

Blue Horizons IV

Deterrence in the Age of Surprise

EXECUTIVE SUMMARY

by

Dr. John P. Geis II
Dr. Grant T. Hammond
Harry A. Foster
Theodore C. Hailes

January 2014

The Occasional papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 71 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, Alabama 36112, or on the CSAT web site at <http://csat.au.af.mil/> The fax number is (334) 953-6158; phone (334) 953-6150.

Occasional Paper No. 70
U.S. Air Force Center for Strategy and Technology

Air University
Maxwell Air Force Base, Alabama 36112

Disclaimer

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of Air University, the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Disclaimer	ii
Contents	iii
Figures.....	iv
About the Authors.....	v
Preface.....	vii
Executive Summary	vii
Introduction.....	1
Background	4
Threats in the Age of Surprise	8
A Structural Model of Deterrence.....	20
The Delphi Study and Results.....	23
Findings & Implications for the U.S. Air Force	27
Recommendations.....	33
Issues for Other Departments.....	35
Summary.....	36

Figures

Figure 1: Research Team Composition by Specialty.....	2
Figure 2: Study Design -- Matrix of Technologies versus Actors.....	3
Figure 3: Number of Transistors per Microprocessor.....	4
Figure 4: The J-Curve and Exponential Change.....	5
Figure 5: Change in Technology Competitiveness 1993-2007.....	6
Figure 6: Warfare is Changing.....	7
Figure 7: Generator During Aurora Test at Idaho National Laboratories.....	9
Figure 8: White Nano-Particles.....	14
Figure 9: Transformer Damage from Solar Flare.....	16
Figure 10: Impact of a May 1921-Class Solar Flare on U.S. Electric Grid.....	17
Figure 11: Spyder Arctic III Blue Laser.....	18
Figure 12: A Structural Model of Deterrence Theory.....	20
Figure 13: The Deterrence Equation.....	21
Figure 14: Difficulty of Deterrence Delphi Results.....	24
Figure 15: Difficulty of Attribution Delphi Results.....	25
Figure 16: Likelihood of Catastrophic Attack Delphi Results.....	26
Figure 17: Delphi Study Threat Data in 3-D.....	27
Figure 18: How Transparency Operates.....	29
Figure 19: Al Udeid Air Base, Qatar on 17 Sept 2009.....	31

About the Authors

Dr. John P. Geis, II, Colonel, USAF (ret.) is a Professor, Air Force Research Institute, and the former Director of the Air Force Center for Strategy and Technology at Maxwell AFB. He retired in 2011 after serving more than 27 years in uniform. Dr. Geis has served as an instructor, weapons systems officer, navigator and fire control officer on such aircraft as the F-111A, F-111E, T-37, AT-38B, T-43, and AC-130H. Operationally, he served as a planner for Operation ELDORADO CANYON, flew combat missions over Bosnia-Herzegovina, and commanded the joint and combined special operations task force that replaced the Independence Carrier Battle Group on the Korean Peninsula. In 1996, Colonel Geis co-authored the Alternate Futures Monograph for the Chief of Staff-directed *Air Force 2025* study. Shortly thereafter, he served as Chief, Strategic Planning, Doctrine, and Force Integration Branch at Headquarters Air Force Special Operations Command, leading all long-range planning, doctrine development, and joint force integration for all Air Force Special Forces. Dr. Geis graduated from the Air War College in 2001 and with the exception of an education sabbatical, has served as the Director of the Center for Strategy and Technology since that time. He is the author or editor of nearly two dozen Air university Press books and monographs. Dr. Geis has a Bachelor of Science Degree in Meteorology from the University of Wisconsin, a Master of Political Science Degree from Auburn University, a Master of Strategic Studies Degree from the Air War College, and both a Master of Arts and a Doctor of Philosophy Degree in Political Science from the University of Wisconsin.

Dr. Grant T. Hammond is Deputy Director of the USAF Center for Strategy and Technology (CSAT) and Professor of International Security at the Air War College (AWC). Dr. Hammond received his BA from Harvard, and an MA and Ph. D. from the School of Advanced International Studies of the Johns Hopkins University. Prior to coming to the Air War College, Dr. Hammond was Chairman of the International Studies Department at Rhodes College and Executive Officer at the Center for International Affairs at Harvard University. He left CSAT and the AWC in 2007 to be Dean and Deputy Commandant of the NATO Defense College in Rome, Italy until returning in late 2010. Dr. Hammond has written three books—*Countertrade Offsets and Barter in International Political Economy* (1990, PB 1993); *Plowshares into Swords: Arms Races in International Politics, 1840-1991* (1993); and *The Mind of War: John Boyd and American Security* (2001, reprinted in PB 2004 and 2007)—and authored numerous book chapters, articles and briefings. He has addressed all the US armed services Command and Staff Colleges and War Colleges as well as military and civilian audiences in Belgium, Germany, Italy, Jordan, Morocco, the Netherlands, Romania, Singapore, Sweden, and the UK.

Harry A. Foster is the Deputy Director of the Center for Strategy and Technology. Prior to joining CSAT, he served as the Chief of Strategy for US Air Forces Central Command at Al-Udeid AB, Qatar. While a student at the Air War College at Maxwell AFB, AL in

2008, he co-authored the Executive Summaries for the last two USAF *Blue Horizons* studies. A combat experienced instructor pilot in three aircraft (F-16, B-2 and B-1), he has commanded an Operations Support Squadron and served in the Air Staff's Checkmate Division. He holds graduate degrees from Marine Command and Staff College at Quantico, Virginia where he was a distinguished graduate, the School of Advanced Air and Space Studies at Maxwell Air Force Base, Alabama, and the Harvard Kennedy School at Cambridge, Massachusetts and the Air War College where he graduated with Highest Distinction.

Colonel (R) Theodore C. Hailes is the Force Transformation Chair at Air University and a founding member of the Center for Strategy and Technology. In addition to his work in technology, he is also on the faculty of the Air War College teaching courses on National Security Decision Making, International Security Studies, and Regional Studies Field Seminars. He retired from the Air Force in 1996 completing a thirty-year tour. During that time he flew the F-4, O-2A, F-5 and the F-15 accumulating over 4,000 hours of which 500 were in combat. He served in Vietnam as a Forward Air Controller with the 2nd Brigade, 101st Airborne Division, and finished his fighter career as Squadron Commander of the 22TFS and then Director of Operations of the Northeast Air Defense Sector. He served in two staff tours; the Pentagon from 1979-1983 where he worked in International Programs and was Executive Officer for AF/A8; and with the Air War College from 1990-1996 where he was a department chairman and Associate Dean of Faculty. He returned to the Air War College faculty in a civilian capacity in 1997 and has worked there since. His military educational background includes SOS (Resident - 1972), Air Command and Staff (Seminar - 1981) and Air War College (Resident - 1987). His civilian education includes a BA in History from Denison University and a MS in International Relations from Troy University. His principle areas of interest in the academic world have been in International Relations and the strategic implication of accelerating technological change.

Preface

In 1996, the Air Force initiated a major study effort under the direction of General Ronald Fogleman, the Air Force Chief of Staff (CSAF). That study, *Air Force 2025*, looked 30 years into the future and made enormous contributions toward directing Air Force research and procurement.

