STRATEGIC STUDIES QUARTERLY

Deterring Emergent Technologies

Col John P. Geis II, USAF, Retired
Col Theodore C. Hailes, USAF, Retired

Abstract

This article examines the implications of emerging technological change on the multiplicity of future threats. Specifically, it examines the relevance of deterrence theory to both existing and new threats, some of which may surpass nuclear weapons in the risk they pose to the United States and humankind. It assumes science and technology growth will continue and will drive proliferation of advanced and potentially dangerous technologies. Rapid advances in biotechnology, nanotechnology, and directed energy may prove to be particularly dangerous. Deterring threats posed by nations, groups, and individuals will require new thinking regarding the application of deterrence theory—particularly deterrence by denial. The article concludes that groups and individuals will continue to gain access to new capabilities and technologies that once were considered the exclusive domain of nation-states. These technologies will enable group and individual adversaries to overcome the tyranny of distance and make it easier to discover, act, surprise, and target almost any place on Earth. Individuals will be more difficult than groups or nation-states to track, but the greatest likelihood of catastrophic attack is likely to be posed by groups. If the United States can ensure adversaries will be precisely attributed through greater system transparency and immunization, attacks may be deterred.[1]

* * * * *

The rapidly changing nature of technology suggests that the world and the associated technological challenges it faces are changing in unprecedented ways.[2] It is not only the scope of technology change that is

Dr. John P. Geis II, USAF, retired, is former director of the Center for Strategy and Technology. Currently, he serves on the leadership and strategy faculty at the Air War College (AWC). Dr. Geis earned a PhD in political science from the University of Wisconsin.

Col Ted Hailes, USAF, retired, is the former force transformation chair at Air University and a founding member of the Center for Strategy and Technology. A graduate of AWC, Col Hailes earned a master's degree in international relations from Troy University.

unprecedented but also its speed. This century will likely see 1,000 times the technological change of the last century, with each decade containing upwards of 70 times more technological development than occurred in the period from the dawn of time up until the year 2000.[3] This combination of great scope and speed of technological change means that the world of the 2030s will not merely be an extension of today. In many respects it will be fundamentally different. As a result, the greatest threats the world could face likewise represent a significant departure from past thinking. This article examines how the United States can best posture itself to deter nation-states, groups, and individuals from using biotechnology, nanotechnology, or directed-energy weapons. It begins by discussing the rapidly changing nature of emerging technology, its proliferation, and the developmental challenges associated with having only a small percentage of global research and development within the nation's military portfolio. It then delves into the nature of the threats across the three technological areas. The article discusses the types of attacks that will be possible over the next 20 years and what the effects could be upon the national critical infrastructure and the population; furthermore, it enables the reader to understand the breadth and depth of the challenges faced. It then introduces a structural model of deterrence based on the writings of many of the preeminent deterrence theorists of the past 60 years. This model dissects the concept of deterrence into its component parts and offers a useful analytic tool to determine how best to address each of the threats discussed. It concludes with a specific set of recommendations, while highlighting a few areas where further research or actions are necessary—particularly action by other governmental agencies to create an optimum deterrent posture.

The Changing Nature of Technology

Profound advancements are occurring across the entire range of sciences at an extremely rapid pace. As a result, the capabilities available to nation-state, group, and individual actors in the international arena will continue to expand at an ever-increasing rate. Driven by motives of profit, social pressures for ever-more-capable goods, as well as scientific curiosity and military necessity, continued exponential technological change is real and inevitable. One of the principal early findings, validated in earlier studies, is that many of the key technologies that will require deterrence in the future continue to evolve at an exponential

rate. As with the number of transistors on a microprocessor and the number of Internet hosts, biology, nanotechnology, pulsed power, and other technical sciences are all racing ahead at ever-increasing speeds.

Research also shows that the United States and its military have an ever-decreasing say in the types of technology being developed. Seventy percent of all research funding happens outside the United States. Further, even among the 30 percent that happens within US borders, 70 percent of those technological developments are privately funded and are solutions or breakthroughs over which the military has no influence or sway.[4] Less than 4 percent of modern technological research is within the purview of the Department of Defense (DOD)—a radical departure from 50 years ago, when that number was nearly 50 percent.

Feeding this development is the collaboration enabled by the Internet. The increased use of the Internet as a source of collaboration results in scientific breakthroughs and technological applications being both increasingly civilian-developed and commercially and globally distributed, and these advancements are accelerating.[5] Moreover, the "half-life" of scientific secrets and their technological applications into militarily critical technologies are shrinking, and they are available to a multitude of actors, both state and nonstate. The result as we look to the future is that the technological dominance the United States has historically enjoyed may no longer be possible. By some measures of innovation, such as the number of major scientific articles published in peer-reviewed journals, China already surpasses the United States. While the United States continues to enjoy the best laboratory infrastructure in the world, our productivity is declining while others are rapidly improving their ability to innovate. This poses the danger of the United States losing the technological race.[6] Technologies formerly in the hands of only the wealthy nation-states are now being developed in what were once called developing countries.[7]

As a result of the decreasing cost of technology, groups and individuals now can acquire advanced capabilities that were once the purview only of states. Power is diffusing to the individual, meaning that attacks and battles of high probability may soon also be events of high consequence, thus changing the nature of warfare. Worse, these conflicts might become more common, meaning the future may be different from our past in significant ways. The world has already seen a rise in groups, including nongovernmental organizations, intergovernmental organiza-

tions, and terrorist organizations (such as al-Qaeda), many of which are able to affect outcomes on at least a regional basis. By 2008 these groups numbered at least 13,425 and possibly as many as 40,000.[8]

As technology becomes even less expensive, as automation increases, and as the ability of single individuals to create major effects is enhanced, the number of actors will grow still further. We are in a world where computers can pass the Turing test, meaning they cannot only assist individuals in carrying out tasks but also carry out these tasks by themselves.[9] As machines empower individuals and potentially even become capable of creating significant impacts on society, the number of potential actors undergoes yet another increase. By this measure, the world of 2030 has not hundreds of actors or even tens of thousands: It might have billions. The human race is likely to number between 8 and 9 billion by 2035, and this number itself may pale in comparison to the number of autonomous machines that might be roaming the planet by that time.[10] In short, the number of actors capable of making a major impact on the world stage will increase dramatically in the next 30 years.

Currently, we refer to the threats we face as *hybrid*. Whatever this future threat is (and there may be no good name for it), it is vastly more complex than anything experienced to date. The cause of the increase in the number of potential actors and of their increased potential capability is illustrated in economic theory. British science journalist Matt Ridley argues that the rapid evolution of human capabilities represents a significant research puzzle, as no other species has managed to adapt and conquer its environment so completely or quickly. Over time, this has led to the increased specialization of employment and the growth of these early communities into the megacities in which many of us live. The critical point is that the concentration of people escalated the interplay of knowledge that leads to increasing innovation. Ridley argues that the advent of the Internet is exponentially increasing the rate of innovation and now allows information sharing on a planetary scale, which will continue to increase our inventiveness as a species, to produce wealth, and to stimulate continued cultural change. From an economic perspective this argument is a story of good news. From the standpoint of biology, however, it has a darker side. As innovation increases at an exponential rate, our ability to understand, contain, and control new concepts and technology is threatened.[11] It would be an act of hubris to believe that we humans are somehow immune from this outcome.

Threats in the Age of Surprise

As a result of this increasing speed of interaction and data sharing, we have entered an "age of surprise." While it is possible to see the broad outlines of the future and to define the strategic planning space, this speed of change is making the specific details harder to see.[12] Whether we call these details turbulence or a form of chaos in complex systems, we have entered a period of inevitable surprises. We can discern the outlines of some in advance, including biotechnology, nanotechnology, and directed energy.[13] The key is to understand some of these potential surprises and know how to deal with the resultant challenges.

