980s, with some in the Department of Defense (DOD) worried about the vulnerabilities that may exist because of foreign source dependence. Almost every part in a complex weapons system is unique and hard to replace in the short run without skipping a lengthy qualification process. For the time being and into the foreseeable future, however, this threat is nominal. The U.S. military has abundant weapons systems for any conceivable foe; many production lines are shut, and others are running well below what they produced in the 1980s. Even in the height of the Reagan buildup the problem was easily manageable. In comparison with their civilian counterparts, defense goods have within them fewer parts from overseas; in the 1980s, the share of value added from imports was roughly 10 times less than for comparable civilian goods. What does come from overseas is primarily sourced from Europe rather than industrializing Asia or the Third World. Finally, the defense sector lags behind others in adopting just-in-time manufacturing. By one estimate, a stock of $15 million would have buffered the production of *all* active precision-guided munition production lines in 1986—a $6 billion activity.

National security aside, does globalization necessarily put the American economy at greater risk from disruption? The flow of goods is subject to all sorts of perturbation: acts of nature, accidents, terrorism, strikes, politics, and war. Some disruptions come from breakdowns in other networks, such as air or ship transport, as well as in support services, such as electricity. A sufficiently broad attack on computer networks may, by disrupting production schedules, hinder the international flow of goods. Buying goods at home rather than overseas (especially from Third World countries) makes them less subject to political and military disruption. Support infrastructures such as power and transport are more reliable at home as well. As a general rule, every transportation hop in a distribution chain adds a little more risk to the total. But the increased risk of disruption from Mother Nature, accidents, terrorism, and strikes cannot be much greater overseas than it is at home. More specifically, the sensitivity of overseas manufacturing to errant computer networks cannot be much greater than the sensitivity of domestic networks—and it is very low in any case. There is some evidence that foreign computer owners are less well protected against viruses than are domestic ones; the Chernobyl virus, by some reports, wreaked considerable damage in Korea. Foreign Y2K preparations also lagged, even if no society was greatly affected in the end. Conversely, foreign firms tend to adopt computers and the Internet less thoroughly and later than have comparable American firms—and are therefore less sensitive to perturbations in such networks. If all this information technology fails, they are more likely to remember how to work without it.

People

The flow of people may be classified into short-term purposes, such as tourism, licit business travel, and illicit business travel; medium-term purposes, such as education and

other temporary relocation; and long-term purposes, such as permanent immigration. Disruptions in flows among four of the categories can be dismissed: a falloff in tourism would be of negligible import to the *overall* American economy, although some regions are more sensitive (for example, Florida lost business after several European automobile renters were murdered; Hawaii has suffered from the Japanese recession). Business travel can be increasingly replaced by communications, and travel for education and temporary relocation can often be postponed.

That leaves illicit business travel (for example, smuggling, or terrorism) and immigration as means by which threats may be discerned from the flow of people—via eruption rather than disruption. Informal networks of former compatriots are often key to making both flows work. In the case of immigration, such networks are encouraged to ensure that newcomers can be supported while they acclimate to the United States. So far, the damage to the U.S. national security caused by illegal entry, whether by criminals or undocumented aliens, has been modest. Indeed, many studies show the United States to be the beneficiary of undocumented aliens who often play a contributing role in the economy, especially as farm workers and other blue-collar jobs.

Germs

AIDS, which in comparison with other pathogens is not particularly infectious, spread throughout southern and central Africa because of interpersonal contacts along truck routes. It spread to North America because of air travel.

Thanks to globalization, Americans now face increased exposure to infectious diseases that hitherto remained localized in some far corner of the world. This phenomenon is not new—measles and smallpox ravaged the population of the New World when it was discovered by the Old—but the plethora of risks that may be uncovered and the speed at which they can propagate are unprecedented. Many synthetic germs may arise from otherwise benign actions (for example, dispensing antibiotics in quantities that accelerate the appearance of drug-resistant strains), accidents (for example, a bad day at the gene-splicing machine), or biological warfare. The threat of new plagues also may be defined as a national security concern: not only might people die in large numbers, but also the various quarantines that may follow could seriously affect international relations.

