Part I

THE FUTURE OF WAR IS NOW

1

THE SUPEREMPOWERED COMPETITION

The near future holds mind-bending promise for American business.[1] Globalization is prying open vast new markets. Technology is plowing ahead, fueling—and transforming—entire industries, creating services we never thought possible. Clever people worldwide are capitalizing every which way. But because globalization and technology are morally neutral forces, they can also drive change of a different sort. We saw this very clearly on September 11, 2001, and are seeing it now in Iraq and in conflicts around the world. In short, despite the aura of limitless possibility, our lives are evolving in ways we can control only if we recognize the new landscape. It's time to take an unblinking look.

We have entered the age of the faceless, agile enemy. From London to Madrid to Nigeria to Russia, stateless terrorist groups have emerged to score blow after blow against us. Driven by cultural fragmentation, schooled in the most sophisticated technologies, and fueled by transnational crime, these groups are forcing corporations and individuals to develop new ways of defending themselves.

The end result of this struggle will be a new, more resilient approach to national security, one built not around the state but around private citizens and companies. That new system will change how we live and work—for the better, in many ways—but the road getting there may seem long at times.

The conflict in Iraq has foreshadowed the future of global security in much the same way that the Spanish civil war prefigured World War II: it's become a testing ground, a dry run for something much larger. Unlike previous insurgencies, the one in Iraq comprises seventy-five to one hundred small, diverse, and autonomous groups of zealots, patriots, and criminals alike. These groups, of course, have access to many of the same tools we do—from satellite phones to engineering degrees—and they use them every bit as effectively. But their single most important asset is their organizational structure, an open-source community network—one that seems to me quite similar to what we see in the software industry. That's how they're able to continually stay one step ahead of us. It is an extremely innovative structure, sadly, and it results in decision-making cycles much shorter than those of the U.S. military. Indeed, because the insurgents in Iraq lack a recognizable center of gravity—a leadership structure or an ideology—they are nearly immune to the application of conventional military force. Like Microsoft, the software superpower, the United States hasn't found its match in a Goliath competitor similar to itself, but in a loose, self-tuning network.

In Iraq, we've also witnessed the convergence of international crime and terrorism as they provide ample fuel and a global platform for these new enemies. Al-Qaeda's attack on Madrid, for example, was funded by the sale of the drug ecstasy. Moisés Naim, a former Venezuelan minister of trade and industry and the editor and publisher of the magazine *Foreign Policy,* documented this trend in his insightful book *Illicit: How Smugglers, Traffickers, and Copycats Are Hijacking the Global Economy.* Globalization has fostered the development of a huge criminal economy that boasts a technologically leveraged global supply chain (like Wal-Mart's) and can handle everything from human trafficking (eastern Europe) to illicit drugs (Asia and South America), pirated goods (Southeast Asia), arms (Central Asia), and money laundering (everywhere). Naim puts the value of that economy at between $2 and $3 trillion a year. He says it is expanding at *seven times* the rate of legitimate world trade.

This terrorist-criminal symbiosis becomes even more powerful when considered next to the most disturbing sign coming out of Iraq: the terrorists have developed the ability to fight nation-states strategically—without weapons of mass destruction. This new method is called *systems disruption,* a simple way of attacking the critical networks (electricity, oil, gas, water, communications, and transportation) that underpin modern life. Such disruptions are designed to erode the target state's legitimacy, to drive it to failure by keeping it from providing the services it must deliver in order to command the allegiance of its citizens. Over the past two years, attacks on the oil and electricity networks in Iraq have reduced and held delivery of these critical services below prewar levels, with a disastrous effect on the country, its people, and its economy.

The early examples of systems disruption in Iraq and elsewhere are ominous. If these techniques are even lightly applied to the fragile electrical and oil-gas systems in Russia, Saudi Arabia, or anywhere in the target-rich West, we could see a rapid onset of economic and political chaos unmatched since the advent of the blitzkrieg. (India's January arrest of militants with explosives in Hyderabad suggests that the country's high-tech industry could be a new target.) It's even worse when we consider the asymmetry of the economics involved: one small attack on an oil pipeline in southeast Iraq, conducted for an estimated $2,000, cost the Iraqi government more than $500 million in lost oil revenues. That is a return on investment of 25 million percent.