Biotechnology

The Human Genome Project, completed in 2003, identified all the genes in human DNA, and since then the threat has been rapidly evolving in biotechnology.[14] Today, it is possible to get your finger pricked and have your genomic code printed out with all the As, Gs, Cs, and Ts. Such a printout would reach about 20 feet high and would likely be meaningless both to you and to your doctor, but it is possible.[15] The step being worked on now is the "Rosetta stone" to those 20,000–25,000 genetic sequences—the part that determines how these genes produce the roughly 20,000 proteins that make each one of us a unique human being. This is called the Human Proteome Project, and it is well and truly under way.[16] Once the project is completed, pharmaceutical companies will be able to use these data to develop cures for many, if not all, genetic diseases. Illnesses like cystic fibrosis, muscular dystrophy, and cancer could all be eradicated. Already some cancers, particularly those such as leukemia, are being attacked by nanoengineered medicines based on an understanding of the ribonucleic acid structure of the underlying disease. The result for many patients is a long life with leukemia in remission. Many more such cures and treatments will follow in the years ahead. Unfortunately, this technology cuts both ways. Once the human genetic code is understood well enough to cure a genetic disease, it will also be understood well enough to engineer an illness for which no immunity can be found within the human genetic code. Leading scientists in our national laboratory system predict that by the year 2025, such capabilities will be resident in the hands of a well-trained microbiologist, whom they define as a master's degree holder from a major university. With a lab costing as little as $100,000, such an individual

would be able to engineer a lethal pathogen inside a one-car garage or a small basement.

Lest this be thought of as only science fiction, such an event—though unintended and contained—already occurred with mice. In 2000, Australian scientists were attempting to modify the mouse pox virus to produce interleukin-4 in the hopes of stimulating the production of viral antibodies. This experiment had two unexpected results.[17] First, it failed to result in the production of the antibodies sought. Second, the resultant mouse pox strain had extraordinary lethality. Researchers arrived one morning to find every mouse in the laboratory dead, including mice immunized against the disease. The virus was 100 percent lethal, had overcome the immunity conferred by prior vaccination, and had spread to every mouse in the lab.[18] Although this incident was an accident, deliberate genetic modifications to existing viruses could produce the same result in other species—including our own.

Nanotechnology

The term *nanotechnology* is recent to science. Some versions of Webster's dictionary do not even contain a definition for the word.[19] Further, even within the discipline, its meaning causes controversy. Some have come to use nanotechnology to refer to any object or technology that is smaller than a micron (1,000 nanometers) in size. This misuse was partly an outgrowth of science fiction and partly of science still catching up to the concept.[20] Adding the marketing aspects of being able to label anything made with a coating or substance that contains small parts as being *nanotechnology*, the environment became ripe for misuse of the term. Here, nanotechnology refers to materials and substances that are constructed using processes to arrange particles of under 100 nanometers in size with submolecular precision, for which the important properties of the materials are governed largely by intermolecular (that is, van der Waals) forces.[21] Technology that merely involves scaling existing micromechanical processes to submicron scale is "nanoscale technology."

The field of nanotechnology offers three key advances as we move toward the future: (1) the nexus of biotechnology and nanotechnology, largely discussed above, (2) the creation of high-density energetic materials much more powerful than those developed to date and, (3) the development of nanomaterials that have specifically engineered properties, such as the ability to cause rapid corrosion, which could become a

new class of weapons against systems and materiel. As indicated above, the first challenge with nanotechnology is the ability to precisely and deliberately create molecules of any design. As pharmaceutical companies are already demonstrating, once the genetic structure of a particular form of an illness is known, it is possible at the submolecular level to design medicines that can cure these diseases. As also mentioned, once the human genome is successfully decoded and the Rosetta stone is built, well-trained microbiologists will have the capacity to engineer pathogens for which, even at the genetic level, the human system has no built-in immunity.[22]

The second area of concern for future attacks deals with the production of high-density materials using precision nanotechnology to arrange molecular structures in a manner optimizing explosive power. While modern explosives are several times more powerful than trinitrotoluene (TNT), future explosives may be much more powerful still. One of the principal limitations of modern explosives is the availability of oxygen at the time and place of detonation. This causes the explosive to do two things. First, some explosive molecules may not ignite due to the oxygen-depleted environment and as such will reduce the total energy produced. Second, the explosive molecules that do not pair with the necessary oxygen immediately may still detonate but will do so after a short delay while they wait for additional oxygen molecules. This extends the duration of an explosion at the cost of reducing the initial blast effect. Using nanotechnology to pair oxygen atoms directly with the explosive atoms that require them would theoretically improve the efficiency of the explosive burn.[23] This same process could be used to enhance the thrust produced by rocket fuels, which are, in essence, controlled explosions themselves.[24]

While it is theoretically possible to achieve explosive yields of up to 1,000 times those of modern explosives, near-term advancements are likely to be much more modest.[25] Though nanotechnology is a rapidly advancing field, the ability to create the assemblers necessary to produce such explosives on a meaningful scale is currently limited; most scientists in the field believe that in the next 10–20 years an advancement of five- to tenfold is likely. Nonetheless, a tenfold advancement makes future explosives so powerful that the three-ounce bottle of liquid passengers are allowed to carry on board a civilian jetliner may have to be reduced to 0.3 ounces—only a few drops. Small, easily concealed explo-

sives could pose significant risks to lives and property, and this miniaturization may result in a more-challenging threat in the years ahead.[26] Militarily, there are two positive aspects to this technology. First, the meticulousness needed to create these explosives would produce a precise and reliable yield, allowing for potentially greater accuracy and lower collateral damage from newer weapons designs. Second, the increased thrust potential emanating from these materials may significantly solve challenges associated with getting heavy objects into space. Historically, roughly 90 percent of all rocket mass has been either fuel or the systems that contain the fuel. The amount of thrust a unit of fuel can produce is called specific impulse (ISP). Increasing the energy content of the fuel five- to tenfold would increase the ISP proportionately and greatly reduce the amount of mass a rocket would need to devote to fuel and its associated system.[27] Though this dynamic has long been understood, the breakthroughs in nanotechnology may soon allow the dynamic to be exploited. While this may make it easier for man or robots to explore the stars or launch satellites, it would also make it easier for other actors to launch objects at long distances, posing yet another potential threat.

The last area where nanotechnology poses a potential threat is in designing molecules or nanoparticles to interact with materiel to cause severe damage to infrastructure or materiel. "White nanoparticles" are designed to specifically interact with their environment and to "pick up" any foreign debris located on the surface to which they are applied. In short, they are created as powerful agents designed to strip the surface of anything that should not be there. Similar agents could be designed to cause the degradation of materials and play havoc with critical components or infrastructure.[28]

Directed Energy

Two different forms of directed energy represent threats to military and civilian personnel. The first is the pulsed type, which includes such phenomena as pulsed high-powered microwaves, electromagnetic pulses, and a set of natural phenomena that mirror the effects of these two weapons types. The second type of directed-energy threat is continuous wave in nature. The power output of these weapons, usually referred to as lasers, has reached tactically significant levels in the past few years, and further developments are likely in the near future.

The discovery of the potential antielectronic utility of pulsed forms of energy came by accident. In 1962, shortly after the Soviet Union breached a nuclear testing moratorium, the United States tested a 1.4-megaton nuclear device 400 kilometers above Johnston Atoll in an experiment called Starfish Prime.[29] Approximately 1,300 kilometers away, in the Hawaiian Islands, street lights burned out, radio stations were knocked off the air, cars stopped due to burned-out generators and alternators, and some telephone systems were knocked off-line. The relationship between these events was not initially obvious and took some time to verify.[30] It is important to note that not every street light was disabled, that many cars still ran, and that some telephones still worked. Nonetheless, many systems stopped working, and only later did the reasons become clear. In 1967, both the United States and the Soviet Union (USSR) replicated these pulsed-energy effects. They discovered that nuclear detonations above the ionosphere would charge this region of the upper atmosphere and generate intense electromagnetic fields across the earth's surface. These fields fluctuate quickly and induce electric currents in all metallic objects they encounter. If the electricity generated is above the designed load for the system, the system shorts out and subsequently fails.[31] Fearing the effects of such weapons, the United States and the USSR together drafted the Outer Space Treaty (more formally, The Treaty on Principals Governing the Activities of States in Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies), which bans only weapons of mass destruction from space and does so because of the electromagnetic-pulse (EMP) phenomenon.[32]

However, a very similar phenomenon can be reproduced using a nonnuclear pulsed-power generator on the earth's surface. While physicists will be quick to point out that the precise shape of the pulsed waveform is different from that of a nuclear blast, its effects on electronics are nonetheless the same.[33] Inducing an electromagnetic field across wires, computer circuits, or any other conductive material produces electric current within the system. Like EMP, this current can wreak havoc with financial systems, computers, power distribution, and communications systems used to command-and-control military forces worldwide.