Fortunately, health networks are improving. Most victims of the 1918–1920 Spanish influenza outbreak died from poorly treated secondary infections that could be more readily treated today. The U.S. Centers for Disease Control and Prevention are building and monitoring complex networks that permit the early identification of life-threatening ailments on a global basis.

Networks of Intangibles

Intangibles, besides being weightless, are of ambiguous character. Money, for instance, is a delicately balanced instrument of value. A currency is no more a credit to its holder than it is a deficit to its issuer. Memes range from true insights to false beliefs;

their value is often known only in deep retrospect. The flow of either money or memes across the seas is potentially corrupting, if the memes are not corrupted themselves.

Money

Financial markets have long been among the pioneer users of information technology (for example, the carrier pigeons that gave the Rothschilds advanced news of Waterloo), not least of which is the Internet (and its predecessors, private networks). Certain types of financial assets have been globalized for decades, and money has as a consequence shown a disturbing propensity to surge into and from markets on the basis of the merest whiff of opportunity or woe.

National economies have, for better or worse, been tightly linked for centuries. The Great Depression was a systemic disaster for the entire industrialized world. The rise in oil prices sparked a bout of inflation in every advanced economy. More recently, the run on the Mexican *peso* put other Latin American currencies at risk. The devaluation of the Thai *baht* not only affected most other Asian currencies but also those of Russia and Brazil—despite their vastly different fundamentals. Although national stock markets can and do go in different directions over time, sharp perturbations during an afternoon on Wall Street tend to show up in Tokyo and London on the following night.

So far, no global economic hiccup has arisen from any computer attack. The Y2K bug might have been a test case, but it was not even close to the disaster that people had expected. Can some computer attack arising overseas create chaos that sparks a financial panic that drives down assets values and leads to a recession or worse? Perhaps. Asset markets that have wandered too far from their long-range values are heir to sudden corrections from any number of causes. Large corrections have been historically correlated with hard times. Nevertheless, a computer attack of sufficient size and breadth would be required to change fundamental perceptions about economics and then wind its way through a long causal chain to a recession. There is not even a guaranteed link between stock market crashes and economic performance. The market crash of October 1987 did no discernible harm to the American economy. The longer lived collapse of the Japanese stock market in the 1990s can hardly be discerned from any other nation's economic statistics. If there is causality, fault is more likely to propagate outward from Wall Street than it is to move inward from overseas.

Counterfeit currency and phony stock and bond certificates constitute a special case of corrupted money (albeit in physical form) that has crossed borders along networks of physical commerce. Queering a nation's paper is not an inconceivable attack on its economy, but instances are rare. Almost all counterfeiting takes place for commercial, rather than political, reasons.

Memes

Memes are concepts or perceptions that spread from one person to another. The term was invented by Richard Dawkins to make an analogy to gene propagation. Fashions (for example, the Goth look) are memes, albeit trivial ones. The notion that so-called Asian values work better than do Western ones, that Anglo-Saxon capitalism is worth emulating, that the Internet has fundamentally changed stock market values, or

that Europe needs an independent military capability are all serious memes, that is, intellectual fashions with consequences that matter.

Many memes fall under the rubric of who-gave-them-that-idea. Why, for instance, is there a rash of high school shootings today, for instance, and not in more generally violent periods? Why are right-wing militias considered by some a plausible form of political activity today, but not earlier? Why did left-wing terrorism become a method of political expression considered acceptable by decades ago, but much less so today? Or, more generally, why do certain disruptive ideologies or beliefs become popular when they do? And what bizarre ideas will the coming years bring?

The Internet—an international network—may well accelerate the spread of memes, both trivial and serious. Not only are there more instant two-way conduits for such ideas, but the rise of services such as instant messaging also means that ideas can spread through interlinked groups with great swiftness: one need not hang up the phone and dial someone else to pass the news along. By one estimate, a meme can travel around the world in 48 hours. Bad ideas can propagate quickly. Even if correctives can also spread, they play catch-up for much of the journey.