In 2007, General T. Michael Mosley, Air Force Chief of Staff, directed a continuous series of future oriented study efforts be undertaken, using Air University (AU) as the “Air Force’s think tank.” This study, *Blue Horizons*, was commissioned by the United States Air Force (USAF) Chief of Staff, to provide “a new look at the future.” Specifically, the Chief of Staff asked the research team to provide “a common understanding of future strategic and technological trends for Air Force leaders to make better decisions.” The Chief also sought to “confirm AU as [the Air Force’s] in-house think tank” and to improve the relevance of Air Force education to the decision-making processes in Washington.¹

A team of 46 officers from the Air Force and the sister services participated in the study during their one-year Masters Degree professional military education program. They examined the question of, “How should the Air Force best posture itself to deter threats by traditional and new weapons of mass destruction or disruption with an eye toward the mid 2030s?”

The authors collectively led the effort and spent the year researching and traveling to identify the range of challenges posed by accelerating exponential technological change and how these changes will modify the types of weapons that may have catastrophic effects in the next 20-30 years. They then examined deterrence theory to determine if this theory would still apply to the new weapons types. Lastly, the authors recommend a new way to apply deterrence theory to counter the wide range of threats that could significantly damage the United States and her interests in the years to come.

Executive Summary

This study examines the implications of exponential technological change on the panoply of threats the U.S. Air Force may have to face in the future, and how the Air Force should posture itself to best deter those threats. Specifically, this study

- Due to the proliferation of disruptive technologies, examines the changes in the array of threats for which deterrence will be needed in the future.
- Explores the relevance of deterrence theory to both existing and new threats, some of which may surpass nuclear weapons in the risk they pose to both the U.S. and humankind.
- Recommends new ways of applying deterrence theory in order to reduce the risk that new disruptive technologies will be used against the U.S. or its interests.

Building on previous *Blue Horizons* studies, this study assumes science and technology (S&T) growth will continue and will drive proliferation of advanced and potentially dangerous technologies. It posits that the result of rapid advances in nanotechnology, biotechnology, directed energy, space, computers and communications technologies may prove to be particularly dangerous. These developments span the private sector and many nations.²

Globalization in the areas of finance, communications, education, industry, trade, governance, and myriad other areas is facilitating the rapid spread of new technologies among nations, groups, and individuals.³ Actors in unstable states and terrorists may use these technologies in malevolent ways to directly threaten U. S. national security and that of friends and allies.⁴ This threat will take the Air Force back to its roots, which began in Intelligence, Surveillance, and Reconnaissance (ISR).

Of principle concern by the year 2035 are threats in six separate areas: Nuclear weapons, attacks in cyberspace, directed energy weapons, space systems, nanotechnology, and biotechnology. Each of these poses the risk of catastrophic attack to the U.S., her citizens, and/or her infrastructure.

Deterring threats posed by nations, groups, and individuals will require new thinking regarding the application of deterrence theory. Fundamentally, deterrence theory suggests that an actor is deterred from attacking a target if (s)he believes that the risk or cost of retribution outweighs the gains to be achieved by carrying out the attack. As such, deterrence theory has always contained two primary branches. One is deterrence by retribution – the cost one can impose on the attacker for either carrying out an attack or making the attempt to do so. The other is deterrence by denial – the ability to deny an adversary the opportunity to attack, or having sufficient resiliency that little is to be gained even if the attack is successful. Each of these branches can affect the deterrence calculus. This study examines the interplay between the six technology threat areas and how deterrence theory applies.

Historically, deterrence theory as it applies to nuclear weaponry has relied almost exclusively on deterrence by retribution. This was necessary, as by treaty each side in the cold war had more weapons than the other had interceptors to protect from those weapons. The result was an implicit assumption that avoiding a devastating attack was impossible. As a result, deterrence with respect to nuclear weapons has historically relied on a credible threat of a massive retaliatory response, the costs of which would be so great that no rational adversary would ever initiate such an attack, as the costs would outweigh the gains to be won. At times, this philosophy was known as mutually assured destruction (MAD). However, this historical thinking focuses on only one-half of the deterrence equation, and this is inappropriate in dealing with the newer threats.

This study finds that deterrence by denial has significant leverage vis-à-vis the newly emerging technological threats. Unlike nuclear weapons, it is possible to deny an adversary the capability, opportunity, and the ability to create significant effects using most new technologies if the appropriate steps are taken in advance. In short, it is possible to significantly mitigate the gains to be achieved by attacking, and thus change the deterrent calculus in the mind of a prospective adversary. As a result, deterrence by denial now needs to be considered as an integral part of deterrence strategy by the United States, and by extension, its Air Force.

Study Scope

Entitled *Deterrence in the Age of Surprise*, this study examines the impact of exponential technological change on potentially catastrophic threats to the United States and her interests, and makes recommendations on how the Air Force should best posture itself to aid the U.S. in deterring these new threats. This study's research team, with more than 650 years of combined airpower and military experience, examined the context of the future strategic environment and researched threats across six technology areas in-depth: nuclear weapons, biotechnology, nanotechnology, directed energy technologies, space systems, and cyberspace systems. They evaluated the nature and extent of the potential threats posed in each of these areas, and examined the relevance and application of existing deterrence theory to these new threats. From this analysis of deterrence theory, the study makes policy recommendations that will enhance the likelihood that the U.S. will be able to deter future attacks across this wide range of technologies from nation-states, groups and individuals.

This study employs the Delphi Study method pioneered by RAND. It highlights the real dangers posed by adversary nations, groups, and individuals possessing advanced technologies. The study 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 these groups to overcome the tyranny of distance and make it easier to discover, act, surprise, and target almost any place on earth. The study concludes that deterrence of individuals will be more difficult than that of groups or nation-states, but that with the most dangerous of new technologies, the greatest likelihood of catastrophic attack is likely to be posed by groups. The study re-confirms that more than three-fourths of all technology research and development is now conducted outside the United States, making it increasingly difficult for DOD to control technology proliferation.

Study Conclusions

The chapters that follow detail the data, findings, analysis and conclusions of the research team. Vetted by senior scientists from the national laboratories and the Air Force Research Laboratory, the contents have been peer-reviewed by technical experts around the world. Based on an in-depth analysis of the six major technology areas, the research team reached the following conclusions and makes the following recommendations:

National critical infrastructure is vulnerable to attack in space (communications), via cyberspace, and via directed energy weapons. The latter two hold the potential to cause permanent damage to parts of the infrastructure, rendering it inoperative for periods ranging from months to years. Additional efforts to guard this infrastructure are required.

While nanotechnology is often thought of as a technology that makes all other things better, it holds the promise and threat of being able to pack large amounts of energy into small spaces. From a battery or space-lift perspective, it offers the ability to solve some of our most important technological challenges. From a weapons perspective, it may enable the creation of bombs that can destroy civilian airliners to be miniaturized to the size of a small coin. This poses risk to the nation's transportation infrastructure upon which all commerce depends.

Nuclear weapons are unlikely to disappear in the next 20-30 years. As in the past, proliferation is likely to continue. In addition to the current nine nuclear states on Earth, others, particularly Iran, appear interested in acquiring this technology. Ensuring weapons remain under the control of the governments that created them will be a key challenge in the future.