The level of damage done to these systems is related to the field strength of the magnetic field induced by the pulsed-microwave device and the sensitivity of the equipment.[34] It is important to realize that as computer-chip spacing becomes more compact in our quest to produce

ever-more powerful and faster computers, the amount of energy needed to short out the computer circuits decreases with the square of the chip spacing. Stated more plainly, the ability to destroy or damage computer control systems is increasing exponentially as the computer chips become faster.[35] At the same time, our ability to store and generate pulsed power in the form of microwaves is also increasing exponentially. In 2003 it was possible to produce 20 gigawatts of pulsed-power output in a 400-pound device. Today several efforts are in the works on terawatt-class devices, some of which are explosively powered, representing a near 100-fold improvement in roughly a decade.[36] In 2002 conventional pulsed-microwave devices had relatively short ranges. Today small, portable, reusable weapons have ranges in the hundreds of meters. At the rate these technologies are changing, by the 2030s the ranges of these systems will be in miles or tens of miles, making them tactically and strategically significant.[37]

The other form of directed energy is continuous wave, the most common being lasers. While lasers have overpromised and under delivered for decades, this is no longer true. In November 2010, one of the authors placed an order for a small, handheld, category-IV, weapons-grade laser for $299. To the researchers' surprise, the order processed on "Black Friday," a shopping holiday after Thanksgiving, resulting in the "three-for-one" special deal. We paid less than $100 for each of the three lasers that arrived about six weeks later. The blue variant of this laser measures approximately 20 centimeters long and approximately five centimeters in diameter, weighing about 250 grams. It is a potentially lethal device, but its greatest dangers come from its ability to permanently blind a person in less than 0.25 seconds at a range of approximately 150 meters. It is capable of melting plastic and setting flammable materials ablaze (451° F or 233° C).[38] The laser runs off a single lithium-ion battery, roughly the size of a standard AA battery, which enables the laser to operate continuously for 120 minutes on a single charge. A company operating in Hong Kong began producing and marketing the laser in the fall of 2010. At that time, only Malta had definitive restrictions on the sale or importation of this device.[39] In the United States, importation was legal. Though not directly attributable to this laser, in the first nine months of 2010, before this laser hit the market, the United States had 299 lasing incidents against civilian aircraft. There were 2,700 more in

the last three months of that year. Blinding incidents have also increased in other countries, including some attacks on motorists.[40]

Meanwhile, lasers for aircraft and weapons applications have reached tactically significant power levels. Chemical oxygen iodine lasers (COIL) have been designed for applications ranging from missile defense to ground attack. The airborne laser system, which the DOD recently decommissioned, was a megawatt-class system, roughly 1 million times more powerful than the handheld laser above. Air Force Special Operations Command placed a much smaller COIL device on board a C-130 aircraft and successfully disabled targets on a weapons range, including a truck.[41] As with pulsed-power devices, laser efficiency and effectiveness are continuing to improve. Small handheld devices powerful enough to blind or kill soon will be in the hands of those who may seek to create fear or terror. Larger lasers, with speed-of-light kill capability, will likewise be obtainable via arms markets well within the next 20–30 years.[42] Directed-energy research is continuing in several countries and will pose a risk to satellite operations in the very near future.[43] Lasers that can dazzle or destroy satellites, likely all the way to geostationary orbit, may be fielded by the 2030s. The result is that space assets, both military and civilian, are and will increasingly be vulnerable to attack, either from the ground or from space. The challenge becomes how the United States deters these threats.

Deterring Emerging Threats

To deter the technological threats of biotechnology, nanotechnology, and directed energy one must first understand deterrence concepts and deterrence theory; extensive literature covers both conventional as well as nuclear deterrence theory. [44] The model below depicts two predominant aspects of deterrence and the relationship between them.

The focus during the Cold War was mainly on the left half of the model—"Fear/Retribution." This thinking made sense because during the Cold War time frame, the treaties in effect limited each side (the United States and Soviet Union) to 100 ballistic missile interceptors.[45] Since each side in the Cold War had vastly more than 100 nuclear weapon systems, there was an implicit assumption that it would be impossible to deny the opposing side the ability to carry out a massive strike that would inflict severe damage on the opponent should it choose to do so. As a result, the "denial" side of the equation was limited in

value to only that necessary to ensure a retaliatory capability existed. There was no method by which one could deny the initial attack, and as such, much of the denial side of the model was ignored, leaving mutual destruction or unacceptable levels of damage (fear) as the linchpin upon which deterrence was based. It is important to recognize that the theory itself is structurally sound, but in deterring emerging technologies the relative importance of the two sides of deterrence theory changes. The difference is, with many of the threats we face in the future, there are opportunities to prevent or protect from attacks, to thwart the goals of prospective adversaries, and to deter or hinder the development of these capabilities in the first place. These key elements of the right-hand side of the model take on new levels of importance in the future and thus constitute a change in the way in which the DOD needs to operate.

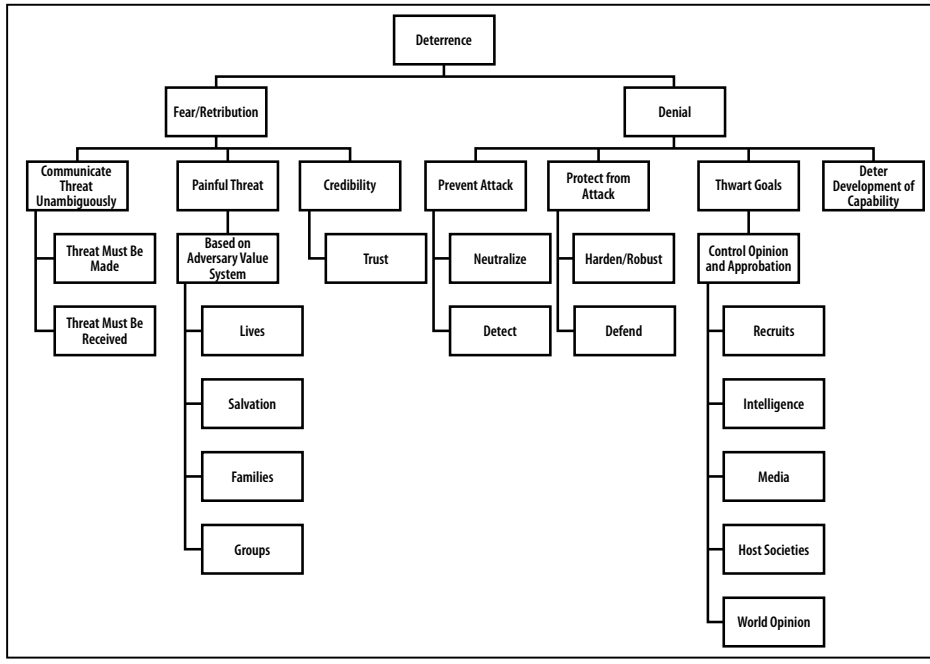

Figure 1. A structural model of deterrence theory

In operationalizing the model against the array of future threats, many of which are conventional, we turned to an equation verbally described in John J. Mearsheimer's book *Conventional Deterrence*. Mearsheimer argues that the failure of deterrence is specified as a calculus in the mind of the actor to be deterred, referring to this calculus as "the attacker's fear to the consequences of . . . action."[46] While he describes this calculus in

great detail, it can be simplified as a mathematical expression. An actor is deterred if the equation depicted in figure 2 holds.