On the whole, the United States has a large export surplus in memes. More people overseas worry about what crazy idea is coming from us than do we worry about what crazy idea we may be subjected to from beyond our borders.

Networks of Bits

Is there a national security threat from international information networks (that is, the Internet, but also telephony, and, for some purposes, satellite and other broadcasting)? A good deal depends on how widely one casts the net, so to speak. If anything coming over the wires but disliked by governing bodies constitutes a threat, the answer is yes. If one considers only those bits that force their way into people's systems, the answer is no. Since there is no forced entry in cyberspace, there is no coercion that can be delivered by wire that one cannot evade (flooding attacks are a partial exception because they appear initially indistinguishable from good traffic). Thus, there is no national security threat. But if one takes into account the evident fact that people and institutions seem to demonstrate only a modest ability to protect themselves, then malefactors can hold, if not their lives, then at least their ways of life, at risk.

The discussion starts by looking at the threat from international networks and then turns to the threat to networks from globalization.

Networks as Conduits

Some nations regard dissent, blasphemy, rampant consumerism, and pornography (displaying for all what one cannot do legally in public) as a threat to their culture and the legitimacy of their institutions—and thus to their national security. Lest such nations be dismissed as primitives, many Western nations put hate speech in the same category. Some of the Internet's traffic is outright illegal in the United States: gambling, commercial fraud, the practice of medicine without a license, theft of intellectual property, money laundering, hard pornography (displaying what one cannot do legally anywhere).

If lawlessness is defined as a national security threat, then these, too, are issues. In no case must one go overseas to return such bits homeward, but doing so makes it harder to be arrested, or at least found. Here, globalization exacerbates the threat potential that already exists from widespread networking.

Another threat from globalization is the loss of privacy if data collected under American law are sent overseas and abused. What if some nefarious group got hold of data—from commerce, government files, or sensors too small to detect—on U.S. citizens and used those data for coercive purposes? Worse, what if such information was used to threaten the stateside families of U.S. warfighters deployed overseas? Americans might find that even the knowledge of their goings-on in the hands of foreign intelligence agencies would be deeply disturbing, even without an explicit threat to exploit such data. Ironically, this is a complaint more frequently directed against the United States (notably by Canada and Europe) than by the United States.

In some cases, bit flows on certain topics, while not necessarily illegal, may induce other threats to national security. It is well understood that terrorists and transnational criminal organizations have been able to extend their range and reach through the adroit use of networking. But other data may also pass through the Internet: classified data (espionage need not rely on hazardous hand passage of material); cryptographic know-how; design information on sensitive technologies (such as supercomputers); nuclear secrets, information on how to build bombs, or, worse, chemical and biological weapons; and information that reveals the vulnerability of specific targets (much of which, such as schematics of nuclear power plant control rooms, has been posted by targets themselves on the World Wide Web). As a general rule, any control regime that, to succeed, must slow the propagation of information or keep it within its borders may be safely consigned to the trash can. A control regime that depends on keeping information within a network (especially if electronically detached from the rest of the world) still stands a chance, although material is likely to leak faster today than it would have 10 or 20 years ago. Again, it is ubiquitous networking rather than its extension overseas that is the fundamental source of difficulty. Here, too, globalization makes it harder to catch the recipient of such information, especially because, in so many cases, only another government would have a great interest in such information (espionage, embargoed technology, or nuclear secrets).

International Threats to Domestic Networks

A hypothetical domestic entity with a purely domestic network with no Internet connections may, nevertheless, face certain risks from globalization.

One risk stems from the growing presence of foreign workers (whether they ultimately intend to become U.S. citizens). In theory, a hostile power could infiltrate them into a United States, especially into high-tech regions, such as Silicon Valley, which can give favored newcomers a very warm welcome and allow them to reap a harvest of ill-gotten knowledge. DOD, for one, is sensitive to such threats and has made U.S. citizenship a general prerequisite to working on classified projects. Some members of the intelligence community would like to extend this restriction to those who administer sensitive software and systems (for example, banking networks). The more paranoid do not even trust U.S. citizens who have relatives or extended family overseas.

