

The Dell Theory of Conflict Prevention

Old-Time Versus Just-in-Time

Free Trade is God's diplomacy. There is no other certain way of uniting people in the bonds of peace.

—British politician Richard Cobden, 1857

Before I share with you the subject of this chapter, I have to tell you a little bit about the computer that I wrote this book on. It's related to the theme I am about to discuss. This book was largely written on a Dell Inspiron 600m notebook, service tag number 9ZRJP41. As part of the research for this book, I visited with the management team at Dell near Austin, Texas. I shared with them the ideas in this book and in return I asked for one favor: I asked them to trace for me the entire global supply chain that assembled the pieces that built the laptop that wrote the book. Yes, I wanted to know every part that went into my Dell notebook, what country it came from, and, if possible, the names of the people who put it together along the way. Here is what I found out.

My computer was conceived when I phoned Dell's 800 number on April 2, 2004, and was connected to sales representative Mujteba Naqvi, who immediately entered my order into Dell's order management system. He typed in both the type of notebook I ordered as well as the special features I wanted, along with my personal information, shipping address, billing address, and credit card information. My credit card was verified by Dell through its work flow connection with Visa, and my order was then released to Dell's production system. Dell has six factories around

the world—in Limerick, Ireland; Xiamen, China; Eldorado do Sul, Brazil; Nashville, Tennessee; Austin, Texas; and Penang, Malaysia. My order went out by e-mail to the Dell notebook factory in Malaysia, where the parts for the computer were immediately ordered from the supplier logistics centers (SLCs) next to the Penang factory. Surrounding every Dell factory in the world are these supplier logistics centers, owned by the different suppliers of Dell parts. These SLCs are like staging areas. If you are a Dell supplier anywhere in the world, your job is to keep your SLC full of your specific parts so they can constantly be trucked over to the Dell factory for just-in-time manufacturing.

“In an average day, we sell 140,000 to 150,000 computers,” explained Dick Hunter, one of Dell’s three global production managers. “Those orders come in over Dell.com or over the telephone. As soon as these orders come in, our suppliers know about it. They get a signal based on every component in the machine you ordered, so the supplier knows just what he has to deliver. If you are supplying power cords for desktops, you can see minute by minute how many power cords you are going to have to deliver.” Every two hours, the Dell factory in Penang sends an e-mail to the various SLCs nearby, telling each one what parts and what quantities of those parts it wants delivered within the next ninety minutes—and not one minute later. Within ninety minutes, trucks from the various SLCs around Penang pull up to the Dell manufacturing plant and unload the parts needed for all those notebooks ordered in the last two hours. This goes on all day, every two hours. As soon as those parts arrive at the factory, it takes thirty minutes for Dell employees to unload the parts, register their bar codes, and put them into the bins for assembly. “We know where every part in every SLC is in the Dell system at all times,” said Hunter.

So where did the parts for my notebook come from? I asked Hunter. To begin with, he said, the notebook was codesigned in Austin, Texas, and in Taiwan by a team of Dell engineers and a team of Taiwanese notebook designers. “The customer’s needs, required technologies, and Dell’s design innovations were all determined by Dell through our direct relationship with customers,” he explained. “The basic design of the motherboard and case—the basic functionality of your machine—was designed to those specifications by an ODM [original design manufac-

turer] in Taiwan. We put our engineers in their facilities and they come to Austin and we actually codesign these systems. This global teamwork brings an added benefit—a globally distributed virtually twenty-four-hour-per-day development cycle. Our partners do the basic electronics and we help them design customer and reliability features that we know our customers want. We know the customers better than our suppliers and our competition, because we are dealing directly with them every day.” Dell notebooks are completely redesigned roughly every twelve months, but new features are constantly added during the year—through the supply chain—as the hardware and software components advance.

It happened that when my notebook order hit the Dell factory in Penang, one part was not available—the wireless card—due to a quality control issue, so the assembly of the notebook was delayed for a few days. Then the truck full of good wireless cards arrived. On April 13, at 10:15 a.m., a Dell Malaysia worker pulled the order slip that automatically popped up once all my parts had arrived from the SLCs to the Penang factory. Another Dell Malaysia employee then took out a “traveler”—a special carrying tote designed to hold and protect parts—and started plucking all the parts that went into my notebook.

Where did those parts come from? Dell uses multiple suppliers for most of the thirty key components that go into its notebooks. That way if one supplier breaks down or cannot meet a surge in demand, Dell is not left in the lurch. So here are the key suppliers for my Inspiron 600m notebook: The Intel microprocessor came from an Intel factory either in the Philippines, Costa Rica, Malaysia, or China. The memory came from a Korean-owned factory in Korea (Samsung), a Taiwanese-owned factory in Taiwan (Nanya), a German-owned factory in Germany (Infineon), or a Japanese-owned factory in Japan (Elpida). My graphics card was shipped from either a Taiwanese-owned factory in China (MSI) or a Chinese-run factory in China (Foxconn). The cooling fan came from a Taiwanese-owned factory in Taiwan (CCI or Auras). The motherboard came from either a Korean-owned factory in Shanghai (Samsung), a Taiwanese-owned factory in Shanghai (Quanta), or a Taiwanese-owned factory in Taiwan (Compal or Wistron). The keyboard came from either a Japanese-owned company in Tianjin, China (Alps), a Taiwanese-owned factory in Shen-