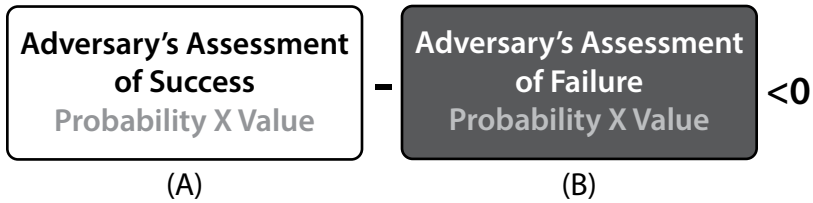

Figure 2. The deterrence equation

Mearsheimer argues that several factors play in this calculus of whether deterrence will succeed. The first is the adversary's perception of the value of success itself—the gain to be incurred by attacking. The second factor is the probability that the attack will succeed. The product of these two elements comprises the potential adversary's assessment of success (A). Only if the assessment of failure is greater than that of success will a rational actor be deterred. This failure assessment is calculated in much the same manner—the cost of failing is multiplied by the probability of failure. If the failure assessment (B) is the greater of the two terms, then the value of the equation is less than zero, and the actor is deterred.[47] Some assumptions are embedded in this calculus that must be highlighted in light of the new threats. First, it assumes the actor is rational. This does not mean the actor's calculus is the same as one's own or that it matches one's values—only that it has a rational basis underpinning it. Second, it assumes that one can attribute the attack to the proper actor. While in the nuclear era this was relatively easy, it has proven much more difficult in newly created artificial domains such as cyberspace. It is crucially important to explore what happens to the deterrence equation in the absence of attribution. Should attribution be problematic, it tilts both parts of the deterrence equation in favor of the potential aggressor. An inability to attribute an attack means the probability of successfully carrying it out likely rises or at a minimum remains the same. The probability of incurring punishment clearly diminishes because without attribution it is impossible to know toward whom the punishment should be directed. As a result, in the absence of proper attribution, the deterrence equation tilts in favor of the potential adversary, making successful deterrence less likely.

Of equal concern is what happens when attribution is either assumed or figured incorrectly. A failure to properly attribute often leads to sim-

pleminded decisions along the lines of what actors expect.[48] Further, in the absence of data or in the midst of uncertainty, decision makers tend to engage in more violent modes of coping with the ambiguity.[49] These dynamics were tested in exercises conducted in conjunction with this research—exercises that placed participants in a war game in a position of relative uncertainty with regard to adverse conditions experienced by the United States and its allies. Even though sufficient data were available to the participants to uncover the actual actors, the vast majority of the participants attributed the hostile actions to the wrong actor. In a real-world situation, such misattribution can have disastrous consequences.

Getting attribution correct is essential not only to realize deterrence but also to avoid unintended conflict. Complicating the problem of attribution is the fact that the time to respond to attacks from several emerging threats is much less than the reaction time that was available in the nuclear-deterrence era. As a result, the time necessary to observe events, orient to these events, decide on a course of action, and then act (OODA) on that decision is shrinking.[50] The OODA loop decision cycle is rapidly collapsing into an OODA point. With several new technologies operating either at or near the speed of light, this decision loop is moving toward a point requiring much more rapid capabilities to observe and attribute incoming attacks. The nation-states that comprise our global security system are similarly chaotic and capable of rapidly tipping from one state to the next. In the end, the human system in which we must deter is complex and chaotic while the credibility of deterrence hinges on the capacity to accurately attribute such actions at ever-increasing speeds.

The Delphi Study and Results

To better understand where the greatest challenges for deterring emerging technologies lay, we conducted a formal and informal Delphi study using three questions.[51] It drew upon participants who had studied the technologies and had a working knowledge of deterrence theory and military strategy. Each question explored the three technologies and parsed the responses to separate dynamics that differed among nation-states, groups, and individuals.

The first question asked the respondents to use a Likert scale of one to five (very easy, easy, neutral, difficult, and very difficult) to rate the level of difficulty of deterring nation-states, groups, and individuals from

launching an attack using each of the technologies shown in figure 3. The results show that it is more difficult to deter individuals, regardless of technology, than to deter nation-states. In addition we found that bio- and nanotechnologies would likely be the most difficult to deter. Further, although the slope changed for each technology, the relationship across the three categories took on a mostly linear shape. In general, the study participants believed nation-states and groups placed value on their respective reputations. Moral constraints to use force and the results of international approbation act most strongly on nation-states.[52] Yet for groups, especially the larger ones, the reputational issues were strong enough to make them easier to deter than small groups and individuals. Individuals would be least affected by international norms and thus the hardest to deter.

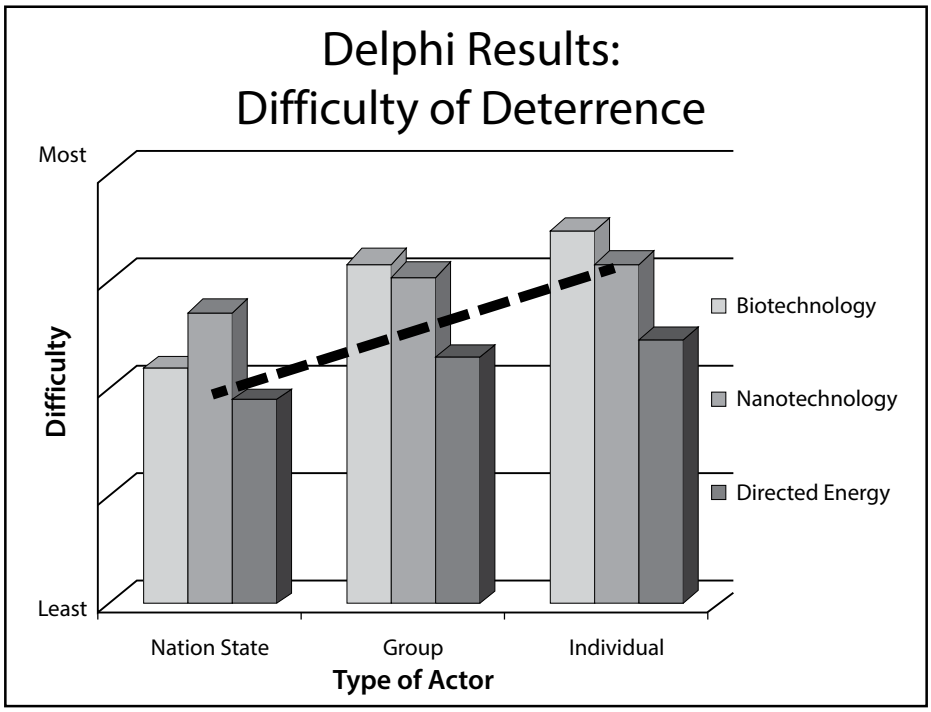

Figure 3. Difficulty of deterrence: Delphi results

The second question focused on the difficulty of attribution. As with the previous question, this one was parsed by both type of actor and technologies involved.

The depiction in figure 4 takes on the same shape as the previous one but for different reasons. Here, individuals were considered the most difficult

to attribute across all technologies since they were the most likely to conduct an attack and successfully avoid leaving a distinguishing trail that would lead to properly attributing the source of the attack. States, on the other hand, because of their size and the bureaucracies that must approve these actions, often leave traceable indications of their responsibility for certain actions. Additionally, in some cases, the research efforts necessary to launch attack programs by nation-states in these areas would require funding of sufficient size to make it possible to trace the program. Biological attacks were considered problematic because tracing the source of a disease or pathogen may be difficult, especially if it has a considerable incubation period. Should such an agent be distributed at a major transit hub, such as a major international airport, viruses would be hard to trace to their origins since the passenger traffic would leave a very large number of potential paths to trace.[53] Nanotechnology threats also were considered difficult because they are small enough in size that they could remain dormant for extended periods, leaving great doubt as to when they were positioned.