Others fear that the rising share of software and software-encoding hardware (that is, silicon chips) coming from overseas presages an especially insidious form of threat—even to purely domestic and unconnected enterprises. Many firms from India are working on software fixes; could they, in the process, sneak logic bombs or back doors into the code that give them entrée to later mischief? Are the chip-packaging facilities in Malaysia secretly inserting a few rogue transistors that can, on command, cause everything with the chip in it to shut down or go haywire at once? True, at least some software repair persons have slipped a little extra in on top, and not every chip that has come off a production line is gotcha-free. Nonetheless, there is no evidence that foreign concerns are more likely than domestic ones to engage in nefarious activities. Furthermore, being removed from the domestic market, foreigners would have a harder time determining the effects of skullduggery or blackmail.

Threats to International Networks

Simply by building a network that can be accessed through the Internet (or at least through phone lines) entities put themselves at risk. With globalization, the risks are putatively greater because there are more sources of trouble, and some of these sources are foreign governments with their own motive for probing or even attacking U.S. systems. Attacks can be divided into the general and the specific.

Viruses (and worms, a variant propagated through email but often less destructive to files) are general threats. They are not aimed at a specific system but seek to wreak havoc on a whole class of systems. Here, globalization adds to the threat. Certain countries (for example, Bulgaria, Pakistan, Israel, the Philippines) have been associated with some of the more virulent strains. In general, the more nodes in the Internet, the greater the likelihood of a virus arising in the world system. One might think that virus attacks should be favored over intrusion attacks by underemployed programmers who work where cycles are abundant (so one can test many configurations) but network connections are weak (and so direct hacking is harder). However, the current flock of new viruses (such as the Love Bug, Melissa, Chernobyl, Bubble Boy, the Tribal Flood Network) prey on unsuspecting messaging systems (Microsoft Outlook) and thus require networking, at least to test.

There has also been considerable military speculation in Russia and China on the efficacy of viruses as an information warfare tool. True, they are a expensive annoyance (if the tens of billion dollars spent annually on antivirus software is indicative) that can idle computers and are time-consuming to eradicate. But are they threats in the sense that they can be directed against a target? They are usable for denial-of-service attacks, but not for collection (reading sensitive files) or corruption (writing bad data to sensitive files), except randomly. Infected computers may be easier to break into; they may be programmed to email passwords back to the originator.

The world of viruses mutates rapidly, and even really good viruses have a lifetime measured, at most, in days (by which time their prevalence will have been detected, and countermeasures devised). They do not work well a second time. General virus techniques also induce countermeasures. Boot sector viruses (that is, those that infect computers booted up from a bad floppy) are rare; macroviruses (that is, those that infect computers when document or spreadsheet files containing executable sequences are

loaded) can be easily disabled if identified as such. Web-based viruses have been nearly eliminated through better browsers. Email viruses are still hazardous, but perhaps email programs will get better. By analogy to the human immune system, the more exposure to viruses today, the better the defenses tomorrow. Many laboratories (including some overseas) are creating theoretical viruses whose antidote can be put into virus-checking programs before the viruses themselves are unleashed. By contrast, unexposed populations are often the ones at greatest risk. Thus, globalization may confer security benefits, at least in a left-handed fashion.

Most specific attacks require that the attacker log onto the target computer system. In the 1980s, this was done through phone-and-modem connections, a technique that reduced the volume of attacks from overseas (because of slow connect times, the lack of direct-dial from some places, and costly per-minute charges). By the 1990s, with the Internet, attacks from overseas were only slightly more difficult to undertake than those from the United States. Defense networks, in particular, have been hit by attacks from overseas (or, in the case of Solar Sunrise, from domestic sources under overseas tutelage). Many, but not all, attacks are casual in the sense they are hacking attacks first and attacks on defense systems second. Not only is DOD disliked by some, but also breaking into defense networks supposedly has a special cachet.