The most dangerous technology is nano-enabled biotechnology. While the nexus of these two sciences has already produced extremely effective medicines for certain types of cancer and will likely cure other diseases in time, the same technologies that can cure disease can also be perverted to cause it. With the “Rosetta Stone” for the human genome only a handful of years away, the world is entering an era where it is possible to design a perfectly lethal virus for which no immunity exists. By 2030 this capability could reside in the hands of a masters degree holder in microbiology.

Deterring nation-states, groups and individuals from using these technologies in ways that would cause catastrophic harm to society is of national importance. While more than merely an Air Force problem, the Air Force has a major role to play in providing the nation the necessary capabilities to make successful deterrence more likely.

The Air Force’s roots begin with observers in balloons overlooking battle lines in World War I, conducting surveillance and reconnaissance of the adversary, and using this information to guide military operations on the ground below. This same fundamental core competency, now called “information superiority” is able to monitor potential adversaries and attribute their activities and strike them as needed, is extremely important in successfully deterring an adversary strike. As it did in the first two World Wars, the Air Force must again pioneer new methods of conducting intelligence, surveillance, and reconnaissance of our adversaries to make certain that they know that no attack will go unnoticed, unattributed, or undetected.

Secondly, the Air Force needs to make itself more resilient in the face of potential adversary attack. In a process this study refers to as immunization, the Air Force needs to assess the risks it is currently taking vis-à-vis these new technology threats with regards to its interdependence with other services and the national critical infrastructure for key functions. Once these risks are mapped, research and development will be required to mitigate the risks to make the Air Force, and by extension the U.S., less vulnerable to an adversary attack.

The study concludes that by making it more likely that an adversary will be accurately attributed, ideally before an attack is launched, and by making it less likely that significant damage would occur in such an attack due to greater system resiliency, adversaries will find launching an attack a risky option with little payoff. In short, they are more likely to be deterred. By increasing the likelihood that future adversaries will find themselves deterred, this will decrease the likelihood that such an attack would ever take place. Greater detail on what these threats are, how they could be implemented, and what steps the Air Force can take to begin the process of readying itself for the future are contained in the pages that follow.

Introduction

This study is the fourth in the *Blue Horizons* series. This series explores topics of interest to the Chief of Staff and senior leadership of the Air Force, and recommends solutions to strategic challenges created by emerging technologies.

In the Spring of 2009, the Air Force Center for Strategy and Technology began discussions with the Air Staff regarding the findings of the first two *Blue Horizons* studies.⁵ In these discussions, concerns were raised by the Deputy Chief of Staff for Plans and Programs, then Lieutenant General Raymond Johns, that a new examination of how deterrence operated in the future was necessary. The topic of study for 2010 was derived from these discussions and the memoranda that followed.

This study examines the question, “How should the Air Force best posture itself to assist the nation in deterring nation-states, groups, and individuals from attacking the United States in space or cyberspace, or by using nuclear, nanotechnological, biotechnological or directed energy weapons from now to the year 2035?” This monograph discusses what has become known as “the future deterrence study” inside the Air Force to include the methods of examination used, the findings surrounding these emerging technologies and the conclusions as to how the Air Force best postures itself to deter the “threats of the responsibly imaginable.”⁶

Methodology

The *Blue Horizons IV* study draws upon extensive background research, site visits to the U.S. Air Force and National Laboratories, interviews with scientists, researchers, policy analysts, senior officials in agencies across the “whole of government,” and engineers building the technologies that will help shape the future strategic environment.⁷ The team of 35 researchers spanning two colleges, and five faculty, began with a search across the science and technology, education and training, governmental policy, organizational culture, national strategies, and military studies literatures.⁸ The research team was deliberately selected for its breadth of expertise across all relevant military specialties. The team composition is in Figure 1 below.

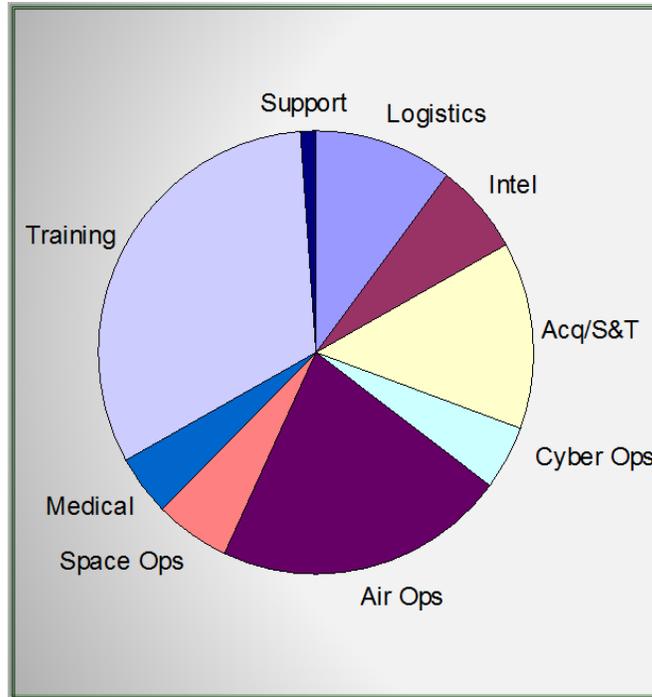


Figure 1: Research Team Composition by Specialty

These researchers also visited three of the major national laboratories.⁹ In addition, the team visited seven of the ten Air Force Research Laboratory directorates, including those responsible for research in Space Vehicles, Directed Energy, Materials Sciences, Human Factors Engineering, Propulsion, Air Vehicles, and Sensors. In each, presentations were made by senior scientists; and the researchers had time to discuss and interview these scientists regarding current projects, as well as those that were in the conceptualization stages. This research helped define the range of technologies likely to be available in the field in the 2030-2035 timeframe, for which this study was commissioned.

Once equipped with this understanding of the threat environment of the future, the research team embarked on research specific to the technological threat across six technology areas and across three types of actors. Specifically, the team examined nanotechnology, nuclear weapons, directed energy technologies, space systems, cyberspace as a domain and as a set of systems and biotechnology. These six technological areas were researched as they pertained to potential threats from three actor types, namely nation-states, groups, and individuals. This created a matrix of 18 squares that required detailed examination (figure 2). Two of the eighteen boxes were eliminated early in the study. Nuclear weapon threats from single individuals were ruled as implausible on two grounds. First, it is improbable for a single person to produce such a weapon, the threshold of a group for study definition purposes. Similarly, space attack by a single individual was deemed unlikely in the study timeframe as the team concluded the infrastructure and materials needed to successfully carry out such an attack would exceed the capacity of a single individual.

Category	Nano	Nuclear	DE	Space	Cyber	Bio
Nation						
Group						
Individual						

Figure 2: Study Design -- Matrix of Technologies versus Actors

The team, initially divided into sub-groups to conduct the specific research above, was later re-combined to conduct a more holistic look at the challenges presented across the matrix. The team built a structural model of deterrence, and then embarked on a formal Delphi study, followed by an informal version of the Delphi method to evaluate risks and opportunities to deter across the various boxes of the matrix.¹⁰ The formal Delphi study lasted three rounds before convergence was found on the values and was thus terminated. The informal Delphi discussions took place across five rounds of approximately three hours duration each. The former generated 3528 data points for quantitative analysis; the latter helped add a qualitative understanding to the meaning of the quantitative figures.

