1

Introduction

"Eternal vigilance is the price of liberty." —Wendell Phillips

The Great Awakening

> *These are extraordinary times. And we face an extraordinary challenge. Our strength as well as our convictions have imposed upon this nation the role of leader in freedom's cause. No role in history could be more difficult or more important. We stand for freedom.... The great battleground for the defense and expansion of freedom today is the whole southern half of the globe—Asia, Latin America, Africa and the Middle East.... Yet [our opponents'] aggression is more often concealed than open. They have fired no missiles; and their troops are seldom seen. They send arms, agitators, aid, technicians and propaganda to every troubled area. But where fighting is required, it is usually done by others—by guerrillas striking at night, by assassins striking alone—assassins who have taken the lives of four thousand civil officers in the last twelve months in Vietnam alone—by subversives and saboteurs and insurrectionists, who in some cases control whole areas inside of independent nations.*

The reference to Vietnam is the only thing that differentiates this portion of John F. Kennedy's 1961 State of the Union address from one that might be heard today. Since the 1960s the nature of war and of national security has changed drastically. JFK sought a way to address a world where terrorism and unconventional warfare were the rule and not the exception.

America had—and still has—the strongest conventional and nuclear military in the world, but JFK realized that its ability to address these new threats was limited. He requested funds for a variety of programs to increase national security. Perhaps the most long lasting of these programs was the further establishment and expansion of the Special Forces, which have been a keystone of America's strategy in every conflict since.

Two years before Kennedy's address, in California, Richard Feynman, a Nobel Prize–winning physicist and one of the century's great scientific visionaries, was giving a very different speech:

> *I would like to describe a field in which little has been done, but in which an enormous amount can be done in principle. This field is not quite the same as the others in that it will not tell us much of fundamental physics (in the sense of, 'What are the strange particles?') but it is more like solid-state physics in the sense that it might tell us much of great interest about the strange phenomena that occur in complex situations. Furthermore, a point that is most important is that it would have an enormous number of technical applications. What I want to talk about is the problem of manipulating and controlling things on a small scale.*
>
> *As soon as I mention this, people tell me about miniaturization, and how far it has progressed today. They tell me about electric motors that are the size of the nail on your small finger. And there is a device on the market, they tell me, by which you can write the Lord's Prayer on the head of a pin. But that's nothing; that's the most primitive, halting step in the direction I intend to discuss. It is a staggeringly small world that is below. In the year 2000, when they look back at this age, they will wonder why it was not until the year 1960 that anybody began seriously to move in this direction.*

Feynman went on to lay out his vision for this entirely new field. He described computers that could adapt to changing circumstances, primitive artificial intelligence, and data storage that could put the contents of every book in the California

Institute of Technology library onto a single library card. Moreover, he spoke of dozens of applications for this new field that hinged on the ability to manipulate matter at its ultimate scale, atom-by-atom and molecule-by-molecule. This was in the days when vacuum tubes were common, and computers were the size of a whole room yet less powerful than a modern cellular phone.

The challenge was not taken up immediately. Instead, miniaturization continued to take its "primitive, halting steps" forward toward the information technology revolution in the 1990s. It wasn't until close to the year 2000 (as Feynman foretold with uncanny accuracy) that new tools to see and work at the level of atoms and molecules became widely available. At around the same time, it became clear that microchips could not continue to be improved by evolving current techniques. Feynman's science of the very small suddenly became both possible and necessary. It became known as nanoscience, and its applications became known as nanotechnology.

On September 11, 2001, America became the victim of the most violent terrorist attack it had yet endured—an attack carried out by fewer than 20 men using knives and box cutters killed more than 3,000 people in New York, Pennsylvania, and Washington, D.C. The attacks broke the nation's heart and forced its citizens to reconsider many of JFK's observations. How can a country protect itself against forces that, while possibly state-sponsored, are not the troops of a sovereign nation? How do we protect our children, airplanes, roads, schools, buildings, and infrastructure against the threat of terrorism?

Terrorism was not new to America. The World Trade Center had been bombed before, Pan Am flight 103 was hijacked, Al Capone bombed businesses that would not pay protection money, the Unabomber sent explosives to leading scientists, and Timothy McVeigh attacked the Oklahoma City Federal Building. Nonetheless, an attack of the size and scope of 9/11—carried out just as America's economy was entering a recession after its euphoric "tech bubble" years—resulted in a great awakening to the fact that all was not right in the world and that we were not, even on our home soil, anywhere near so safe and omnipotent as we had thought.