zhen, China (Sunrex), or a Taiwanese-owned factory in Suzhou, China (Darfon). The LCD was made in either South Korea (Samsung or LG.Philips LCD), Japan (Toshiba or Sharp), or Taiwan (Chi Mei Optoelectronics, Hannstar Display, or AU Optronics). The wireless card came from either an American-owned factory in China (Agere) or Malaysia (Arrow), or a Taiwanese-owned factory in Taiwan (Askey or Gemtek) or China (USI). The modem was made by either a Taiwanese-owned company in China (Asustek or Liteon) or a Chinese-run company in China (Foxconn). The battery came from an American-owned factory in Malaysia (Motorola), a Japanese-owned factory in Mexico or Malaysia or China (Sanyo), or a South Korean or Taiwanese factory in either of those two countries (SDI or Simplo). The hard disk drive was made by an American-owned factory in Singapore (Seagate), a Japanese-owned company in Thailand (Hitachi or Fujitsu), or a Japanese-owned factory in the Philippines (Toshiba). The CD/DVD drive came from a South Korean-owned company with factories in Indonesia and the Philippines (Samsung); a Japanese-owned factory in China or Malaysia (NEC); a Japanese-owned factory in Indonesia, China, or Malaysia (Teac); or a Japanese-owned factory in China (Sony). The notebook carrying bag was made by either an Irish-owned company in China (Tenba) or an American-owned company in China (Targus, Samsonite, or Pacific Design). The power adapter was made by either a Thai-owned factory in Thailand (Delta) or a Taiwanese-, Korean-, or American-owned factory in China (Liteon, Samsung, or Mobility). The power cord was made by a British-owned company with factories in China, Malaysia, and India (Volex). The removable memory stick was made by either an Israeli-owned company in Israel (M-System) or an American-owned company with a factory in Malaysia (Smart Modular).

This supply chain symphony—from my order over the phone to production to delivery to my house—is one of the wonders of the flat world.

“We have to do a lot of collaborating,” said Hunter. “Michael [Dell] personally knows the CEOs of these companies, and we are constantly working with them on process improvements and real-time demand/supply balancing.” Demand shaping goes on constantly, said Hunter.

What is “demand shaping”? It works like this: At 10 a.m. Austin time, Dell discovers that so many customers have ordered notebooks with 40-gigabyte hard drives since the morning that its supply chain will run short in two hours. That signal is automatically relayed to Dell’s marketing department and to Dell.com and to all the Dell phone operators taking orders. If I happen to call to place my Dell order at 10:30 a.m., the Dell representative will say to me, “Tom, it’s your lucky day! For the next hour we are offering 60-gigabyte hard drives with the notebook you want—for only \$10 more than the 40-gig drive. And if you act now, Dell will throw in a carrying case along with your purchase, because we so value you as a customer.” In an hour or two, using such promotions, Dell can reshape the demand for any part of any notebook or desktop to correspond with the projected supply in its global supply chain. Today memory might be on sale, tomorrow it might be CD-ROMs.

Picking up the story of my notebook, on April 13, at 11:29 a.m., all the parts had been plucked from the just-in-time inventory bins in Penang, and the computer was assembled there by A. Sathini, a team member “who manually screwed together all of the parts from kitting as well as the labels needed for Tom’s system,” said Dell in their production report to me. “The system was then sent down the conveyor to go to burn, where Tom’s specified software was downloaded.” Dell has huge server banks stocked with the latest in Microsoft, Norton Utilities, and other popular software applications, which are downloaded into each new computer according to the specific tastes of the customer.

“By 2:45 p.m., Tom’s software had been successfully downloaded, and [the system was] manually moved to the boxing line. By 4:05 p.m., Tom’s system [was] placed in protective foam and a shuttle box, with a label, which contains his order number, tracking code, system type, and shipping code. By 6:04 p.m., Tom’s system had been loaded on a pallet with a specified manifest, which gives the Merge facility visibility to when the system will arrive, what pallet it will be on (out of 75+ pallets with 152 systems per pallet), and to what address Tom’s system will ship. By 6:26 p.m., Tom’s system left [the Dell factory] to head to the Penang, Malaysia, airport.”

Six days a week Dell charters a China Airlines 747 out of Taiwan and

flies it from Penang to Nashville via Taipei. Each 747 leaves with twenty-five thousand Dell notebooks that weigh altogether 110,000 kilograms, or 242,506 pounds. It is the only 747 that ever lands in Nashville, except Air Force One, when the president visits. "By April 15, 2004, at 7:41 a.m., Tom's system arrived at [Nashville] with other Dell systems from Penang and Limerick. By 11:58 a.m., Tom's system [was] inserted into a larger box, which went down the boxing line to the specific external parts that Tom had ordered."

That was thirteen days after I'd ordered it. Had there not been a parts delay in Malaysia when my order first arrived, the time between when I phoned in my purchase, when the notebook was assembled in Penang, and its arrival in Nashville would have been only four days. Hunter said the total supply chain for my computer, including suppliers of suppliers, involved about four hundred companies in North America, Europe, and primarily Asia, but with thirty key players. Somehow, though, it all came together. As Dell reported: On April 15, 2004, at 12:59 p.m., "Tom's system had been shipped from [Nashville] and was tenured by UPS shipping LTL (3–5-day ground, specified by Tom), with UPS tracking number 1Z13WA374253514697. By April 19, 2004, at 6:41 p.m., Tom's system arrived in Bethesda, MD, and was signed for."

I am telling you the story of my notebook to tell a larger story of geopolitics in the flat world. To all the forces mentioned in the previous chapter that are still holding back the flattening of the world, or could actually reverse the process, one has to add a more traditional threat, and that is an outbreak of a good, old-fashioned, world-shaking, economy-destroying war. It could be China deciding once and for all to eliminate Taiwan as an independent state; or North Korea, out of fear or insanity, using one of its nuclear weapons against South Korea or Japan; or Israel and a soon-to-be-nuclear Iran going at each other; or India and Pakistan finally nuking it out. These and other classic geopolitical conflicts could erupt at any time and either slow the flattening of the world or seriously unflatten it.