In the end, the team concluded that the greatest future risks lie not in the area of nuclear weapons, though threats there do remain; but rather in areas of biotechnology and in cyberspace. The team also found that while the body of literature on deterrence theory remains valid for future threats, the areas of focus to put the theory into practice will change in the years ahead.

Overview

This paper begins with a discussion of conclusions reached in previous *Blue Horizons* studies that are applicable to deterring threats emanating from new and emerging technologies. Here, the paper will briefly discuss the rapidly changing nature of technology, its proliferation, and the developmental challenges associated with having only a small percentage of global research and development within one's military portfolio. It will then delve into the nature of the threats across the six technological areas the Center was asked to examine. The paper will discuss the types of attacks that will be possible over the next 20 years, what the effects upon the national critical infrastructure and the population could be, and enable the reader to understand the breadth and depth of the challenges faced.

The paper will then introduce a structural model of deterrence. Based on the writings of many of the preeminent deterrence theorists over the past 60 years, this model dissects the concept of deterrence into its component parts, and is a useful analytic tool to determine how best to address each of the threats discussed. Through the lens of Air Force history, the paper will recommend two main areas of emphasis for the Air Force as it seeks to better posture itself to deter threats across these technological realms or domains. It will conclude with a specific set of recommendations that were presented to the Air Force Chief of Staff. Finally, the paper will conclude with a few areas where further research or actions are required, as the Air Force is not the only agency that has a role in this process, and while the Air Force can make a major difference, action by other governmental agencies is also required to create an optimum deterrent posture.

Background

In the first year of the *Blue Horizons* program, entitled *Horizons 21*, the Center for Strategy and Technology (CSAT) examined a broad range of emerging technologies. The researchers found that improvements in the underlying science were happening across the entire range of sciences at an exponential rate. The researchers concluded then that the capabilities available to 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.

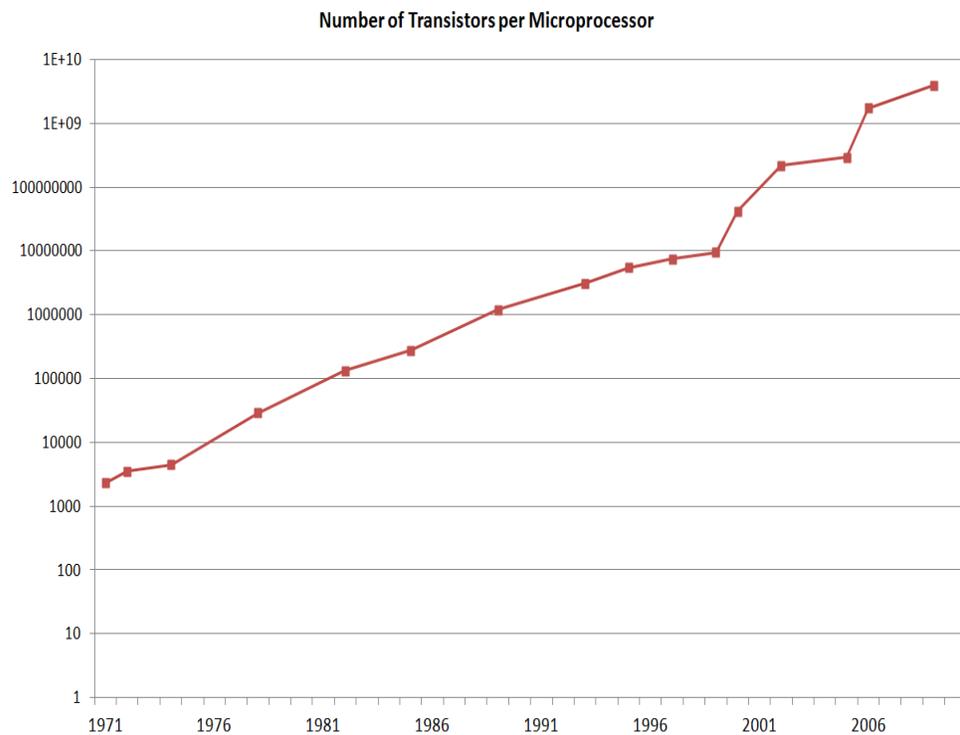


Figure 3: Number of Transistors per Microprocessor¹¹

One of the principle 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. Presented in *Blue Horizons III*, the research team again discovered what is often called the “J Curve.”¹² Figure 3 above shows the number of transistors per microprocessor on a base 10 logarithmic graph. Each horizontal line represents a 10-fold increase over the line below. On this graph, technological change looks like a straight line. When this, or similar technologies are plotted on linear axes, as in figure 4 below, the curve takes on the appearance of the letter “J,” from which this curve gets its name. As with the number of transistors on a microprocessor and the number of internet hosts, the team re-validated that information, biological, pulsed power, nanotechnology, and other technical sciences are all racing ahead at ever increasing speeds.

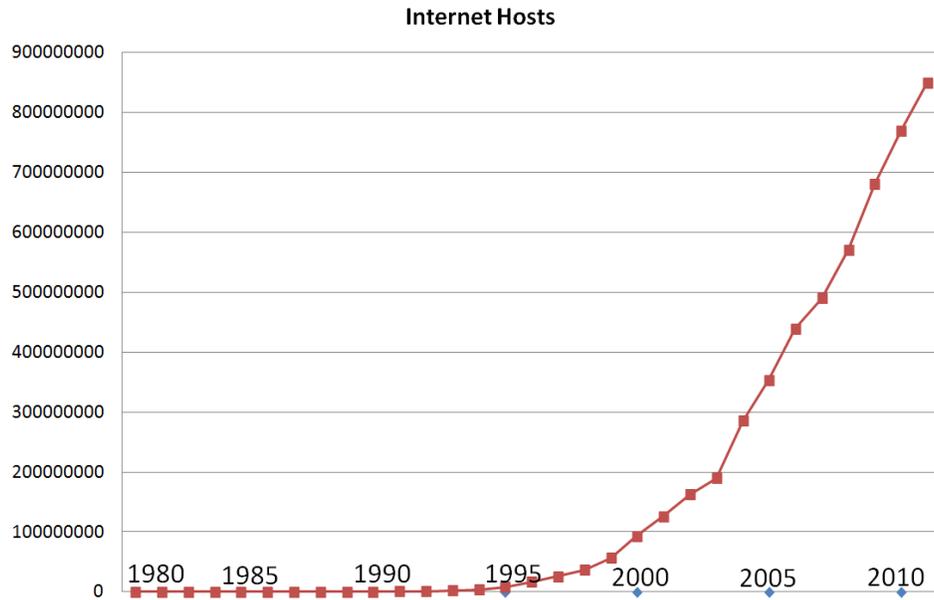


Figure 4: The J-Curve and Exponential Change¹³

The rapidly changing nature of technology suggests that the world, and the associated technological challenges it faces are changing in unprecedented ways.¹⁴ It is not only the scope of technology change that is unprecedented, but also its speed. This century will likely see 1000 times the technological change of the last, with each decade containing upwards of 70 times more technology development than occurred in the period from the dawn of time up until the year 2000.¹⁵ 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 may face likewise represent a significant departure from past thinking.

The Center’s recent research also shows that 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.¹⁶ Less than four percent of modern technological research is within the purview of the Department of Defense – a radical departure from 50 years ago, when that number was nearly 50 percent.