With American borders so porous, a serious attacker could as easily come here and work the networks as stay home and do so and, thereby, if caught, cast suspicious fingers at the source. Nevertheless, it is astonishing how lazy people can be: denial-of-service attacks against the Falun Gong networks in 1999 were readily traceable not only to China but also to the networks used by state security services. Attacks that require access to large intelligence files (for example, known vulnerabilities of connected systems that control specific processes) may create risks if such files have to be moved (although good cryptography obviates that risk—if the intelligence organizations that hold such files trust in such methods). Attacks that originate overseas are also more difficult to trace. Search warrants for traps and traces are tedious to acquire, even from cooperative foreign governments, and some governments may not permit such forensic activity by foreigners on their soil. The disadvantage of operating from overseas is that if the level of annoyance therefrom is sufficiently high, a government that shelters such activity risks upsetting the rest of the international community and thus being cut off from easy communications to the outside.

Globalized Relationships

Extending a corporate network overseas subjects it to risks over and above those associated with a domestic network connected to the Internet. First, until January 2000, it was impossible to export hard encryption technology that used key lengths longer than 40 bits even within the walls of a single corporation. Since encryption is one of the more reliable computer defenses, it left overseas networks potentially more vulnerable than were domestic ones (or forced network administrators to buy foreign products and integrate them into U.S.-supplied network software). Second, foreign nationals overseas may prove less trustworthy than Americans if the personnel vetting process overseas is weaker or if they are approached by local intelligence officials. Third, some foreign laws may complicate securing systems against, or prosecuting, hackers. Fourth, well-known

hacker techniques such as dumpster diving (looking through a firm's garbage to collect sensitive or revealing information), surreptitious entry (gaining physical access to terminals), or social engineering (persuading an employee to give out passwords or accept queered software by pretending to be a network administrator or a inconvenienced user) usually require being there.

Other risks come from establishing a trusted relationship with an overseas entity, a necessity in many industries. Telephone networks have to be connected in order to exchange signaling and call-control information. Likewise, railroad operators connect with one another in order to move cargo across lines. Merchants have terminals on their premises to connect them with credit card companies. Electricity producers are connected in power pools. Many of these connections are long-standing. With digitization, computer-generated data come to replace handcrafted exchanges.

Recent years have seen network relationships grow increasingly sophisticated and intrusive. Wal-Mart makes its just-in-time logistics work by giving daily per-store sales data directly to, for instance, Procter and Gamble, which then uses the information to plan shipping schedules and, ultimately, manufacturing schedules. It logically follows that Procter and Gamble would provide its manufacturing schedules to its own suppliers (for example, Dow Chemical), who then plan shipping and production schedules accordingly. Other tentacles go out to shipping companies, machinery maintenance firms, and computer service suppliers; indeed, the trend is to outsource *all* information-intensive operations.

The risks of such relationships depend on the privileges that each side accords the other. A firm that gives partners full access to its system is only as secure as the least trustworthy partner. Systems linked at the syntactic level (they exchange computer commands) when they were supposed to be linked only at the semantic level (they exchange data) are less secure than they were thought to be. Even systems linked at the semantic level could experience troubles if the information that crosses borders is unreliable (whether through error or malevolence) and unchecked.

A foreign firm intimately linked to an American firm is just one more source of risk. The more firms are so linked, within and across industries, the greater is the potential for bad information anywhere to create fault conditions all over the world. A well-known fault cascade known as the network storm occurs when a problem in one network yields a series of error messages that clog other networks, and these networks respond by releasing error messages of their own, bringing everything down. But for one network to have this effect on another presumes that each network is interested in the other's network management data. This remains the exception rather than the rule.

Certain sectors are more prone to cascading corruption than are others. Electric power is an easy example, but electricity networks do not cross oceans—nor do oil, gas, ethylene pipelines, or railroads. Air traffic control systems rely on explicit, well-practiced hand-offs at sector boundaries. Hospitals are weakly networked internally, much less globally. Emergency services (for example, 911) are provided at local levels. Few governments trust each other sufficiently to keep them continually fed with data that pass without human intervention. The sectors of greatest concern are telecommunications (including Internet service) and finance because they exchange high volumes of data with their overseas counterparts. In the decade to come, just-in-time manufacturing

and electronic commerce may join that list: everything depends on how institutions engineer their connections, what data they exchange, and what provisions they make for filtering clearly errant transmissions.