The real subject of this chapter is how these classic geopolitical threats might be moderated or influenced by the new forms of collabo-

ration fostered and demanded by the flat world—particularly supply-chaining. The flattening of the world is too young for us to draw any definitive conclusions. What is certain, though, is that as the world flattens, one of the most interesting dramas to watch in international relations will be the interplay between the traditional global threats and the newly emergent global supply chains. The interaction between old-time threats (like China *versus* Taiwan) and just-in-time supply chains (like China *plus* Taiwan) will be a rich source of study for the field of international relations in the early twenty-first century.

In *The Lexus and the Olive Tree* I argued that to the extent that countries tied their economies and futures to global integration and trade, it would act as a restraint on going to war with their neighbors. I first started thinking about this in the late 1990s, when, during my travels, I noticed that no two countries that both had McDonald's had ever fought a war against each other since each got its McDonald's. (Border skirmishes and civil wars don't count, because McDonald's usually served both sides.) After confirming this with McDonald's, I offered what I called the Golden Arches Theory of Conflict Prevention. The Golden Arches Theory stipulated that when a country reached the level of economic development where it had a middle class big enough to support a network of McDonald's, it became a McDonald's country. And people in McDonald's countries didn't like to fight wars anymore. They preferred to wait in line for burgers. While this was offered slightly tongue in cheek, the serious point I was trying to make was that as countries got woven into the fabric of global trade and rising living standards, which having a network of McDonald's franchises had come to symbolize, the cost of war for victor and vanquished became prohibitively high.

This McDonald's theory has held up pretty well, but now that almost every country has acquired a McDonald's, except the worst rogues like North Korea and Iran, it seemed to me that this theory needed updating for the flat world. In that spirit, and again with tongue slightly in cheek, I offer the Dell Theory of Conflict Prevention, the essence of which is that the advent and spread of just-in-time global supply chains in the flat world are an even greater restraint on geopolitical adventurism than the more general rising standard of living that McDonald's symbolized.

The Dell Theory stipulates: No two countries that are both part of a major global supply chain, like Dell's, will ever fight a war against each other as long as they are both part of the same global supply chain. Because people embedded in major global supply chains don't want to fight old-time wars anymore. They want to make just-in-time deliveries of goods and services—and enjoy the rising standards of living that come with that. One of the people with the best feel for the logic behind this theory is Michael Dell, the founder and chairman of Dell.

“These countries understand the risk premium that they have,” said Dell of the countries in his Asian supply chain. “They are pretty careful to protect the equity that they have built up or tell us why we should not worry [about their doing anything adventurous]. My belief after visiting China is that the change that has occurred there is in the best interest of the world and China. Once people get a taste for whatever you want to call it—economic independence, a better lifestyle, and a better life for their child or children—they grab on to that and don't want to give it up.”

Any sort of war or prolonged political upheaval in East Asia or China “would have a massive chilling effect on the investment there and on all the progress that has been made there,” said Dell, who added that he believes the governments in that part of the world understand this very clearly. “We certainly make clear to them that stability is important to us. [Right now] it is not a day-to-day worry for us . . . I believe that as time and progress go on there, the chance for a really disruptive event goes down exponentially. I don't think our industry gets enough credit for the good we are doing in these areas. If you are making money and being productive and raising your standard of living, you're not sitting around thinking, Who did this to us? or Why is our life so bad?”

There is a lot of truth to this. Countries whose workers and industries are woven into a major global supply chain know that they cannot take an hour, a week, or a month off for war without disrupting industries and economies around the world and thereby risking the loss of their place in that supply chain for a long time, which could be extremely costly. For a country with no natural resources, being part of a global supply chain is like striking oil—oil that never runs out. And therefore, getting dropped from such a chain because you start a war is like having your oil wells go

dry or having someone pour cement down them. They will not come back anytime soon.

“You are going to pay for it really dearly,” said Glenn E. Neland, senior vice president for worldwide procurement at Dell, when I asked him what would happen to a major supply-chain member in Asia that decided to start fighting with its neighbor and disrupt the supply chain. “It will not only bring you to your knees [today], but you will pay for a long time—because you just won’t have any credibility if you demonstrate you are going to go [off] the political deep end. And China is just now starting to develop a level of credibility in the business community that it is creating a business environment you can prosper in—with transparent and consistent rules.” Neland said that suppliers regularly ask him whether he is worried about China and Taiwan, which have threatened to go to war at several points in the past half century, but his standard response is that he cannot imagine them “doing anything more than flexing muscles with each other.” Neland said he can tell in his conversations and dealings with companies and governments in the Dell supply chain, particularly the Chinese, that “they recognize the opportunity and are really hungry to participate in the same things they have seen other countries in Asia do. They know there is a big economic pot at the end of the rainbow and they are really after it. We will spend about \$35 billion producing parts this year, and 30 percent of that is [in] China.”

If you follow the evolution of supply chains, added Neland, you see the prosperity and stability they promoted first in Japan, and then in Korea and Taiwan, and now in Malaysia, Singapore, the Philippines, Thailand, and Indonesia. Once countries get embedded in these global supply chains, “they feel part of something much bigger than their own businesses,” he said. Osamu Watanabe, the CEO of the Japan External Trade Organization, was explaining to me one afternoon in Tokyo how Japanese companies were moving vast amounts of low- and middle-range technical work and manufacturing to China, doing the basic fabrication there, and then bringing it back to Japan for final assembly. Japan was doing this despite a bitter legacy of mistrust between the two countries, which was intensified by the Japanese invasion of China in the last century. Historically, he noted, a strong Japan and a strong China

have had a hard time coexisting. But not today, at least not for the moment. Why not? I asked. The reason you can have a strong Japan and a strong China at the same time, he said, “is because of the supply chain.” It is a win-win for both.