Feeding this development is the collaboration enabled by the internet. Specific Center research across a multiplicity of disciplines including computing, alternative energy, nanotechnology and cyberspace continues to tell this same story. Both scientific breakthroughs and technological applications are increasingly civilian developed, commercially distributed and globally distributed, and like the number of transistors on a single microprocessor chip (figure 2), these advancements are continuing at an exponential rate.¹⁷ Moreover, the “half-life” of scientific secrets and their technological applications into militarily critical technologies is shrinking rapidly and available to an ever larger panoply of actors, both state and non-state.

The result as we look to the far future is the technological dominance the United States has historically enjoyed may well be no longer possible. By some measures of innovation, such as the number of major scientific articles published in peer-reviewed journals, China is already passing the United States. Figure 5 is taken from a February 2008 study conducted by Georgia Tech on behalf of the National Science Foundation. What it shows is that while the U.S. continues to enjoy the best laboratory infrastructure in the world, we are declining in our productivity while others are rapidly improving in their ability to innovate. We are in danger of losing the technological race, and our education systems across the U.S. are setting the nation up to lose even more badly in the future.¹⁸

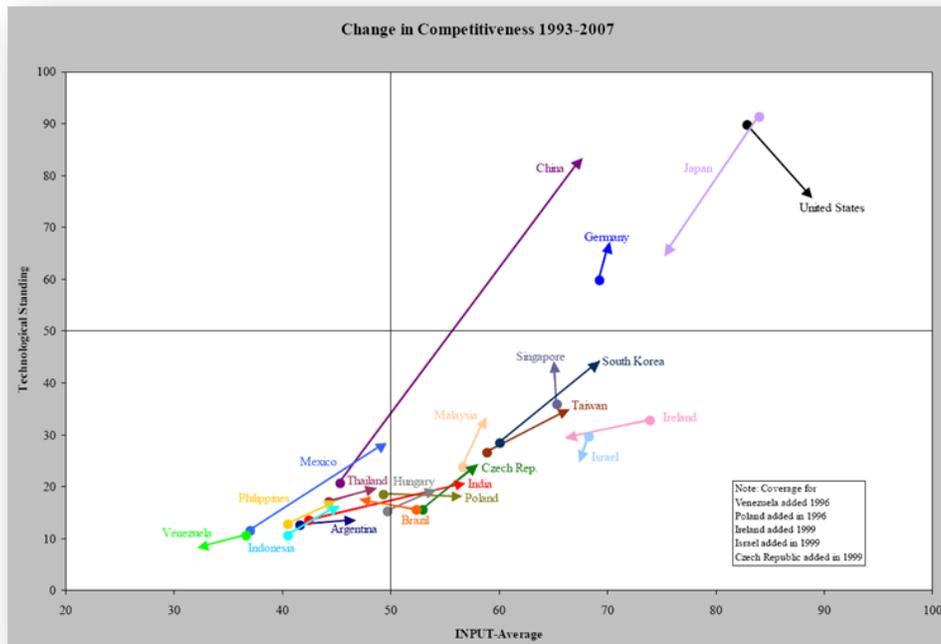


Figure 5: Change in Technology Competitiveness 1993-2007¹⁹

These forces are, in the words of Thomas Friedman, flattening our world. Technologies formerly in the hands of only the wealthy states are now being developed in what were once called “developing countries.”²⁰ This has, in turn, made advanced technologies once the purview only of nation-states to now reside in the hands of groups and individuals. Computer systems superior to the supercomputers in the 1980s now reside in the cell phones of people living in developing countries today.²¹ Based on a continuation of Moore’s law, computers in the next 30 years will become more than 1 billion times more powerful and less expensive than those of today.²² As a result of this flattening of our world and cheapening of technology, warfare is changing.

Historically, wars of high consequence have been relatively rare – sometimes only happening once or twice per century. These were the wars where catastrophic damage could occur, or the existence of a state or empire could be threatened. Conflicts with less serious results have been more frequent. In short, warfare has never strayed far from the orange line in figure 6. Today, however, the power once in the hands of states is

diffusing to the individual, meaning that attacks and battles of high probability may soon also be events of high consequence. Worse, these conflicts may become more common. This would allow warfare to move into the upper right quadrant of this strategic planning space – a place it has never been before. This means the future may be different from our past in significant ways.

Most probable becoming very dangerous

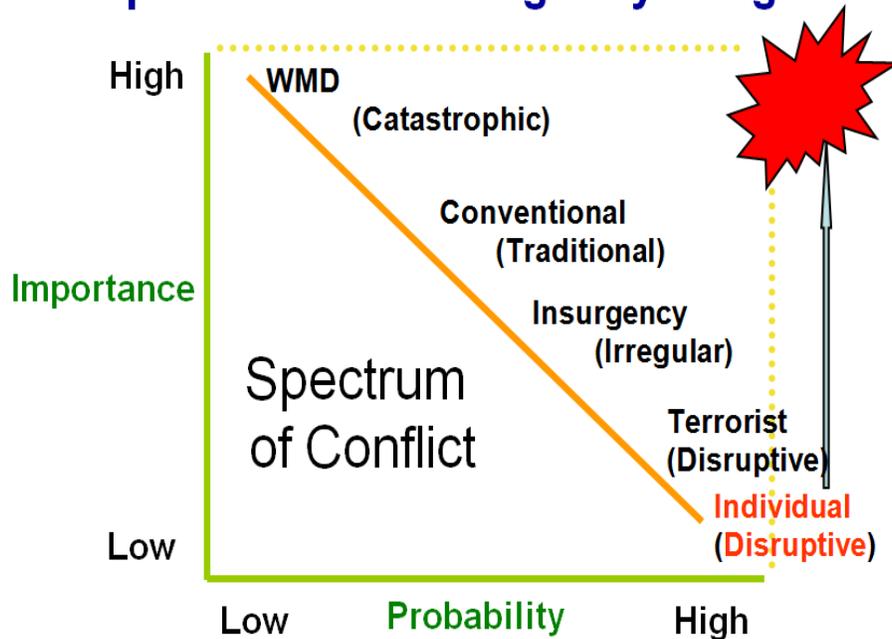


Figure 6: Warfare is Changing²³

Another factor that is changing is the number of actors that occupy this new space that may threaten the world. In 1980, UN membership stood at 154 nation-states. At the time, these were the primary actors in the world. Today, UN membership stands at 192, an increase of nearly 25 percent. However, the world has also seen a rise in groups, including non-governmental organizations, intergovernmental organizations, and terrorist organizations, many of which are able to affect outcomes on at least a regional basis. One such group, Al Qaeda, started the longest war in U.S. history. By 2008, these groups numbered at least 13,425 and may have been as many as 40,000.²⁴ This represents a three order of magnitude jump in the number of salient actors.