Now that the tipping point has been reached, the rise of global virtual states—with their thriving criminal economies, innovative networks, and hyperefficient war craft—will rapidly undermine public confidence in our national-security systems. In fact, this process has already begun. We've seen disruption of our oil supply in Iraq, Nigeria, Venezuela, and Colombia; the market's fear of more disruptions contributes mightily to the current high prices for oil. As these disruptions continue, the damage will spill over into the very structure of our society. Our profligate U.S. Department of Defense, reeling from its inability to defend our borders on 9/11 or to pacify even a small country like Iraq, will increasingly be seen as obsolete.

Technological Multipliers

> Accustomed to living with almost routine scientific breakthroughs, we have yet to come to terms with the fact that the most compelling 21st-century technologies—robotics, genetic engineering, and nanotechnology—pose a different threat than the technologies that have come before. Specifically, robots, engineered organisms, and nanobots share a dangerous amplifying factor: They can self-replicate. A bomb is blown up only once—but one bot can become many, and quickly get out of control.
>
> —Bill Joy, cofounder and chief scientist of Sun Microsystems[2]

From a security perspective, the most disturbing aspect of 9/11 wasn't the horrible destruction, but that the men who attacked us on that day didn't even factor the opposition of the U.S. military into their planning. Despite tens of trillions of dollars spent on defense over the last decades, this military force proved ineffectual as a deterrent at the point when we needed it most.

Worse yet, nothing has changed since then. The U.S. military, in budget after budget since 9/11, has continued to plan, build, and fund forces dedicated to fighting a great power war—with an increasing emphasis on China and to a lesser extent Iran. Even the guerrilla war in Iraq hasn't forced any substantive changes to our defense structure. This isn't due to a nefarious plot at the highest levels of government. It is due to the fundamental inability of the nation-state to conceptualize a role that makes sense in fighting and deterring the emerging threat.

The real threat, as seen in the rapid rise in global terrorism over the past five years, is that this threat isn't another state but rather the superempowered group. This group, riding on the leverage provided by rapid technology improvement and global integration, is and will remain the major threat to our way of life.

To really understand this future, you need to discard the idea of state-versus-state conflict. That age is over. It ended with the rise of nuclear weapons, the integration of the world's economies, and the end of the cold war. Wars between states are now, for all intents and purposes, obsolete. The real remaining threat posed by wars between states, in those rare cases when they do occur by choice, is that they will create a vacuum within which these nonstate groups can thrive. Every time we shuffle the playing cards with state-versus-state conflict, we will find that we are ultimately less well off than before it occurred.

Given the withering away of state-versus-state conflict, we shouldn't assume that the reasons for warfare have departed with it. All the economic, environmental, social, religious, and ethnic drivers of conflict are still in place. In fact, there is every reason to believe they actually may be strengthening, given the fragmenting power of the Internet. The real change is that wars fought over these issues won't be fought by states, but at a level below that of the state.

This new granular level, the realm of superempowered groups, is where the seeds of epochal conflict now reside. Unfortunately, as demonstrated by 9/11 and Iraq, these groups have now gained the ability to wage war on states and win. How this came about should sound familiar. It leverages the tools you use every day.

The rise of superempowered groups is part of a larger historical trend. This trend is in the process of putting ever-more-powerful technological tools and the knowledge of how to use them into an ever-increasing number of hands. Economically, this is fantastic news. This transfer of technological leverage means faster productivity growth and improvements in incomes. Within the context of war, however, this is dire news, because this trend dictates that technology will leverage the ability of individuals and small groups to wage war with equal alacrity.