Obviously, since Iraq, Syria, south Lebanon, North Korea, Pakistan, Afghanistan, and Iran are not part of any major global supply chains, all of them remain hot spots that could explode at any time and slow or reverse the flattening of the world. As my own notebook story attests, the most important test case of the Dell Theory of Conflict Prevention is the situation between China and Taiwan—since both are deeply embedded in several of the world’s most important computer, consumer electronics, and, increasingly, software supply chains. The vast majority of computer components for every major company come from coastal China, Taiwan, and East Asia. In addition, Taiwan alone has more than \$100 billion in investments in mainland China today, and Taiwanese experts run many of the cutting-edge Chinese high-tech manufacturing companies.

It is no wonder that Craig Addison, the former editor of *Electronic Business Asia* magazine, wrote an essay for the *International Herald Tribune* (September 29, 2000) headlined “A ‘Silicon Shield’ Protects Taiwan from China.” He argued that “Silicon-based products, such as computers and networking systems, form the basis of the digital economies in the United States, Japan and other developed nations. In the past decade, Taiwan has become the third-largest information technology hardware producer after the United States and Japan. Military aggression by China against Taiwan would cut off a large portion of the world’s supply of these products . . . Such a development would wipe trillions of dollars off the market value of technology companies listed in the United States, Japan and Europe.” Even if China’s leaders, like former president Jiang Zemin, who was once minister of electronics, lose sight of how integrated China and Taiwan are in the world’s computer supply chain, they need only ask their kids for an update. Jiang Zemin’s son, Jiang Mianheng, wrote Addison, “is a partner in a wafer fabrication project in Shanghai with Winston Wang of Taiwan’s Grace T.H.W. Group.” And it is not just Taiwanese. Hundreds of big American tech companies now have R & D operations in China; a war that disrupted them could lead not only to the

companies moving their plants elsewhere but also to a significant loss of R & D investment in China, which the Beijing government has been betting on to advance its development. Such a war could also, depending on how it started, trigger a widespread American boycott of Chinese goods—if China were to snuff out the Taiwanese democracy—which would lead to serious economic turmoil inside China.

The Dell Theory had its first real test in December 2004, when Taiwan held parliamentary elections. President Chen Shui-bian's pro-independence Democratic Progressive Party was expected to win the legislative runoff over the main opposition Nationalist Party, which favored closer ties with Beijing. Chen framed the election as a popular referendum on his proposal to write a new constitution that would formally enshrine Taiwan's independence, ending the purposely ambiguous status quo. Had Chen won and moved ahead on his agenda to make Taiwan its own motherland, as opposed to maintaining the status quo fiction that it is a province of the mainland, it could have led to a Chinese military assault on Taiwan. Everyone in the region was holding his or her breath. And what happened? *Motherboards won over motherland*. A majority of Taiwanese voted against the pro-independence governing party legislative candidates, ensuring that the DPP would not have a majority in parliament. I believe the message Taiwanese voters were sending was not that they never want Taiwan to be independent. It was that they do not want to upset the status quo right now, which has been so beneficial to so many Taiwanese. The voters seemed to understand clearly how interwoven they had become with the mainland, and they wisely opted to maintain their de facto independence rather than force de jure independence, which might have triggered a Chinese invasion and a very uncertain future.

Warning: What I said when I put forth the McDonald's theory, I would repeat even more strenuously with the Dell Theory: It does not make wars obsolete. And it does not guarantee that governments will not engage in wars of choice, even governments that are part of major supply chains. To suggest so would be naïve. It guarantees only that governments whose countries are enmeshed in global supply chains will have to think three times, not just twice, about engaging in anything but a war

of self-defense. And if they choose to go to war anyway, the price they will pay will be ten times higher than it was a decade ago and probably ten times higher than whatever the leaders of that country think. It is one thing to lose your McDonald's. It's quite another to fight a war that costs you your place in a twenty-first-century supply chain that may not come back around for a long time.

While the biggest test case of the Dell Theory is China versus Taiwan, the fact is that the Dell Theory has already proved itself to some degree in the case of India and Pakistan, the context in which I first started to think about it. I happened to be in India in 2002, when its just-in-time services supply chains ran into some very old-time geopolitics—and the supply chain won. In the case of India and Pakistan, the Dell Theory was working on only one party—India—but it still had a major impact. India is to the world's knowledge and service supply chain what China and Taiwan are to the manufacturing ones. By now readers of this book know all the highlights: General Electric's biggest research center outside the United States is in Bangalore, with seventeen hundred Indian engineers, designers, and scientists. The brain chips for many brand-name cell phones are designed in Bangalore. Renting a car from Avis online? It's managed in Bangalore. Tracing your lost luggage on Delta or British Airways is done from Bangalore, and the backroom accounting and computer maintenance for scores of global firms are done from Bangalore, Mumbai, Chennai, and other major Indian cities.

Here's what happened: On May 31, 2002, State Department spokesman Richard Boucher issued a travel advisory saying, "We urge American citizens currently in India to depart the country," because the prospect of a nuclear exchange with Pakistan was becoming very real. Both nations were massing troops on their borders, intelligence reports were suggesting that they both might be dusting off their nuclear warheads, and CNN was flashing images of people flooding out of India. The global American firms that had moved their back rooms and R & D operations to Bangalore were deeply unnerved.