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 already in a world where computers can pass the Turing test, meaning that they can not only assist individuals in carrying out tasks, but also carry out these tasks by themselves.²⁵ As machines empower individuals, and potentially even become capable of creating significant impacts on society all by themselves, the number of potential actors undergoes yet another quantum increase. By this measure, the world of 2030 has not hundreds of actors, or even tens of thousands, but will 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 may be roaming the

planet by that time.²⁶ In short, the number of actors capable of making a major impact on the world stage will increase by another 5 or 6 order of magnitude in the next 30 years – nearly a 100,000-fold increase. Today, 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 the cause of their increased potential capability is illustrated in economic theory. 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. As recently as 45,000 years ago, a blink of an eye in Darwinian evolutionary time, mankind was mostly cave dwellers and solitary creatures. The discovery and rapid adoption of early tools enabled man to live off the land, and provided an incentive for larger communities to form. It also enabled specialization, as with the tools, the farmers could produce enough food for the community, allowing others to specialize in making improved tools or other crafts. By living together, knowledge sharing caused technology, even in this nascent stage, to begin to increase exponentially, and over time this has led to the increased specialization of employment and the growth of these early communities into the mega-cities in which many of us live. The critical point made is that the concentration of people increased 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, produce wealth, and result in continued cultural change. In short, the story of the advancement of humanity is the spread of specialization and exchange, with our prosperity being derived from becoming more narrow in what we make, and more diverse in what we purchase.²⁷

Ridley is an economist, and 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 contain and control new concepts and technology are threatened.²⁸ 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.”²⁹ 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.³⁰ Whether we call these details “turbulence” or a form of chaos in complex systems, we have entered a period of inevitable surprises, the outlines of some, we can discern in advance.³¹ The key is to understand some of these potential surprises, and know how to deal with the resultant challenges.

Cyberspace

Much of the United States critical infrastructure is dependent on cyberspace. To research exactly how vulnerable this infrastructure is, the Department of Energy has

created a National Critical Infrastructure Test Range as part of the Idaho National Laboratories. In 2007, a test of the robustness of our electrical grids against cyber-attacks was first conducted on the lab's 860 square-mile test range.³² Dubbed "Aurora," the attack simulated a single cyber-attacker tapping into a supervisory control and data acquisition (SCADA) system controlling an electrical power generator similar to those used in the power plants across the United States. The result of the attack, depicted in figure 7 below, was a loss of control of systems critical to generator operation, which caused the generator to be destroyed.³³



Figure 7: Generator During Aurora Test at Idaho National Laboratories³⁴

It is important to note that large electrical generation components like the generator in the Aurora test are typically custom manufactured parts. Utility companies often have spare wire on hand, but spare generators are rare. The usual time to receive a new generator from the time the order is placed is around 18 months, assuming, of course, that the plant that manufactures them has electricity in the first place. In a large cyber-attack, this assumption may be invalid.

This demonstration is disturbing on three grounds. First, it is not unique. Several instances of system malfunctions, arguably because of hacking into these types of systems, have already occurred and have caused damage to various infrastructures. Second, the U.S. Air Force is heavily reliant on the national critical infrastructure, and if it were to incur a massive failure, it is highly likely the Air Force would be unable to carry out its principle core functions. Lastly, very little has been or is being done to mitigate this problem.

There have been several attacks on critical infrastructure world-wide, many of which predated the Idaho test by years. Among those known to be intentional attacks on SCADA systems for the purpose of causing damage include an attack on the Maroochy Shire's sewage treatment system in Queensland, Australia, in January 2000. During this

attack, more than 264,000 gallons of sewage was spilled over a period of several weeks, just after a new control system had been installed. Pumps were opening and closing without being commanded to do so. Only after months of investigation and 46 successful attacks, was the source of the problem traced back to a disgruntled employee, who was trying to gain employment as the person to trouble shoot the misbehaving control systems.³⁵ In March 1997, a teenager managed to hack into the Bell Atlantic Computer and shut down the Air Traffic Control System in and around Worcester Massachusetts.³⁶ In addition, natural gas pipelines in the former Soviet Union (1982) and Russia in 2000 were disrupted by hacking attacks. The 1982 event resulted in an explosion by what Tsang referred to as a “logic bomb.”³⁷ There are other deliberate events that are also likely, as recent speculation regarding the Stuxnet and Flame malware suggests. It is important to realize that the SCADA systems offer a path into the internal logic of the critical infrastructure, and that attacking these systems is easy enough that even a single hacker can accomplish it.

The Air Force is dependent on these systems. If such outages are sporadic and/or localized, such inconveniences are easily overcome. If, however, the outage is part of a coordinated attack, and it affects the whole nation, then current planning is insufficient. If the national critical infrastructure is disabled, then not only is electrical generation affected, but in time so too are the systems that enable water transport, heating systems, sewage systems, as well as the financial and banking industries upon which modern economies depend. Distribution of foodstuffs, gasoline, and fresh water all require electricity at some stage, even if it is merely to distribute and pump the gasoline to power the trucks. Similarly, communications are electricity dependent. Without it, cell towers and land lines cannot operate. While most Air Force bases have means to recall their members even if there are no communications, the study team could find no one who could articulate how the Air Force would conduct a deployment without the ability to communicate from one base to another.

The Air Force is dependent on these systems not only for deployment, but cyberspace is likely to be the future domain in which most intelligence, surveillance and reconnaissance is to be conducted.³⁸ The rapid increase in the number of cameras and pictures that are both geographically and chronologically referenced combined with the current ability to fuse these images seamlessly together, will enable a new method of creating real-time three-dimensional images of almost any major city on earth.³⁹ As most of these pictures are available on the Internet, the ability to “play” these three-dimensional views back in time will enable the tracking back to its source of many activities of military significance. In addition, cyberspace and the pictures that exist therein, enable reconnaissance in ways impossible via either air or space. Office space layouts, interior building configurations, telephone junction and circuit breaker box locations are all pieces of data that can be found in a picture on the internet, but are pieces of data that one will never see from a satellite.⁴⁰ As a result, ISR in cyberspace may become the principle means of obtaining intelligence data in the future, making the survival of the national critical infrastructure even that much more important.

Perhaps most disturbing is the lack of a sense of urgency in addressing the problem. While research protocols require anonymity, the Center has interviewed senior executives in several utility companies across the Southeast United States regarding the protective measures they are taking to stop potential cyberspace attacks. To a person, we

received the same answer, “nothing.” When we queried these leaders (CEOs and/or COOs) as to why they were not taking action to protect their systems, the answer was likewise always the same. Protective action costs money, and such money would have to come from the dividends to the shareholders. In short, the market incentives that currently exist are a powerful disincentive for leaders of the private companies to do anything to protect against the vulnerabilities that have long been known to exist. As a result, significant threats, not only of disruption but of long-term destruction exist, and will likely remain for some time, in cyberspace.

Biotechnology

The second area where the threat is rapidly evolving is the area of biotechnology. The Human Genome Project was completed in 2003.⁴¹ In this project, completed several years early, all the genes in the human DNA were identified. Today, it is possible to get your finger pricked, and have your genomic code printed out with all the “A”s, “G”s, “C”s, and “T”s. Such a printout would reach about 20 feet in height, and it would likely be meaningless both to you and to your doctor, but today it is possible.⁴² The step being worked on now is the “Rosetta Stone” to those 20-25,000 genetic sequences – the part that determines how these genes produce the roughly 20,000 proteins that make each one of us the unique human beings we are. This is called the Human Proteome Project, and it is well and truly underway.⁴³

Once complete, 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 may all be eradicated. Already today, some cancers, particularly those of the blood like leukemia, are being attacked by nano-engineered medicines based on an understanding of the ribonucleic acid structure of the underlying disease. Medicines like Gleevec and Sprycell are able to bind with the leukemic blood molecules at a sub-molecular level and keep the leukemic molecules from reproducing.⁴⁴ The result for many patients is a long life with the leukemia in remission. More such cures and treatments will follow in the years ahead.