Some physical constraints, however, make international propagation less likely than domestic propagation: overseas bandwidth is still expensive, and just-in-time manufacturing does not work so quickly for products that have to cross oceans and pass customs before they can be used.

Some Effects on Military Operations

International networks make it easier for both the United States and potential adversaries to carry out military operations, but in doing so, they create new vulnerabilities to the successful completion of these missions.

The balance of effects is sensitive to how international networks are defined. The U.S. military relies on satellites to provide its communications backbone and, as such, relies on international networks almost by definition. It would do so regardless of the level of globalization experienced in the rest of the economy. However, the growth of international *commercial* communications networks gives U.S. forces additional options and capacity to support military operations (extensively exploited, for instance, in *Desert Storm* and, to a lesser extent, in Allied Force). To DOD, these are supplementary capabilities. Nevertheless, commercial communications capability (and, of late, commercial remote-sensing capability) may permit adversaries to conduct operations hitherto impossible; to them such networks are enabling.

The essential asymmetry follows. Since the Armed Forces primarily operates overseas, they need international networks. Because they need these networks, however, they provides their own, irrespective of whether economics would otherwise bring them into being. Our foes tend to work in their own backyards; they need such networks less, and so have not built their own, but can then gain much more from those already extant.

One area where foes profit disproportionately from global networks is international trade. True, the United States can realize economies of scale and access to overseas technology through trade. Yet not only do arms traded internationally end up in the wrong hands but such troubling phenomena as the proliferation of nuclear, chemical, and biological weapons would also be much more difficult to carry out were high-technology firms to serve their own markets to the exclusion of others.

The extent to which DOD ought to rely on networks it does not control is, and will long remain, contentious. Prudently, the Pentagon needs some capacity to construct its own networks wherever it goes. Levels of economic development vary widely, and warfare is often inimical to civilian networks, which are not built to withstand hostile activity. Nevertheless, a greater capacity to exploit what overseas networks do exist to move bits or goods may leverage defense assets considerably. At a minimum, intact intermediate facilities (such as jet fuel depots in Third World airports) could reduce the requirement to haul everything out of the United States.

Even discounting the insecurity of the international Internet or phone system, DOD information networks are inherently vulnerable to destruction via electronic warfare, the action of traitors (among U.S. forces, or as was more common in Vietnam, among allied

forces), the physical capture of warfighters and their access equipment, or, speculatively, over-reliance on commercial off-the-shelf software. The existence of commercial networks only increases their vulnerability. Ninety-five percent of all defense traffic traverses the public-switched network at some point in its life. Even if DOD were to electronically isolate itself, there would be some residual risk from unauthorized connections among several million potential junction points. Nevertheless, in *Desert Storm* and Allied Force alike, the United States appears to have enjoyed greater success from exploiting the dependence of its adversaries on international networks than they have from exploiting those of the Department of Defense.

Finally, the national security advantage that comes from international traffic in memes should not be underestimated: it is the critical conduit for soft power. Even viewed narrowly, the infrastructure makes it easy for the United States to put its case to the world and to mobilize others. Viewed broadly, the influence of American ideas presupposes that others give us the benefit of the doubt.

Policy Issues

In terms of U.S. policy, five points need to be made. The first two need little elaboration. First, there is no such thing as an international networks policy per se. Networks vary greatly in their characteristics, and so do the instruments that affect them—for example, trade policy, law enforcement, diplomacy, military operations. Second, the trend toward globalization of networks shows no sign of slowing. Even an abrupt (and unexpected) reversal of favorable trade and financial policies would not overturn the fundamental economics that are shrinking distance.

The third point is that any realistic balance of good and evil would have the United States, as a whole, favor the globalization of networks. The United States has done well by them. Its economy is the envy of the world; it has overcome the employment fluctuations consistent with opening markets so well that unemployment is at a 30-year low. Free trade in money, goods, and ideas is consistent with the 19th-century liberalism that is still the bedrock of our national belief system. Such ideas have swept over much of the world—from the basic liberal values to many of the reigning cultural icons. The United States (notably, but not only, Silicon Valley) still attracts a disproportionate share of the world's best and hungriest.