"I was actually surfing on the Web, and I saw a travel advisory come

up on India on a Friday evening,” said Vivek Paul, president of Wipro, which manages backroom operations from India of many American multinationals. “As soon as I saw that, I said, ‘Oh my gosh, every customer that we have is going to have a million questions on this.’ It was the Friday before a long weekend, so over the weekend we at Wipro developed a fail-safe business continuity plan for all of our customers.” While Wipro’s customers were pleased to see how on top of things the company was, many of them were nevertheless rattled. This was not in the plan when they decided to outsource mission-critical research and operations to India. Said Paul, “I had a CIO from one of our big American clients send me an e-mail saying, ‘I am now spending a lot of time looking for alternative sources to India. I don’t think you want me doing that, and I don’t want to be doing it.’ I immediately forwarded his message to the Indian ambassador in Washington and told him to get it to the right person.” Paul would not tell me what company it was, but I have confirmed through diplomatic sources that it was United Technologies. And plenty of others, like American Express and General Electric, with back rooms in Bangalore, had to have been equally worried.

For many global companies, “the main heart of their business is now supported here,” said N. Krishnakumar, president of MindTree, another leading Indian knowledge outsourcing firm based in Bangalore. “It can cause chaos if there is a disruption.” While not trying to meddle in foreign affairs, he added, “What we explained to our government, through the Confederation of Indian Industry, is that providing a stable, predictable operating environment is now the key to India’s development.” This was a real education for India’s elderly leaders in New Delhi, who had not fully absorbed how critical India had become to the world’s knowledge supply chain. When you are managing vital backroom operations for American Express or General Electric or Avis, or are responsible for tracing all the lost luggage on British Airways or Delta, you cannot take a month, a week, or even a day off for war without causing major disruptions for those companies. Once those companies have made a commitment to outsource business operations or research to India, they expect it to stay there. That is a major commitment. And if geopolitics causes a serious disruption,

they will leave, and they will not come back very easily. When you lose this kind of service trade, you can lose it for good.

“What ends up happening in the flat world you described,” explained Paul, “is that you have only one opportunity to make it right if something [goes] wrong. Because the disadvantage of being in a flat world is that despite all the nice engagements and stuff and the exit barriers that you have, every customer has multiple options, and so the sense of responsibility you have is not just out of a desire to do good by your customers, but also a desire for self-preservation.”

The Indian government got the message. Was India’s central place in the world’s services supply chain the only factor in getting Prime Minister Vajpayee to tone down his rhetoric and step back from the brink? Of course not. There were other factors, to be sure—most notably the deterrent effect of Pakistan’s own nuclear arsenal. But clearly, India’s role in global services was an important additional source of restraint on its behavior, and it was taken into account by New Delhi. “I think it sobered a lot of people,” said Jerry Rao, who heads the Indian high-tech trade association. “We engaged very seriously, and we tried to make the point that this was very bad for Indian business. It was very bad for the Indian economy . . . [Many people] didn’t realize till then how suddenly we had become integrated into the rest of the world. We are now partners in a twenty-four by seven by three-sixty-five supply chain.”

Vivek Kulkarni, then information technology secretary for Bangalore’s regional government, told me back in 2002, “We don’t get involved in politics, but we did bring to the government’s attention the problems the Indian IT industry might face if there were a war.” And this was an altogether new factor for New Delhi to take into consideration. “Ten years ago, [a lobby of IT ministers from different Indian states] never existed,” said Kulkarni. Now it is one of the most important business lobbies in India and a coalition that no Indian government can ignore.

“With all due respect, the McDonald’s [shutting] down doesn’t hurt anything,” said Vivek Paul, “but if Wipro had to shut down we would affect the day-to-day operations of many, many companies.” No one would answer the phones in call centers. Many e-commerce sites that are supported

from Bangalore would shut down. Many major companies that rely on India to maintain their key computer applications or handle their human resources departments or billings would seize up. And these companies did not want to find alternatives, said Paul. Switching is very difficult, because taking over mission-critical day-to-day backroom operations of a global company takes a great deal of training and experience. It's not like opening a fast-food restaurant. That was why, said Paul, Wipro's clients were telling him, "I have made an investment in you. I need you to be very responsible with the trust I have reposed in you." And I think that created an enormous amount of back pressure on us that said we have to act in a responsible fashion . . . All of a sudden it became even clearer that there's more to gain by economic gains than by geopolitical gains. [We had more to gain from building] a vibrant, richer middle class able to create an export industry than we possibly could by having an ego-satisfying war with Pakistan." The Indian government also looked around and realized that the vast majority of India's billion people were saying, "I want a better future, not more territory." Over and over again, when I asked young Indians working at call centers how they felt about Kashmir or a war with Pakistan, they waved me off with the same answer: "We have better things to do." And they do. America needs to keep this in mind as it weighs its overall approach to outsourcing. I would never advocate shipping some American's job overseas just so it will keep Indians and Pakistanis at peace with one another. But I would say that to the extent that this process happens, driven by its own internal economic logic, it will have a net positive geopolitical effect. It will absolutely make the world safer for American kids.

Each of the Indian business leaders I interviewed noted that in the event of some outrageous act of terrorism or aggression from Pakistan, India would do whatever it takes to defend itself, and they would be the first to support that—the Dell Theory be damned. Sometimes war is unavoidable. It is imposed on you by the reckless behavior of others, and you have to just pay the price. But the more India and, one hopes, soon Pakistan get enmeshed in global service supply chains, the greater disincentive they have to fight anything but a border skirmish or a war of words.