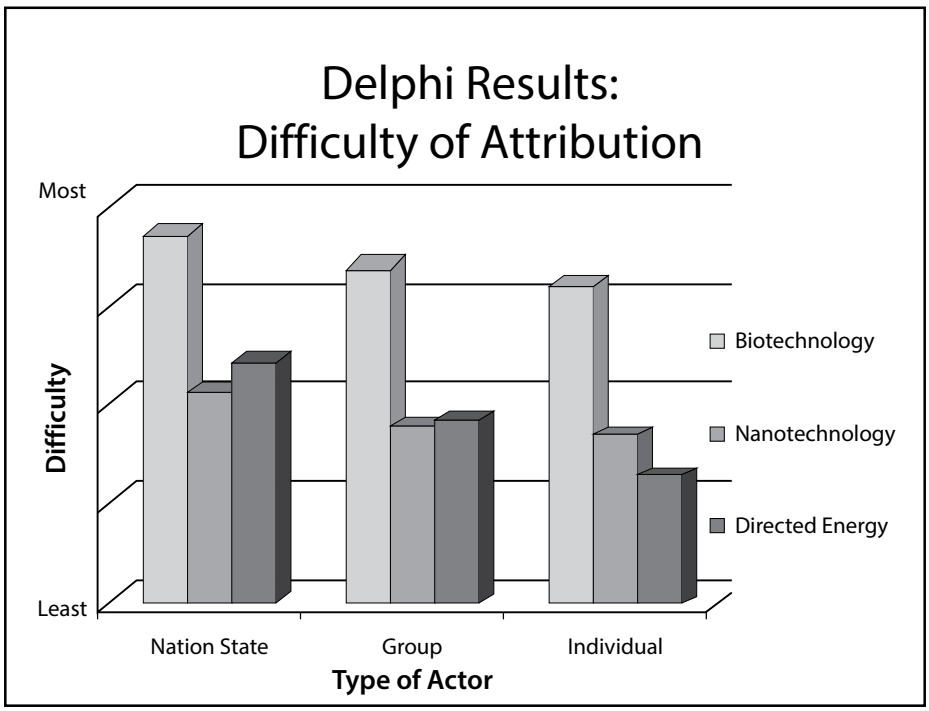

Figure 4. Difficulty of attribution: Delphi results

The last question regarded the likelihood of attack. Here, definitions proved important insofar as we were interested in the likelihood of only very large destructive or catastrophic events. For this question a "catastrophic" attack was considered one that "threatens national survival or eliminates the ability to accomplish the mission." A "destructive" attack was one that "seriously impacts the ability to function or significantly degrades mission performance." The results are depicted in figure 5, which contains three patterns within the data that are worthy of explanation. First, the greatest perceived threats were based on biotechnology. This danger is significant due to the relatively unprotected and very incomplete infrastructure to detect novel pathogens or viruses. Second, the graph has a central "hump," showing a greater probability of catastrophic or destructive attacks coming from groups than from individuals or nation-states. This created a curve that placed the maximum likelihood for attack at the group level. It should be noted that had we lowered the damage threshold of interest, it is likely that individuals would have scored much higher. Lastly, for nanotechnology and directed energy, nation-states were considered the most likely to attack catastrophically because we deemed it unlikely that even groups would have the resources to attack using these weapons on a massive scale.

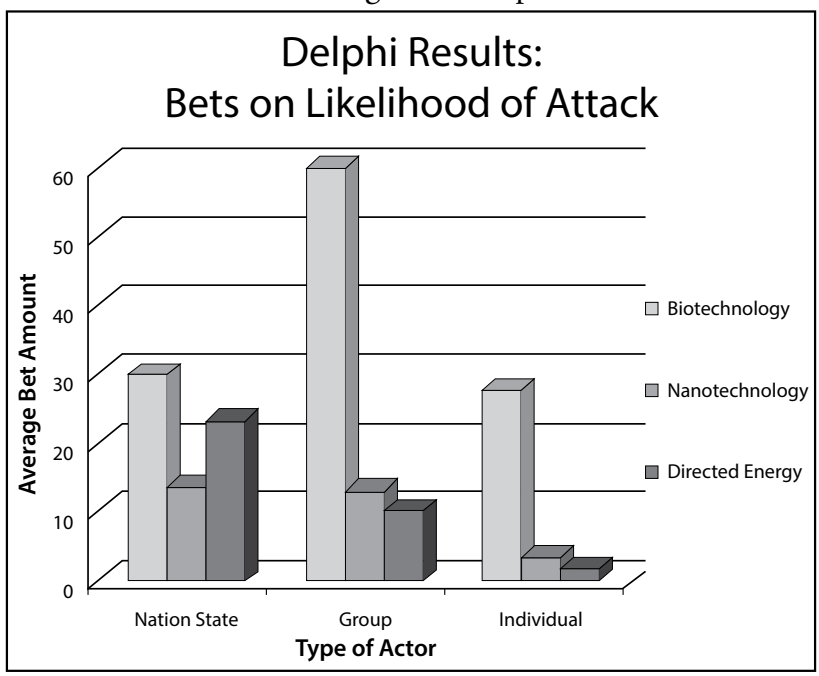

Figure 5. Likelihood of catastrophic attack: Delphi results

Findings and Implications

Deterring future technologies of adversaries remains a great challenge for the DOD, particularly concerning biotechnology, nanotechnology, and directed energy. Solving this challenge will require two specific concepts: transparency and immunization.

Increased transparency is necessary to facilitate proper attribution and early warning of attack. Transparency contains three elements: (1) technical developments that aid in tracking people and objects through space and time, (2) ongoing innovation in this area, and (3) the advent of new command-and-control concepts. With the development of the internet, most data—public and private—is archived for retrieval. Even when websites are updated or personal data removed, the old data is still available and can be retrieved.[54] The result is that anything which has been on the Internet can often still be found, enabling the searching for information not only across geographic space but also across time. These searches can synchronize raw data as well as pictorial information; they archive public (government) as well as private (personal) web postings. In short the technological developments are moving us toward transparency. As this enormous data set becomes available on the Internet, new innovations will be necessary to use it. Some of the necessary algorithms already exist and are able to examine patterns of human behavior and flag for analysis those activities that are unlike others. Such algorithms can be useful for enabling business to foresee the next major consumer product or for enhancing security. One such set of algorithms has been developed as part of the Risk Assessment and Horizons Scanning system in Singapore.[55] That city-state has developed an analyst-intensive process that involves environmental scanning for data, provides indicators of possible activity, enables the conduct of sentiment analysis, and helps with data fusion and analysis that leads to scenario development and the development of strategies. While not fully automated, the system provides "insights to emerging risks and opportunities with national security implications."[56] With a world of data available and the algorithms to flag events that may be indicators of risks, proper command and control can ensure that risks are properly assessed. Global command-and-control capability becomes the last element of a new transparency system. As data suggest that a risk may be emerging in a part of the world, the command and information exchange systems—in conjunction with

well-trained leadership—enable analysis, further research, and assessment of the risks as they emerge.

These data are fused and processed using advanced algorithms that build on work already done. These algorithms will be designed to highlight or flag unusual patterns of behavior worthy of human analysis. Upon seeing such a signal, the analyst initiates tracking. The analyst drills into the data to determine if there is a concern that rises to the level of a threat to US facilities or interests. If such a threat exists, an analyst does additional analytical work with the data to attribute the threat to a specific actor or set of actors and then characterize that threat, including identifying its capabilities, operating procedures, and location. At that point, the government has many options available to deter a potential adversary. Depending on the nature of the threat and how early in the planning process an attack has been identified, the options may range from merely warning the individuals that they have already been discovered to potentially arresting or striking them if the threat they pose is more imminent. As these actions are taken, ripples or perturbations in the networks associated with these actors will likely appear within one or more of the streams of data. Additional fusing of data and repeating the above process will also flag other potentially dangerous actors associated with the initially discovered adversary for further analysis. Iterating this process will soon make obvious to actors who seek to hurt the United States that their likelihood of success has decreased, shifting the deterrence calculus in our favor.