The 2003 war in Iraq has brought these points into even sharper focus. If terrorists or countries sponsoring terror also possess chemical and biological weapons, what can we do to defend our troops and our cities? If our only mode of response to a terrorist attack is to invade an entire nation, how do we protect our people at home from revenge attacks, and how do we assure the safety of innocent civilians in the countries we invade? How do we work quickly and cleanly to avoid having matters spiral out of control the way they did when a terrorist's bullet started World War I? And finally, how do we find and stop the individuals, such as Osama bin Laden or Saddam Hussein, who are most responsible?

The government's initial responses to these problems—the formation of a unified Department of Homeland Security; a new Transportation Security Administration; increased funding for local police, fire departments, and other "first responders"; and a renewed emphasis on intelligence gathering and interagency coordination—were important but not sufficient. Faced with the grim possibilities of chemical or biological attacks and with the increased threats of terrorism brought about by the wars in Iraq and Afghanistan, some of these multibillion dollar agencies did little more than increase the national threat advisory level, recommend limited inoculation for some common bioagents such as anthrax and smallpox, and suggest that citizens purchase duct tape and plastic sheeting to create a protected room at home.

None of these precautions were terribly helpful or workable. Few civilians understood the obscure color-coded system of the national threat advisory level, and they were given no practical recommendations for heightening their security when the level was increased, other than to curtail travel and other unnecessary activities, such as shopping—something which did not help a depressed economy. Sealing rooms with plastic sheeting and duct tape would do little or no good in the case of attack, since any room that will seal out toxins will also seal out breathable air. Inoculation regimens for certain biological agents made a bit more sense, but there are so many different biotoxins and biotoxin strains that inoculating against all of them is impossible. Finally, renewed intelligence efforts have certainly helped in catching terrorists, but they also resulted in policies such as the USA Patriot Act and the proposed Total Information Awareness Act that may destroy the very freedoms and liberties we are trying to protect. As Benjamin Franklin, scientist and politician, remarked, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

In the battlefield, the situation is little better than in the homeland scenario we have just discussed. When facing the threat of chemical or biological attack, soldiers had either to wear thick chemical defense suits, which were similar in weight and comfort to SCUBA suits and made desert fighting next to impossible, or to take their chances in the face of these serious threats.

While the search for long-term solutions to these problems continues, what America and all the other nations of the free world need is an arsenal of "silver bullet" technologies that address these very specific needs. The military needs lightweight uniforms that allow troops to fight in the desert while protecting them from bullets, shrapnel, chemical gases, and biological toxins. It also needs better smart munitions; improved stealth features; tougher, lighter vehicles and battle gear; more unmanned combat capabilities; and better battlefield information systems that emphasize smaller units well inside hostile territory. UN inspectors need to be able to find and trace weapons of mass destruction quickly and efficiently. Water treatment facilities, mail sorting rooms, and transportation centers need sensors that can find explosives and other dangerous cargoes immediately, in small quantities, and without error. First responders need substances that can neutralize chemical and biological warfare agents. Doctors need treatments to help those who have been exposed. Industry needs more secure and robust communications and computer systems. Law enforcement agencies need better capability to identify, intercept, and decode information from potentially hostile groups. And everyone needs new economic drivers and alternative sources of clean, cheap energy that will solve environmental problems and reduce our dependence on the foreign oil that so often comes from troubled parts of the world.

All of these things and many, many more are being made possible by nanoscience and nanotechnology, converging the visions of Feynman and JFK. These sciences have prompted Clifford Lau, director of the Office of Basic Research at the U.S. Department of Defense, to say that nanotechnology will eventually alter warfare more than the invention of gunpowder. While policy and the people in all the uniformed services are crucial to security, without the tools made possible by nanotechnology, the world may not be much safer than it was before September 11th. With the first wave of intense fighting in Iraq and Afghanistan over, the urgency of these issues may seem to have diminished. It has not. Complacency in the wake of victory is among the most dangerous mistakes to make in war. Security is a long-term problem, and though it may not be the sole obsession of most citizens (as it has been during most periods of human history), it remains a great concern and the first duty of government.