The example of the 2002 India-Pakistan nuclear crisis at least gives us

some hope. That cease-fire was brought to us not by General Powell but by General Electric.

We bring good things to life.

INFOSYS VERSUS AL-QAEDA

Unfortunately, even GE can do only so much. Because, alas, a new source for geopolitical instability has emerged only in recent years, for which even the updated Dell Theory can provide no restraint. It is the emergence of mutant global supply chains—that is, nonstate actors, be they criminals or terrorists, who learn to use all the elements of the flat world to advance a highly destabilizing, even nihilistic agenda. I first started thinking about this when Nandan Nilekani, the Infosys CEO, was giving me that tour I referred to in Chapter 1 of his company's global videoconferencing center at its Bangalore headquarters. As Nandan explained to me how Infosys could get its global supply chain together at once for a virtual conference in that room, a thought popped into my head: Who else uses uploading and supply-chaining so imaginatively? The answer, of course, is al-Qaeda.

Al-Qaeda has learned to use many of the same instruments for global collaboration that Infosys uses, but instead of producing products and profits with them, it has produced mayhem and murder. This is a particularly difficult problem. In fact, it may be the most vexing geopolitical problem for flat-world countries that want to focus on the future. The flat world—unfortunately—is a friend of both Infosys and al-Qaeda. The Dell Theory will not work at all against these informal Islamo-Leninist terror networks, because they are not a state with a population that will hold its leaders accountable or with a domestic business lobby that might restrain them. These mutant global supply chains are formed for the purpose of destruction, not profit. They don't need investors, only recruits, donors, and victims. Yet these mobile, self-financing mutant supply chains use all the tools of collaboration offered by the flat world—uploading to raise

money, to recruit followers, and to stimulate and disseminate ideas; outsourcing to train recruits; and supply-chaining to distribute the tools and the suicide bombers to undertake operations. The U.S. Central Command has a name for this whole underground network: the Virtual Caliphate. And its leaders and innovators understand the flat world almost as well as Wal-Mart, Dell, and Infosys do.

In Chapter 15, I tried to explain that you cannot understand the rise of al-Qaeda emotionally and politically without reference to the flattening of the world. What I am arguing here is that you cannot understand the rise of al-Qaeda technically without reference to the flattening of the world, either. Globalization in general has been al-Qaeda's friend in that it has helped to solidify a revival of Muslim identity and solidarity, with Muslims in one country much better able to see and sympathize with the struggles of their brethren in another country—thanks to the Internet and satellite television. At the same time, as I pointed out, this flattening process has intensified the feelings of humiliation in some quarters of the Muslim world over the fact that civilizations to which the Muslim world once felt superior—Hindus, Jews, Christians, Chinese—are now all doing better than many Muslim countries, and everyone can see it. The flattening of the world has also led to more urbanization and large-scale immigration to the West of many of these young, unemployed, frustrated Arab-Muslim males, while simultaneously making it much easier for informal networks of these young men to form, operate, and interconnect. This certainly has been a boon for underground extremist Muslim political groups. There has been a proliferation of these informal mutual supply chains throughout the Arab-Muslim world today—small networks of people who move money through *hawalas* (hand-to-hand financing networks), who recruit through alternative education systems like the madrassas, and who communicate through the Internet and other tools of the global information revolution. Think about it: A century ago, anarchists were limited in their ability to communicate and collaborate with one another, to find sympathizers, and to band together for an operation. Today, with the Internet, that is not a problem. Today even the Unabomber could find friends to join a consortium where his “strengths” could be magnified and reinforced by others who had just as warped a worldview as he did.

What we have witnessed in Iraq is an even more perverse mutation of this mutant supply chain—the suicide supply chain. Since the start of the U.S. invasion in March 2003, hundreds of suicide bombers have been recruited from within Iraq and from across the Muslim world, brought to the Iraqi front by some underground railroad, connected with the bomb makers there, and then dispatched against U.S. and Iraqi targets according to whatever suits the daily tactical needs of the insurgent Islamist forces in Iraq. I can understand, but not accept, the notion that more than thirty-seven years of Israeli occupation of the West Bank might have driven some Palestinians into a suicidal rage. But the American occupation of Iraq was only a few months old before it started to get hit by this suicide supply chain. How do you recruit so many young men “off the shelf” who are ready to commit suicide in the cause of jihad, many of them apparently not even Iraqis? And they don’t even identify themselves by name or want to get credit—at least in this world. The fact is that Western intelligence agencies seem to have little clue how this underground suicide supply chain works, and it has basically stymied the U.S. armed forces in Iraq. From what we do know, though, this Virtual Caliphate works just like the supply chains I described earlier. Just as you take an item off the shelf in a discount store in Birmingham and another one is immediately made in Beijing, so the retailers of suicide deploy a human bomber in Baghdad and another one is immediately recruited and indoctrinated in Beirut. To the extent that this tactic spreads, it will require a major rethinking of U.S. military doctrine.

The flat world has also been such a huge boon for al-Qaeda and its ilk because of the way it enables the small to act big, and the way it enables small acts—the killing of just a few people—to have big effects. The horrific video of the beheading of *Wall Street Journal* reporter Danny Pearl by Islamist militants in Pakistan was transmitted by the Internet all over the world. There is not a journalist anywhere who saw or even just read about that who was not terrified. But those same beheading videos are also used as tools of recruitment. The flat world makes it much easier for terrorists to transmit their terror. With the Internet they don’t even have to go through Western or Arab news organizations but can broadcast right into your computer. It takes much less dynamite to transmit so much more

anxiety. Just as the U.S. Army had embedded journalists, so the suicide supply chain has embedded terrorists, in their own way, to tell us their side of the story. How many times have I gotten up in the morning, fired up the Internet, and been confronted by the video image of some masked gunman threatening to behead an American—all brought to me courtesy of AOL's home page? The Internet is an enormously useful tool for the dissemination of propaganda, conspiracy theories, and plain old untruths, because it combines a huge reach with a patina of technology that makes anything on the Internet somehow more believable.