From this proposed operational concept, transparency should be thought of as a second pillar of deterrence since it has benefits similar to those of attack and defense. More importantly, transparency has a deterrent quality all its own. It is important to understand that transparency is about knowledge rather than control. Along with the ability to strike globally, transparency has the potential to radically alter adversaries' deterrence calculus. If they believe their actions will likely be discovered and attributed and then punished severely, then the attack will likely be deterred. As a result of the development and proliferation of technologies that can create catastrophic effects over the next 10–20 years, transparency and the associated concept of attribution will be essential. Moreover, as a requirement it will drive defense procurement spending.

Unfortunately, transparency is a two-way street and by itself it does not fully address all the aspects of deterrence by denial. It is likely ad-

versaries will have some level of transparency against the United States. As a result of this transparency, we need a set of means to deny potential adversaries a chance to succeed, even when our forces or infrastructure are in known locations. In short we need to deny success, and to do this, we need a second concept called immunization.

Immunization

As it applies to emerging technological threats, immunization is a protective measure that reduces attack effectiveness. Similarly, a nation-state properly immunized against attack will not suffer significant damage, even if an attack is launched against it. For the United States, this immunization process involves implementing physical safeguards around certain critical infrastructure. It involves creating backup methods of operation and functional resilience that result in little or no degradation to operations should an attack occur, creating strategies that enable flexible options to mitigate the effects of an attack. It also results in the development of cognitive resilience within the populace and the military, creating a mind-set in which, even if an attack occurs, there is not a disproportionate psychological reaction to the strike.

As threats become more numerous and span increasingly large technological sets, immunization will require time, resources, and practice to attain. The methods of immunizing computer systems will be different from those of immunizing the populace against a biological pathogen. Nonetheless, the country must be prepared to do so. If we can achieve a level of immunization that minimizes the gains realized by attacking the United States and its interests abroad, then the deterrence calculus shifts in favor of the defender, and the nation becomes more secure. To insure that immunization actions are considered in that calculus, demonstrations of these capabilities will likely be required.

Issues for Other Departments

Because of the breadth of challenges that will confront the United States in the 2030s, this is much more than a Department of Defense problem. There are issues for the departments of Homeland Security (DHS), Transportation, Health and Human Services, and Commerce, as a minimum. The DHS is responsible for the defense of our national infrastructure and air transport system. Consequently it needs to understand

the potential impact that directed energy will have on our electrical and banking systems. The DHS is also responsible for airline safety. Nanotechnological explosives will soon increase the potential for very small amounts of a substance to create very large explosions. While there is substantial public backlash against strictures such as the three-ounce-bottle limits on commercial aircraft, this problem is about to become worse. The DHS will need to develop methods of detecting which compounds can explode and which cannot—and further, detect these when they may be chemically new materials or something nanoengineered in an adversary's laboratory. The Department of Transportation has this same requirement but with respect to our major highways and bridges. The destruction of all bridges that cross the Missouri–Mississippi river system with nanoexplosives is something that must be guarded against as well.

The one potential extinction-level event discussed above is biological attack. Previous studies have recommended major efforts to enable rapid detection and decoding of new genomic structures along with the ability to quickly prototype and produce vaccines.[57] We stated then and reiterate now that a major project is needed on biogenetics to ready the nation and the world to rapidly respond to the outbreak of a novel virus, whether man-made or a natural mutation, within a matter of hours instead of the nearly one year it currently takes to develop the annual influenza vaccine. However, implementation lies within the purview of the Centers for Disease Control and the National Institutes of Health.

Conclusion

It is important to note that deterrence by denial is not new. It has been a part of deterrence theory for over 50 years, but it is more important now than it has been in the past. In short, we are entering a world where the proliferation and cheapening of potentially harmful technologies will impose costs on those nation-states that value protecting their populace. The panoply of new threats increases the requirements for the services to work together to create effective transparency and immunization to provide resilience. As we do this, we need to understand not only who is theoretically responsible for certain mission sets but also who will accomplish them. While the threats in this study may come from terrorists, what is necessary to defeat this threat bears little resemblance to the types of combat in which we have been engaged over the past 15 years. Further, technology is changing at such a pace that those who fail

to make a concerted effort to stay abreast of new developments will find their thinking quickly rendered obsolete. The scope of the threats we may face from emerging technologies is disturbing. Properly addressing these two broad areas will make attacks easier to attribute, adversary opportunities easier to deny, and adversary success harder to achieve. Collectively these tilt the deterrence calculus in favor of the United States, making it much less likely that the adverse and severe consequences of the threats discussed above will ever be endured. SSQ

Notes

1. The authors want to thank the scientists, researchers and policy analysts of the US Air Force and National Laboratories. The authors also wish to extend a special thank-you to academic leaders and government officials who provided commentary and insights. Among these are John Mearsheimer and Bob Pape of the University of Chicago; Gen Mike Hayden, USAF, retired; and Dennis Bushnell of NASA. Air War College students involved in the study included Lt Col Joel Almosara, Col David Blanks, Lt Col Darren Buck, Lt Col Patrick Burke, Col Christopher Kinnan, Col Tom Coglitore, Lt Col Miguel Colon, CDR Peter Falk, Col Michael Finn, Col John Gloystein, Col Christopher Hauth and Col Wiliam Jensen. The team of 35 researchers and five faculty members from Air War and Air Command and Staff Colleges began with a search across science and technology, education and training, governmental policy, organizational culture, national strategies, and military studies literatures. The research team was deliberately selected for its breadth of expertise across all relevant military specialties. These researchers visited Sandia, Los Alamos, and Lawrence Livermore national laboratories. In addition the team visited seven of the 10 Air Force Research Laboratory directorates, including Space Vehicles, Directed Energy, Materials Sciences, Human Factors Engineering, Propulsion, Air Vehicles, and Sensors. In each, senior scientists made presentations, and the researchers had time to discuss and interview these scientists regarding current projects, including those that were in the conceptualization stages. This research helped define the range of technologies likely to be available in the field in the 2030–35 time frame for which this study was commissioned.

2. John L. Petersen, "Punctuations," *FUTUREdition* 15, no. 8 (30 April 2012), http://www.arlingtoninstitute.org/fe-archive-volume-15-number-8. Also published as the foreword in Finley Eversole, ed., *Infinite Energy Technologies*: *Tesla, Cold Fusion, Antigravity and the Future of Sustainability* (Rochester, VT: Simon & Schuster, 2012).

3. Ray Kurzweil, *The Singularity Is Near* (New York: Penguin Books, 2005), 10–50.

4. T. Michael Moseley, *Blue Horizons: Horizons 21 Study Report* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2007). These numbers have not changed much since 2007, as verified in a 2012 study by Battelle Corporation. See Martin Grueber et al., "2012 Global R&D Funding Forecast," *R&D Magazine*, 16 December 2011, http://www.rdmag.com/articles/2011/12/2012-global-r-d-funding-forecast. Grueber and company point out that US research and development spending will top $420 billion but that only $128 billion will be driven by the government—a total of 29 percent. The United States continues to hold about 30 percent of the global research and development share.

5. Air War College papers written on this topic include: Christopher Coates, *The Air Force in SILICO: Computational Biology in 2025* (Maxwell AFB, AL: Air University Press, 2007); Shane Courville, *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future* (Maxwell AFB, AL: Air University Press, 2007); Mark S. Danigole, *Biofuels: An Alternative to US Petroleum Dependency* (Maxwell AFB, AL: Air University Press, 2007); and Vincent T. Jovene, *Next Generation Nanotechnology Assembly Fabrication Methods: A Technology Forecast* (Maxwell AFB, AL: Air University Press, 2008).

6. Organisation for Economic Co-operation and Development (OECD). The United States ranks last among OECD countries in reading, 27th in math (between Russia and Portugal), and 22nd in science (between Iceland and the Slovak Republic).

7. Thomas L. Friedman, "The Ten Forces That Flattened the World," in *The World Is Flat: A Brief History of the 21st Century* (New York: Farrar, Straus and Giroux, 2007), 51–199.