Unfortunately, this same technology which may bring almost miraculous cures 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. By the year 2025, such capabilities, we are told by the leading scientists in our national laboratory system, will be resident in the hands of a “well-trained microbiologist,” which they define as a masters degree holder from a major university.⁴⁵ Such an individual, with a lab costing as little as \$100,000, would be able to engineer such a 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, has already occurred with mice. In 2000, Australian scientists were attempting to modify the mouse pox virus to produce interleukin-four in the hopes of stimulating the production of viral antibodies. This experiment had two unexpected results.⁴⁶ First, it failed to result in the production of the antibodies sought. Secondly, the resultant mousepox strain had extraordinary lethality. Researchers awoke one

morning to find every mouse in the laboratory was dead, including the mice for which precautions were taken to immunize them against the disease before the experiment had begun. The virus was 100 percent lethal, had overcome the immunity conferred by prior vaccination, and had spread to every mouse in the lab.⁴⁷ While an accident, deliberate genetic modifications to existing viruses could produce the same result in other species, including our own.

Nanotechnology

The field of nanotechnology offers three key advances as we move toward the future. The first is at the nexus of biotechnology and nanotechnology, largely discussed above. The second is in the creation of high-density energetic materials much more powerful than those developed to date. The third deals with the development of nanomaterials that will have specifically engineered properties, such as the ability to cause rapid corrosion, which could become a new class of weapons against systems and materiel.

Nanotechnology is a term which is recent to science. Some reasonably recent versions of Webster's dictionary do not even contain a definition for the word.⁴⁸ Further, even within the discipline, there is some controversy over its meaning. 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 an outgrowth of science still catching up to the concept.⁴⁹ When this is added to 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 sub-molecular precision, for which the important properties of the materials are governed largely by intermolecular (i.e., van der Waals) forces.⁵⁰ Technology that merely involves scaling existing micro-mechanical processes to sub-micron scale is "nano-scale technology."

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 sub-molecular level to design medicines that can cure these diseases. As also mentioned above, 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.⁵¹

The second area of concern for future attacks deals with the production of high density materials using nanotechnology to precisely arrange molecular structures in a manner which optimizes explosive power. While modern explosives are several times more powerful than tri-nitro-toluene (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. Secondly, the explosive molecules that are not able to pair with the necessary oxygen immediately may still detonate, but after a short delay while they are waiting 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.⁵² This same process could be used to enhance the thrust produced by rocket fuels, which are, in essence, controlled explosions themselves.⁵³

While it is theoretically possible to achieve explosive yields of up to 1000 times those of modern explosives, near-term advancements are likely to be much more modest.⁵⁴ While nanotechnology is a very fast moving field, the ability to create the assemblers necessary to produce such explosives on a meaningful scale is currently limited, and in the next 10-20 years, most scientists in the field believe an advancement of five to ten-fold is likely. Nonetheless, a 10-fold advancement makes future explosives so powerful that the three-ounce bottle of liquid one is allowed to carry on-board a civilian jetliner may have to be reduced to 0.3 ounces – or only a few drops in the future. Very small and easily concealed explosives could pose significant risk to lives and property, and this miniaturization may result in a more challenging threat in the years ahead.⁵⁵

Militarily, there are two positive aspects to this technology. First, the precision needed to create these explosives would produce a very precise and reliable yield, allowing for potentially greater precision and lower collateral damage from newer weapons designs. Secondly, 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 either been fuel, or the systems with which to contain the fuel. The amount of thrust a unit of fuel can produce is called specific impulse, or ISP. Increasing the energy content of the fuel 5 to 10 fold would increase the ISP proportionately, and with it, greatly reduce the amount of mass of a rocket that would need to be devoted to fuel and its associated system.⁵⁶ While this dynamic has long been understood, the breakthroughs in nanotechnology may soon allow them to be exploited. While this may make it easier for man or robots to explore the stars or launch satellites, it would, of course, 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 nano-particles to interact with materiel to cause severe damage to infrastructure or materiel. In figure 8 below, several “white nanoparticles” are depicted. These particles 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 a very powerful agent 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.⁵⁷



Figure 8: White Nano-Particles⁵⁸

Nuclear Weapons

The study participants do not see nuclear weapons disappearing from the world stage during the time frame being examined. Nuclear weapons will remain a threat. Today, the “nuclear club” is estimated to stand at nine, and for the record, the study participants do include Israel in this number.⁵⁹ Iran’s nascent nuclear program has been well-reported in the press, and North Korea has already successfully accomplished nuclear tests.

Counterproliferation as a mission set would appear to have failed. While the Stuxnet virus may set Iran’s program back by a few years, it does not guarantee an ending to their program. While the engineering to refine the materials is dangerous and difficult, and the safety systems needed to protect workers are complex, the science behind these devices has been published in high school physics textbooks for the past 30 years.⁶⁰

By the 2030s, it would seem likely that the gradual upward trend of states with nuclear weapons will continue. Already, Iran’s potential quest for a nuclear weapon has triggered interest in the Arabian Gulf region, and this dynamic may well spread elsewhere. As will be discussed further below, it seems likely nation-states can be deterred from using these weapons. However, the more widely proliferated they become, the more opportunities groups and individuals may have to appropriate one. This is perceived by this study team as the greater risk of proliferation for reasons that will be discussed more fully below.

Directed Energy

This study addresses two different forms of directed energy, both of which represent threats to military and civilian personnel. The first is the pulsed type, which includes such phenomena as pulsed high-powered microwaves, electro-magnetic 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. Usually referred to as lasers, the power output of these weapons has reached tactically significant levels in the last few years, and further developments are likely in the near future.

Pulsed Weapons or Phenomena (HPM, EMP, or Major Solar Flares)

The discovery of the potential anti-electronic utility of pulsed forms of energy came by accident. In 1962, shortly after the Soviet Union had 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.⁶¹ Approximately 1300 kilometers away, in the islands of Hawaii, 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 be made.⁶² It is important to note that not every street light was disabled, many cars still ran, and some telephones still worked. Nonetheless, many systems stopped working that night. Only later did the reasons become clear.

A few years later, in 1967, both the United States and the Soviet Union had replicated these pulsed energy effects. We collectively 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.⁶³ Fearing the effects such weapons could create, the U.S. and U.S.S.R. together drafted the "Outer Space Treaty." More formally, it is entitled *The Treaty on Principles Governing the Activities of States in Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, which only bans weapons of mass destruction from space, and does so because of the electromagnetic pulse phenomenon known as EMP.⁶⁴

A very similar phenomenon can be reproduced using a non-nuclear 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.⁶⁵ By inducing an electromagnetic field across wires, computer circuits, or any other conductive material, electric current is produced within the wires. Like EMP, this current can play havoc with computers, power distribution and electronic control systems – the very systems involved in controlling our national critical infrastructure, financial and banking systems, and computers 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.⁶⁶ 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.⁶⁷ Just as important, our ability to store and generate pulsed power in the form of microwaves is also increasing exponentially with time. In 2003, it was possible to produce 20 gigawatts of pulsed power output in a 400-pound device.⁶⁸ 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.⁶⁹ In 2002, conventional pulsed microwave devices had relatively short ranges. Today, small portable reusable weapons have ranges in the 100s of meters.⁷⁰ 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.⁷¹