“The new system of diffusion—the Internet—is more likely to transmit irrationality than rationality,” said political theorist Yaron Ezrahi, who specializes in the interaction between media and politics. “Because irrationality is more emotionally loaded, it requires less knowledge, it explains more to more people, it goes down easier.” That is why conspiracy theories are so rife in the Arab-Muslim world today—and unfortunately are becoming so in many quarters of the Western world, for that matter. Conspiracy theories are like a drug that goes right into your bloodstream, enabling you to see “the Light.” And the Internet is the needle. Young people used to have to take LSD to escape. Now they just go online. Now you don't shoot up, you download. You download the precise point of view that speaks to all your own biases. And the flat world makes it all so much easier.

In many cases, networks like al-Qaeda use the Internet—not only for easy, cheap, global command and control but, even more important, as a global megaphone to radiate ideas. Indeed, some Islamist radical movements have no real command and control and don't even pretend that they do. They simply disseminate their ideas globally, using the flat-world platform, and inspire and exhort people to use their own local capacity to take initiatives—to blow up a train in Spain or a subway in London. There are no orders going from a single headquarters to the field, just inspiration and maybe some training. The locals do the rest on their own.

Gabriel Weimann, a professor of communications at Haifa University, Israel, did an incisive study of terrorists' use of the Internet, which was published in March 2004 by the United States Institute of Peace and

excerpted on YaleGlobal Online on April 26, 2004. He made the following points:

While the danger that cyber-terrorism poses to the Internet is frequently debated, surprisingly little is known about the threat posed by terrorists' use of the Internet. A recent six-year-long study shows that terrorist organizations and their supporters have been using all of the tools that the Internet offers to recruit supporters, raise funds, and launch a worldwide campaign of fear. It is also clear that to combat terrorism effectively, mere suppression of their Internet tools is not enough. Our scan of the Internet in 2003–04 revealed the existence of hundreds of websites serving terrorists in different, albeit sometimes overlapping, ways . . . There are countless examples of how [terrorists] use this uncensored medium to spread disinformation, to deliver threats intended to instill fear and helplessness, and to disseminate horrific images of recent actions. Since September 11, 2001, al-Qaeda has festooned its websites with a string of announcements of an impending "large attack" on US targets. These warnings have received considerable media coverage, which has helped to generate a widespread sense of dread and insecurity among audiences throughout the world and especially within the United States . . .

The Internet has significantly expanded the opportunities for terrorists to secure publicity. Until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. The fact that terrorists themselves have direct control over the content of their websites offers further opportunities to shape how they are perceived by different target audiences and to manipulate their image and the images of their enemies. Most terrorist sites do not celebrate their violent activities. Instead—regardless of their nature, motives, or location—most terrorist sites emphasize two issues: the restrictions placed on freedom of expression; and the plight of their comrades who are now political prisoners.

These issues resonate powerfully with their own supporters and are also calculated to elicit sympathy from Western audiences that cherish freedom of expression and frown on measures to silence political opposition . . .

Terrorists have proven not only skillful at online marketing but also adept at mining the data offered by the billion-some pages of the World Wide Web. They can learn from the Internet about the schedules and locations of targets such as transportation facilities, nuclear power plants, public buildings, airports and ports, and even counterterrorism measures. According to Secretary of Defense Donald Rumsfeld, an al-Qaeda training manual recovered in Afghanistan tells its readers, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy." One captured al-Qaeda computer contained engineering and structural architecture features of a dam, which had been downloaded from the Internet and which would enable al-Qaeda engineers and planners to simulate catastrophic failures. In other captured computers, U.S. investigators found evidence that al-Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transportation, and communications grids.

Like many other political organizations, terrorist groups use the Internet to raise funds. Al-Qaeda, for instance, has always depended heavily on donations, and its global fundraising network is built upon a foundation of charities, nongovernmental organizations, and other financial institutions that use websites and Internet-based chat rooms and forums. The fighters in the Russian breakaway republic of Chechnya have likewise used the Internet to publicize the numbers of bank accounts to which sympathizers can contribute. And in December 2001, the U.S. government seized the assets of a Texas-based charity because of its ties to Hamas.

In addition to soliciting financial aid online, terrorists recruit converts by using the full panoply of website technologies (audio,

digital video, etc.) to enhance the presentation of their message. And like commercial sites that track visitors to develop consumer profiles, terrorist organizations capture information about the users who browse their websites. Visitors who seem most interested in the organization's cause or well suited to carrying out its work are then contacted. Recruiters may also use more interactive Internet technology to roam online chat rooms and cyber cafes, looking for receptive members of the public, particularly young people. The SITE Institute, a Washington, D.C.-based terrorism research group that monitors al-Qaeda's Internet communications, has provided chilling details of a high-tech recruitment drive launched in 2003 to recruit fighters to travel to Iraq and attack U.S. and coalition forces there. The Internet also grants terrorists a cheap and efficient means of networking. Many terrorist groups, among them Hamas and al-Qaeda, have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells that have no single commanding hierarchy. Through the Internet, these loosely interconnected groups are able to maintain contact with one another—and with members of other terrorist groups. The Internet connects not only members of the same terrorist organizations but also members of different groups. For instance, dozens of sites supporting terrorism in the name of jihad permit terrorists in places as far removed from one another as Chechnya and Malaysia to exchange ideas and practical information about how to build bombs, establish terror cells, and carry out attacks . . . Al-Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks.