8. Estimates of the numbers of these groups vary widely. The lowest estimate the authors encountered in their research was 13,425. See *The United Nations Today* (New York: United Nations Department of Public Information, 2008). Mainstream estimates are in the range of a few tens of thousands, with some upper-end estimates around 60,000. See Marlies Glasius, Helmut-Anheier, and Mary Kaldor, "Introducing Global Civil Society," *Global Civil Society Yearbook 2001* (Oxford, UK: Oxford University Press, 2001), 2–38.

9. Two computers have, arguably, successfully passed a version of the Turing test wherein a computer mimics human behavior so closely that in a blind test observers cannot discern which actor in a lineup is the computer. The most recent event was in 2014, when "Eugene Goostman," a chat bot designed by Vladimir Veselov and Eugene Demchenko, successfully convinced judges after a five-minute interview that it was a human. "Turing Test Passed by Computer," *CBCNews*, 9 June 2014, http://www.cbc.ca/news/technology/turing-test-passed-by-computer-1.2669649. For details on the nature of the test, see Alan M. Turing, "Computing Machinery and Intelligence" in *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*, ed. Robert Epstein, Gary Roberts, and Grace Beber (Dordrecht, Netherlands: Springer, 2009), 23–66. The other computer sometimes argued as having passed the test is Watson. See Ray Kurzweil, "The Significance of Watson," *Kurzweil Accelerating Intelligence* (blog), 13 February 2011, http://www.kurzweilai.net/the-significance-of-watson. It is worth noting that Kurzweil believes that the Loebner threshold for passing the Turing test is too low but that genuine human intelligence will be reached by 2029.

10. US Census Bureau, Department of Commerce, "U.S. & World Population Clocks," accessed 12 May 2012, http://www.census.gov/main/www/popclock.html.

11. Matt Ridley, "Humans: Why They Triumphed," *Wall Street Journal*, 22 May 2010, http://online.wsj.com/article/SB10001424052748703691804575254533386933138.html; Matt Ridley, *The Rational Optimist: How Prosperity Evolves* (New York: HarperCollins, 2010), and Anthony Hallam and Paul B. Wignall, *Mass Extinctions and Their Aftermath* (Oxford, UK: Oxford University Press, 2002). Based on Hallam and Wignall's calculations, the combined extinction loss from the five major extinction events (End-Ordovician [84 percent], Late Devonian [83 percent], End Permian [95 percent], End Triassic [80 percent], and End Cretaceous [76 percent]) would be 99.994 percent. This figure does not include the background extinction rate of those species that died out between these events, which would raise this figure still higher.

12. Peter Schwartz, *The Art of the Long View* (New York: Doubleday, 1991), 17–169.

13. Peter Schwartz, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence* (New York: Gotham Books, 2003).

14. Human Genome Program, Office of Biological and Environmental Research, Department of Energy, "Human Genome Project Information," 21 March 2014, http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml.

15. Michael B. Miller, "How Tall of a Stack of Paper Would We Need to Print Out an Entire Human Genome?," working paper (Minneapolis: Division of Epidemiology and Community Health, University of Minnesota, 15 October 2005), http://bio4.us/biotrends/human_genome_height.html.

16. Human Proteome Organisation (HUPO), "Human Proteome Project (HPP)," HUPO, 21 March 2012, accessed 11 June 2016, http://www.hupo.org/research/hpp/.

17. BBC, "Mouse Pox or Bioweapon?" *BBC World Service*, 17 January 2001, accessed 12 June 2016, http://www.bbc.co.uk/worldservice/sci_tech/highlights/010117_mousepox.shtml.

18. William Bains, *Biotechnology from A to Z* (New York: Oxford University Press, 2004), 52.

19. The dictionaries issued to the authors by the federal government are among those that do not yet contain an entry for nanotechnology.

20. J. Hall Stores, *Nanofuture: What's Next for Nanotechnology* (Amherst, NY: Prometheus, 2005), 15–22.

21. Ibid, 15–51.

22. Leading biological scientists, interviews.

23. Witold Gutkowski and Tomasz A. Kowalewski, *Mechanics of the 21st Century: Proceedings of the 21st International Congress of Theoretical and Applied Mechanics*, Warsaw, Poland, 15–21 August 2004 (Dordrecht, Netherlands: Springer, 2005), 379; and Oleg Vasylkiv, Yoshio Sakka, and Valeriy V. Skorokhod, "Nano-Blast Synthesis of Nano-size CeO2-Gd2O3 Powders," *Journal of American Ceramic Society* 89, no. 6 (June 2006): 1822–26.

24. John W. Cole, Isaac F. Silvera, and John P. Foote, "Conceptual Launch Vehicles Using Metallic Hydrogen Propellant," *American Institute of Physics Conference Proceedings* 969 (2008): 977–84.

25. It is interesting to note that a yield increase of 1,000-fold would create a set of conventional ordnance with yields in excess of the bombs dropped on Hiroshima and Nagasaki during World War II. This would necessitate revisiting the question of what constitutes a weapon of mass destruction.

26. Ancel Yarbrough, *The Impact of Nanotechnology Energetics on the Department of Defense by 2035* (Maxwell AFB, AL: Air War College, 2010), http://www.au.af.mil/au/awc/awcgate/cst/bh2010_yarbrough.pdf.

27. Henry D. Baird et al., "Spacelift 2025: The Supporting Pillar for Space Superiority," in *Air Force 2025*, vol. 2 (Maxwell AFB, AL: Air University Press, 1996), 117–50.

28. Of course nanotechnology, like biotechnology above, can cut both ways. The same basic science that can create nanocorrosives can also create nanocoatings that would make systems resist corrosion. There are over 30,000 scholarly articles on this subject. Among the more heavily cited are S. Radhakrishnana, C. R. Sijua, Debajyoti Mahantab, Satish Patilb, and Giridhar Madras, "Conducting Polyaniline-nano-TiO2 Composites for Smart Corrosion Resistant Coatings," *Electrochimica Acta* 54, no. 4 (30 January 2009): 1249–54; Lidia Beneaa, Pier Luigi Bonorab, Alberto Borelloc, and Stefano Martelli, "Wear Corrosion Properties of Nano-Structured SiC-Nickel Composite Coatings Obtained by Electroplating," *Wear* 249, no. 10–11 (November 2001): 995–1003; and Martin Kendig, Melitta Hon, and Leslie Warren, " 'Smart' Corrosion Inhibiting Coating," *Progress in Organic Coatings* 47, no. 3 (September 2003): 183–89.

29. House of Representatives, *Electromagnetic Pulse Threats to U.S. Military and Civilian Infrastructure: Hearing before the Military Research and Development Subcommittee of the Committee on Armed Services*, 106th Cong., 1st sess., 7 October 1999 (prepared statement of Lowell Wood, member of director's technical staff, Lawrence Livermore National Laboratory), 30–36. See also John P. Geis II, *Directed Energy Weapons on the Battlefield: A New Vision for 2025* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2003), 8–11.

30. Ibid.

31. A. Barrie Pittock et al., "Direct Effects of Nuclear Detonations," in *Environmental Consequences of Nuclear War, vol. 1*, eds. A. Barrie Pittock, Mark Harwell, and T. C. Hutchinson (New York: John Wiley and Sons, 1986), 1–23.

32. Geis, *Directed Energy Weapons*, 9.

33. Pittock et al., "Direct Effects of Nuclear Detonations," 17–20; and Geis, *Directed Energy Weapons*, 11–14.

34. For a discussion on the precise field strengths to cause specific amounts of damage, see Geis, *Directed Energy* Weapons, 11–15.

35. There is a method to harden computer chips against this phenomenon, but such hardening is expensive, and very few foundries in the world produce these chips.

36. Carlo Kopp, "The Electronmagnetic Bomb—A Weapon of Electrical Mass Destruction," *Air and Space Power Journal: Chronicles Online Journal*, 1996, http://www.airpower.au.af.mil/airchronicles/cc/apjemp.html.

37. Geis, *Directed Energy Weapons*, 11–15.

38. No endorsement of the product being discussed is intended or implied. The products listed here are dangerous and require substantial training to handle safely. For academic purposes, additional data may be found at Wicked Lasers, "Spyder Arctic," accessed 12 June 2016, http://www.wickedlasers.com/arctic. Following our initial research, a new company began marketing an even smaller laser that is much more powerful than the Spyder. Its laser creates temperatures of up to 850 degrees at the point of lasing, which the newly upgraded Arctic Laser (now $199) at 2 watts of power is now also capable of attaining.