The fourth point is that looking across the seven types of network flows suggests that the Nation is less at risk from what may come over international networks than are other countries. Almost all countries are more dependent on the fluctuations of the American economy, monetary policy, or immigration quotas than the reverse. Whatever American fears exist of foreign memes is dwarfed by other countries' fears of ours (unjustifiably, perhaps, but no less so for all that). The United States is a net importer of contraband, but it is worth asking whether the cocaine trade harms the United States or Colombia more. Although the next plague is more likely to come from the Third World to the First than the reverse, such First World tricks as genetic manipulation and the overuse of antibiotics make this prediction tentative over the longer term. So far, our computers have imported more attacks and viruses than they have *been known* to ex-

port, but the fact that most of the world's vulnerable software (for example, Microsoft Outlook) comes from the United States appears to be just deserts.

The fifth point is that the United States cannot easily manage the ill effects of global networks on its own. In the 1970s, price controls were breathtakingly ineffective in coping with Organization of the Petroleum Exporting Countries, and today's calls to release oil from the Strategic Petroleum Reserve to tame higher oil prices are only somewhat less hare-brained. Nonetheless, cooperation seems to work. It took sub rosa negotiations with the Cubans to tame the surge off the island in 1980. International pressure has persuaded nations to criminalize computer network attacks and virus creation. Institutions such as the International Monetary Fund have the capacity, if not necessarily the wit, to mitigate flows of hot money. Interpol helps deal with transnational criminal organizations. The West has funded networks of public health agencies worldwide to give early warnings of epidemics. Conversely, China would have loved to see the United States crack down on the production of memes by the U.S.-based leader of the Falun Gong (ditto for pre-Khatami Iran and Salman Rushdie), but with no hope of success. In other words, opposing the dark side of globalization will require the kind of globalized policymaking toward which the United States has taken tentative steps today.

Concluding Generalizations

The national security threats from globalization are, at worst, exacerbations of threats to people or institutions that networks themselves give rise to. An institution that has promiscuously exposed its workings to everyone via the Internet may be attacked from overseas. Had the Internet stopped at the borders, attackers could also come to America for the same purposes—just not as easily.

The ripples of propagation are often correlated across many different types of networks. The foreign hacker who came to the United States may have come here courtesy of the airline networks; may have initially stayed in a franchise of an international hotel chain; may have paid for that stay with an internationally recognized credit card; may then crash with a member of his or her extended and thus networked family; and may have moved to a college town favored by compatriots who have established informal networks of friends and acquaintances to make each other feel at home. Here, the presence of certain networks permits others to be activated.

Network failures are often correlated across media. An attack on the air traffic control network of Europe may make it difficult for aircraft to leave the Continent, leading to the cancellation of flights in the United States that were waiting for such equipment. If goods or people scheduled to arrive do not show up, processes in the United States (for example, just-in-time manufacturing) may be further disrupted.

Axiomatically, the more open a society, the more risks it is exposed to. Some risks are notional or nearly so (such as the belief that resident aliens are more likely to commit computer crimes than are U.S. citizens). Small dollops of everyday nuisance (viruses) can also bolster a system's immune defenses (for example, antivirus innovations) against catastrophic threats. Apparent threats from globalization may come to be seen as opportunities (for example, high immigration levels) or spurs to

change (Japanese automobile imports). Off-shore sourcing can also mitigate the consequences of variations in domestic supply. What is left, however, has to be handled with the same analytic composure that domestic threats merit.

Many threats to U.S. security come from overseas because they come from hostile states. The extent that U.S. networks—of many types—reach overseas gives them levers they may not otherwise have had. But other threats come from nonstate actors, and many such actors are domestic as well as foreign. Many in the United States fear that foreign governments do not take network-based attacks as seriously as ours does, or claims to. Greater attention on their part might alleviate some risk. But gaining their cooperation for taking action against threats against our society may require that we modify our practices to mollify their concerns: the current hands-off approach to privacy violation in this country is a case in point—but hardly the only one.