Within this larger context, the conflict we are currently engaged in is merely a waypoint on this trend line. The threshold necessary for small groups to conduct warfare has finally been breached, and we are only starting to feel its effects. Over time, perhaps in as little as twenty years, and as the leverage provided by technology increases, this threshold will finally reach its culmination—*with the ability of one man to declare war on the world and win*. Now, with every improvement in genetic engineering and nanotechnology (only some of many potential threats), we come closer to the day when a single individual will have the budget, the knowledge, and the tools necessary to make this future possible.

Years ago, I had a college physics instructor who was on leave from his primary job: designing nuclear weapons for the military. He was, and likely still is, a tightly controlled person. The knowledge he held in his head was dangerous, and as a result the government carefully controlled his movements. Those days of tight control are quickly ending, however. The knowledge of dangerous technologies that was typically harnessed and closely monitored by the government is quickly proliferating beyond its control. This knowledge is now becoming something a great many people will possess and be able to use. Furthermore, this knowledge is now global, driven by the winds of ever-increasing interconnectivity.

The root of this transformation is the accelerating rate of change in the power of ubiquitously available technology. Over the last twenty years or so, the ability to manipulate and use technology has decentralized to become widely accessible. Not only are the tools accelerating in power but also the breadth of access to these tools has become nearly universal.

Technology's Paradox

It's well known that technology can be used for both good and bad ends. The classic example of this is nuclear power (although many would argue that it is entirely bad). Under the classic rules of this paradox, these rogue technologies occurred only rarely and required a nation-state to produce them.

Today's rules are different. Technology is now rapidly advancing across a broad front, and the barriers to usage have dropped to nothing. A recent example of this new rule set is Japan's realization that Sony's PlayStation 2 console has sufficient graphics-crunching capability to pilot a missile to its desired target.[3] In essence, anyone can now buy a critical component for an advanced weapons guidance system on eBay for $200.

The reason for this breakout from technology's historically glacial and seemingly linear pace of improvement is Moore's law. Named for a claim made by Gordon E. Moore, the cofounder of Intel in the 1960s, Moore's law states that the number of transistors on a computer chip (integrated circuit) doubles every eighteen months.

Moore was right, and this exponential pace of improvement has been holding steady within this technology cycle since the middle of the twentieth century. In fact, the technologist Ray Kurzweil has shown that it reaches back to technology cycles before the integrated circuit as well. It is only now making its effects known, as the curve of this exponential rate of improvement breaks above the horizon of linear progress.

Furthermore, since this improvement was packaged in a product that is globally accessible (the computer chip), Moore's law has now begun to permeate every field of technology. For the purposes of our discussion, the fact that Moore's law is packaged in an affordable form means that the tools available to individuals are also improving at an exponential pace. You can now run programs on your laptop that previously would have taken a team of accountants, a laboratory of biologists, a pool of secretaries, or a group of engineers to accomplish.

Right behind Moore's law is a second inexorable trend. That trend is the increasing power and complexity provided by a ubiquitous global network. That network, of course, is the Internet, and its most important application, the World Wide Web, is an example of the reverse of the dual use of technology since the Internet started within the Department of Defense. Again, within economic terms this is a cornucopia of plenty, powering a bewildering, complex array of global goods and services. Within the context of warfare, however, it takes a different form altogether.

The leverage provided by these technologies has finally reached a point where small superempowered groups, and not yet individuals, now have the capability to challenge the state in warfare and win. For the most part, these nonstate groups have been using these new technologies mostly as a means to recruit, train, equip, and mobilize decentralized organizations. A more ominous trend has developed, however. These groups are quickly learning to use—against us—the technologies we use daily.

Airplanes are being turned into flying bombs, cell phone networks are being used to simultaneously detonate bombs from miles away, and critical computer networks are being hacked. More important, a growing number of attacks are being made on the underlying computerized networks that support our very economic fabric: from the oil distribution system to electricity grids. If this is what we are already seeing with the first iteration of this trend, then it is a safe bet that the capability to instantly leverage the rapid technological progress under way will soon be dangerous enough to threaten the world with catastrophe.

It's my belief that our response to the threats posed by the superempowered groups that we face today will define our survivability against the threat of extermination in the future. If we continue to expect the next major terrorist attack to look just like the last one, the odds will not be in our favor.