39. The authors searched for importation restrictions on lasers across the world. While it is possible some were missed, after an exhaustive search, only the country of Malta had laws we could locate that prevented the importation of a category-IV device.

40. The authors presented early findings at the Aircraft Survivability Conference in Berlin, Germany, 13 October 2010. Discussions with members of the German parliament who were present revealed concern over recent lasing incidents on the autobahn. These government leaders were unaware of the newly marketed handheld device.

41. Matthew Potter, "Boeing Video of Advanced Tactical Laser (ATL) Aircraft," *Defense Procurement News*, 2 October 2009, accessed 12 June 2016, http://www.defenseprocurementnews.com/2009/10/02/boeing-video-of-advanced-tactical-laser-atl-aircraft.

42. Geis, *Directed Energy Weapons*, 16.

43. William Diehl, *Continued Optical Sensor Operations in a Laser Environment* (Maxwell AFB, AL: Air War College, 2011), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA570475.

44. The authors believe this may be the first structural model of deterrence, laid out in a manner that would invite future value model-based research. We derived the model primarily from the following scholars and works (the list is not exhaustive): Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900–1989," *World Politics* 36, no. 4 (July 1984): 496; Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press, 2004); Christopher Layne,

"From Preponderance to Offshore Balancing," in *The Use of Force: Military Power and International Politics*, 7th ed., ed. Robert J. Art and Kenneth N. Waltz (Lanham, MD: Rowman and Littlefield Publishers, 2009), 311–26; Andrew J. Goodpaster, C. Richard Nelson, and Seymour J. Deitchman, "Deterrence: An Overview," in *Post–Cold War Conflict Deterrence* (Washington, DC: National Academy Press, 1997), 10–38; Keith B. Payne, *The Fallacies of Cold War Deterrence* (Lexington: University Press of Kentucky, 2001); Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Longman, 1999); John P. Geis II et al., *Discord or "Harmonious Society"? China in 2030*, (Maxwell AFB, AL: Air University Press, 2011); Bruce Russett and Alan C. Stam, "Courting Disaster: An Expanded NATO vs. Russia and China," *Political Science Quarterly* 113, no. 3 (Fall 1998): 361–82; Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008); Union of Concerned Scientists, "Nuclear Weapons & Global Security: History of Russia's Anti-Ballistic Missile System," 2012, http://www.ucsusa.org/nuclear_weapons_and_global_security/missile_defense/policy_issues/history-of-russias.html; Yao Yunzhu, "Chinese Nuclear Policy and the Future of Minimum Deterrence," *Pacific Forum CSIS* 6, no. 2 (September 2005): 31–40, http://csis.org/files/media/csis/pubs/issuesinsights_v06n02.pdf; Kenneth N. Waltz, "Nuclear Myths and Nuclear Realities," in *The Use of Force: Military Power and International Politics*, 6th ed., eds. Robert J. Art and Kenneth N. Waltz (Malden, MA: Rowman and Littlefield, 2004), 102–18; Bob Gourley, "Towards a Cyber Deterrent" (working paper, Cyber Conflict Studies Association, Vienna, VA, 29 May 2008), http://www.ctovision.com/cyber-deterrence-initiative.html; Thomas P. M. Barnett, "Deterrence in the 21st Century," in *Deterrence 2.0: Deterring Violent Non-State Actors in Cyberspace*, ed. Carl Hunt and Nancy Chesser (Washington, DC: US Strategic Command Global Innovation and Strategy Center, 10 January 2008), 25–31; Edward D. Mansfield, *Power Trade and War* (Princeton, NJ: Princeton University Press, 1994); John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1985); Jack S. Levy, "The Causes of War: A Review of Theories," in *Behavior, Society and Nuclear War*, vol. 1, edd. Philip E. Tetlock et al. (New York: Oxford University Press, 1989), 209–333; A. F. K. Organski and Jacek Kugler, *The War Ledger* (Chicago: University of Chicago Press, 1980); Michael W. Doyle and Stephen Macedo, *Striking First: Preemption and Prevention in International Conflict* (Princeton, NJ: Princeton University Press, 2008); T. V. Paul, Patrick M. Morgan, and James J. Wirtz, eds., *Complex Deterrence* (Chicago: University of Chicago Press, 2009); and Anthony C. Cain, ed., *Deterrence in the Twenty-First Century: Proceedings* (Maxwell AFB, AL: Air University Press, 2010).

45. Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems, US-USSR, 26 May 1972, accessed 13 June 2016, http://www.state.gov/t/isn/trty/16332.htm.

46. Mearsheimer, *Conventional Deterrence*, 23

47. This calculus can be traced to Thucydides, who lamented in the fifth book of his *History of the Peloponnesian War* that in war "one side thinks that the profits to be won outweigh the risks to be incurred, and the other side is ready to face danger rather than accept an immediate loss." Cited in Athanassios G. Platias and Constantinos Koliopoulos, *Thucydides on Strategy: Grand Strategies in the Peloponnesian War and Their Relevance Today* (New York: Columbia University Press, 2010), 125.

48. Harold H. Kelly, "The Process of Causal Attribution," *American Psychology* 28, no. 2 (1973): 107–28; Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (27 September 1974): 1124–31; and Rich-

ard Nisbett and Lee Ross, *Human Interference: Strategies and Shortcomings of Social Judgment* (Englewood Cliffs, NJ: Prentice Hall, 1980).

49. Irving L. Janis and Leon Mann, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment* (New York: Free Press, 1977); Daniel Heradstveit and G. Matthew Bonham, "Decision-Making in the Face of Uncertainty: Attributions of Norwegian and American Officials," *Journal of Peace Research* 23, no 4. (December 1986): 339–56.

50. Briefing, John R. Boyd, subject: A Discourse on Winning and Losing, 1987, accessed 13 June 2016, http://dnipogo.org/john-r-boyd/.

51. Norman Dalkey and Olaf Helmer, *An Experimental Application of the Delphi Method to the Use of Experts* (Santa Monica, CA: RAND, July 1962); and Harold A. Linstone and Murray Turoff, eds., *The Delphi Method: Techniques and Applications* (University Heights: New Jersey Institute of Technology, 2002).

52. William D. Rogers, "The Principles of Force, the Force of Principles," in *Right v. Might: International Law and the Use of Force*, ed. Louis Henkin et al. (New York: Council on Foreign Relations, 1991), 95–108.

53. This type of thinking can also be found in Ali Karami, "Pandemics and Its Consequences for the Future of Asia," in *Imagining Asia in 2030: Trends, Scenarios and Alternatives*, ed. Ajey Lele and Namrata Goswami (New Delhi, India: Academic Foundation Press, 2011), 153–65; and Angela Woodward, "Biological and Chemical Terrorism," in *Imagining Asia in 2030: Trends, Scenarios and Alternatives*, ed. Ajey Lele and Namrata Goswami (New Delhi, India: Academic Foundation Press, 2011), 323–35.

54. "Wayback Machine," *Internet Archive* (web site), n.d., accessed 24 April 2012, http://archive.org/web/web.php.

55. Peter Ho and Adiran W. J. Kuah, "Governing for the Future: What Governments Can Do," *Prism* 5, no. 1 (2014): 8–21.

56. See Risk Assessment and Horizon Scanning (RAHS) Programme Office, Government of Singapore, "About Us: Vision, Mission & Values," 13 January 2012, accessed 24 April 2012, http://app.rahs.gov.sg/public/www/content.aspx?sid=2951; and RAHS Programme Office, Government of Singapore, "Organisation Structure Website," 30 March 2012, accessed 13 June 2016, http://app.rahs.gov.sg/public/www/home.aspx.

57. John P. Geis II, Grant T. Hammond, Ted C. Hailes, and Harry Foster, "Blue Horizons III: The Age of Surprise" (unpublished briefing given to AF/A8, April 2010).

Disclaimer