The Case for Nanotechnology

Nanotechnology has immediate applications for defense and security, and they are the focus of this book, but it also has broader possibilities that will eventually touch every aspect of our lives. Many of the applications discussed here will have a profound impact on how we deal with disease outbreaks such as AIDS or SARS. Energy production, environmental repair and remediation, and advanced computing are also so-called dual-use applications, where industry and the military can pool resources for mutual benefit. There is also a host of completely nonmilitary applications—nanotechnology is already used for making better clothing, sports equipment, and treatments for diseases from diabetes to cancer—but much of that is beyond the scope of this book. Still, the applications abound. As Shimon Peres, former prime minister of Israel, observed, "That which has been achieved by the atomic bomb in the field of military strategy will be accomplished in the future by nanotechnology in the field of civil potential."

Unfortunately, technology is often a double-edged sword. The cellular phones and airplanes that are so much a part of everyday life were also necessary elements to the terrorists' plot on 9/11. Nanotechnology could be the same. Never before has a single branch of technology promised to be so transforming or powerful, nor has a technological revolution happened so quickly. It is of enormous importance that we examine both the promise and perils of nanotechnology and that we embark on this task quickly, with our full attention.

With the first nanotechnology products already appearing on store shelves and on the battlefield, we cannot afford to wait.

There has been a great deal of hype about nanotechnology. Enthusiasts say that it will solve all the world's problems, from ending hunger to achieving eternal life. Critics cite concerns ranging from regulatory and intellectual property issues to the idea of "gray goo," usually meaning nanotechnology-enabled, self-aware, self-replicating machines that would ultimately take over the world. Different views of nanotechnology inform movies, TV, and science fiction from *Star Trek* and the *X-Files* to Michael Crichton's thriller *Prey.* Almost none of these portray what nanotechnology is really about. Nanoscience is not the science of creating invisible robots to assemble kitchen sinks out of the air or to invade a human body. It is the science of utilizing the unique properties of the design scale of nature to make materials and perform functions that could not be made or performed any other way. While it might be exaggerating to say that nanobots (those tiny, invisible robots) are absolutely impossible, there is a compelling body of evidence showing that their near-term development is extraordinarily unlikely.

Criticism of nanotechnology also takes another form. Many observers point out that while there has been a great deal of hype and a reasonable amount of investment in nanoscience and nanotechnology (governments and private firms worldwide spent some $4 billion on these fields in 2002, though less than half of the total was spent in the U.S.), there are few nanotechnology products to justify the excitement. This is unfair and a bit premature. While $1 billion may sound like a great deal of money, it is widely distributed for a host of new applications, and it is less than the military often spends to develop a single new weapons system. (Ballistic missile defense, for example, consumes some $8 billion per year with far fewer results.) It is less than 3% of the cost of the war in Iraq. And it is smaller than the internal R&D budgets of some individual pharmaceutical firms. In military development terms, nanotechnology still has a very small budget and a small program, but it is growing rapidly.

There are other flaws in the argument that nanotechnology is more hype than substance. Most of the dollars spent to date have been on fundamental research, and it may take several years to develop the results into useful products. Also, some heavy-hitting, nanotechnology-based products are already on the market: zeolite technology for oil refining currently saves the U.S. some 400 million barrels of oil a year, and GMR (giant magneto-resistance) technology is what makes multi-gigabyte computer hard drives possible. Since not all nanotechnology products have labels saying "Nano Inside," it is sometimes difficult for consumers to know which products are nano-enabled and which are not. However, with the U.S. defense budget above $400 billion per year, and the combined market impact of global defense and energy at more than $4 trillion, if nanotechnology achieves its expected impact over the next 10 years in these sectors alone, the National Science Foundation's estimate that it will be a $1 trillion industry by 2015 could, if anything, be rather low.

This book examines some of the more immediate and key areas of nanoscience and nanotechnology as they apply to homeland security and to national defense. It emphasizes the capabilities of these new fields and makes some recommendations for integrating them into policy while avoiding the perils they pose. There is also a significant section on the ethical aspects of nanotechnology. The book is intended to be almost entirely nontechnical except to the extent that is necessary to explain the basic ideas. For a more general description of nanotechnology, more detail on how it works, or more analysis of the business of nanotechnology, we encourage you to read our previous book, *Nanotechnology: A Gentle Introduction to the Next Big Idea* (Prentice Hall, 2002).