For all of these reasons we are just at the beginning of understanding the geopolitical impact of the flattening of the world. On the one hand, failed states and failed regions are places we have every incentive to avoid today. They offer no economic opportunity and there is no Soviet Union out there competing with us for influence over such countries. On the other hand, there may be nothing more dangerous today than a failed

state with broadband capability. That is, even failed states tend to have telecommunications systems and satellite links, and therefore if a terrorist group infiltrates a failed state, as al-Qaeda did with Afghanistan, it can amplify its power enormously. As much as big powers want to stay away from such states, they may feel compelled to get even more deeply embroiled in them. Think of America in Afghanistan and Iraq, Russia in Chechnya, Australia in East Timor.

In the flat world it is much more difficult to hide, but much easier to get connected. "Think of Mao at the beginning of the Chinese Communist revolution," remarked Michael Mandelbaum, the Johns Hopkins foreign policy specialist. "The Chinese Communists had to hide in caves in northwest China, but they could move around in whatever territory they were able to control. Bin Laden, by contrast, can't show his face, but he can reach every household in the world, thanks to the Internet." Bin Laden cannot capture any territory, but he can capture the imagination of millions of people. And he has, broadcasting right into American living rooms on the eve of the 2004 presidential election.

Hell hath no fury like a terrorist with a satellite dish and an interactive Web site.

TOO PERSONALLY INSECURE

In the fall of 2004, I was invited to speak at a synagogue in Woodstock, New York, not far from Yasgur's farm, home of the famous Woodstock music festival. I asked my hosts how was it that they were able to get a synagogue in Woodstock, of all places, big enough to support a lecture series. Very simple, they said. Since 9/11, Jews, and others, have been moving from New York City to places like Woodstock, to get away from what they fear will be the next ground zero. Right now this trend is a trickle, but it would become a torrent if a nuclear device were detonated in any European or American city.

Since this threat is the mother of all unflatteners, this book would not be complete without a discussion of it. We can live with a lot. We lived

through 9/11. But we cannot live with nuclear terrorism. That would unflatten the world permanently.

The only reason that Osama bin Laden did not use a nuclear device on 9/11 was not that he did not have the intention but that he did not have the capability. And since the Dell Theory offers no hope of restraining the suicide supply chains, the only strategy we have is to limit their worst capabilities. That means a much more serious global effort to stanch nuclear proliferation by limiting the supply—to buy up the fissile material that is already out there, particularly in the former Soviet Union, and prevent more states from going nuclear. Harvard University international affairs expert Graham Allison, in his book *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, outlines just such a strategy for denying terrorists access to nuclear weapons and nuclear materials. It can be done, he insists. It is a challenge to our will and convictions, but *not to our capabilities*. Allison proposes a new American-led international security order to deal with this problem based on what he calls “a doctrine of the Three No’s: No loose nukes, No new nascent nukes, and No new nuclear states.” No loose nukes, says Allison, means locking down all nuclear weapons and all nuclear material from which bombs could be made—in a much more serious way than we have done up till now. “We don’t lose gold from Fort Knox,” says Allison. “Russia doesn’t lose treasures from the Kremlin armory. So we both know how to prevent theft of those things that are super valuable to us if we are determined to do it.” No new nascent nukes means recognizing that there is a group of actors out there who can and do produce highly enriched uranium or plutonium, which is nothing more than nuclear bombs just about to hatch. We need a much more credible, multilateral nonproliferation regime that soaks up this fissile material. Finally, no new nuclear states means “drawing a line under the current eight nuclear powers and determining that, however unfair and unreasonable it may be, that club will have no more members than those eight,” says Allison, adding that these three steps might then buy us time to develop a more formal, sustainable, internationally approved regime.

It would be nice also to be able to deny the Internet to al-Qaeda and its ilk, but that, alas, is impossible—without undermining ourselves.

That is why limiting their capabilities is necessary but not sufficient. We also have to find a way to get at their worst intentions. If we are not going to shut down the Internet and all the other creative and collaborative tools that have flattened the world, and if we can't restrict access to them, the only thing we can do is try to influence the imagination and intentions that people bring to them and draw from them. When I raised this issue, and the broad themes of this book, with my religious teacher, Rabbi Tzvi Marx from Holland, he surprised me by saying that the flat world I was describing reminded him of the story of the Tower of Babel.

How so? I asked. "The reason God banished all the people from the Tower of Babel and made them all speak different languages was not because he did not want them to collaborate *per se*," answered Rabbi Marx. "It was because he was enraged at what they were collaborating on—an effort to build a tower to the heavens so they could become God." This was a distortion of the human capacity, so God broke their union and their ability to communicate with one another. Now, all these years later, humankind has again created a new platform for more people from more places to communicate and collaborate with less friction and more ease than ever: the Internet. Would God see the Internet as heresy?

"Absolutely not," said Marx. "The heresy is not that mankind works together—it is to what ends. It is essential that we use this new ability to communicate and collaborate for the right ends—for constructive human aims and not megalomaniacal ends. Building a tower was megalomaniacal. Bin Laden's insistence that he has the truth and can flatten anyone else's tower who doesn't heed him is megalomaniacal. Collaborating so mankind can achieve its full potential is God's hope."

How we promote more of that kind of collaboration is what the final chapter is all about.