As the team was studying the disturbing effects of pulsed power on computer and electrical systems, we stumbled upon a disturbing finding that changes the way the U.S. must look at deterrence specifically in this area. There is a natural phenomenon that creates these same electromagnetic fields, at very high levels, that can damage or destroy the nation's computer and electrical infrastructure. Unlike individuals, groups, or nation-states, this phenomenon is not deterrable. In short, the day will come when the U.S., and indeed the world, will have to deal with this problem on a massive scale, and the astronomical record suggests it happens on average once every 50 years or so.⁷²

Solar coronal mass ejections, or solar flares, send charged particles into the earth's ionosphere, which in turn can create strong magnetic fields on Earth. One such flare, much smaller than the one-every-50-year event referred to above, occurred on March 13, 1989. Perturbations in earth's magnetic field caused by the charged solar particles induced electrical currents in power lines and all conductive metals. These currents flowed into the generators and transformers of power plants across the globe, affecting some severely. The power failed across much of Eastern Canada, and due to continued current fluctuations in the power lines, restoration could not begin for nine hours. The Toronto Stock Exchange had to be closed.⁷³ While most pieces of the power grid survived the flare, some did not. The transformer in figure 9, below, was among those partially melted and shattered in the event.⁷⁴

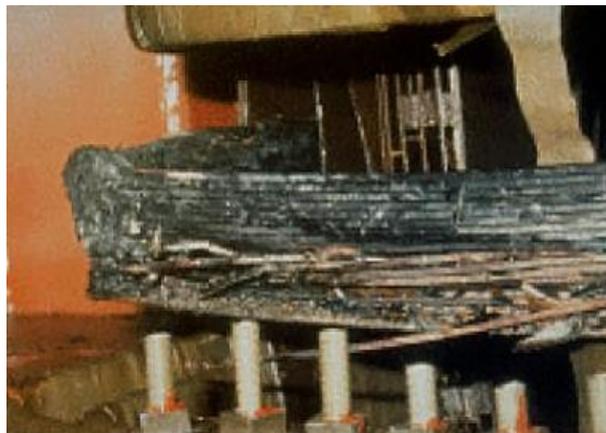


Figure 9: Transformer Damage from Solar Flare

It is important that the flare of March 13 was just barely an X-class flare. Much larger solar flares are in the astronomical record, but they pre-date the construction of the modern electrical grid. The result is that our electrical and computer systems have never faced an extremely large flare, and as a result, no one has personal experience with what such an event would be like. We do have computer models based on smaller flares that give us an indication of what could happen, and what they tell us is disturbing.

Figure 10 shows the impact of a once-every-50-year solar flare, notionally at a level of 4800 nano-Tesla per minute centered at about the latitude of the U.S.-Canadian border. This is a flare similar to the one which did hit the earth in May 1921. The areas outline in black would see blackouts with concomitant destruction of the electrical producing infrastructure. The sizes of the circles (both red and green) indicate the level of current that would be induced along the power lines and other metallic objects. The color merely indicates whether the charge would be positive or negative, but it is important to note that both can cause catastrophic damage. The transformers that would be destroyed, like the one in figure 7 above, would take years to replace as these are custom manufactured pieces of equipment. The economic impact would be well into the trillions of dollars, and result in an economic downturn of depression magnitude.⁷⁵

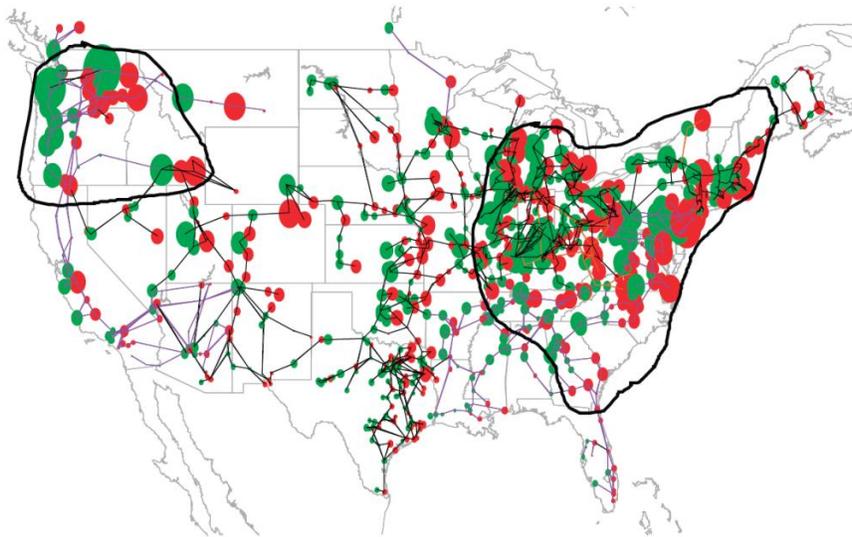


Figure 10: Impact of a May 1921-Class Solar Flare on U.S. Electric Grid⁷⁶

The May 1921 solar flare is not, however, the worst case scenario. On September 1, 1859, a British scientist had sketched a set of sunspots. As he was drawing them, a solar flare so large that it could be seen with the unaided eye blotted out the spots. Within a minute, the flare was over. The next morning, the Aurora Borealis and Aurora Australis were seen well into the tropics. The Auroras were so bright that newspapers could be read outside at night as if it were daytime. Telegraph wires went haywire and operated even after the batteries had been disconnected. Electric arcing from these systems electrocuted operators and set telegraph papers on fire.⁷⁷ There were reports of electrical arcing or lightning bolts dancing from cattle fences in the Great Plains to the ground as the wires between posts had become energized. The models that suggest nearly half the nation would lose electricity in a 1921-like event above, indicate that

should another flare of the size of the 1859 event occur, virtually the entire electrical grid would be catastrophically damaged with recovery time estimated at over ten years.⁷⁸

As we found with cyber-security issues, very little is being done to address this problem. Protection of our computer and electrical infrastructure against pulsed wave forms, whether man-made or natural, is not occurring. In addition, policy guidance is also lacking. The result is that while the dangers of our current systems are known, the vulnerabilities remain.⁷⁹

Lasers

The other form of directed energy is continuous wave, the most common being lasers. While lasers have over-promised and under-delivered for decades, this is no longer true. In November 2010, the Air Force Center for Strategy and Technology placed an order for a small hand-held, category IV weapons-grade laser. The cost was \$299. To the Center's surprise, the order processed on "Black Friday," the Friday after the U.S. holiday of Thanksgiving, resulting in the Center receiving the "three-for-one" special deal. We paid less than \$100 for each of the three lasers that arrived on our doorstep about six weeks later. Figure 11 depicts the blue variant of this laser. It measures approximately 20 centimeters long, is approximately 5 centimeters in diameter and weighs 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 out to approximately 150 meters. It is capable of melting plastic and setting flammable materials ablaze.⁸⁰ The laser runs off of a single lithium-ion battery, roughly size AA, which enables the laser to continuously operate for 120 minutes on a single charge.



Figure 11: Spyder Arctic III Blue Laser

The laser began to be marketed in the fall of 2010, and was produced by a company operating in Hong Kong. At the time of production, only the country of Malta had definitive restrictions on the sale or importation of this device.⁸¹ In the U.S. importation was legal. Though not directly attributable to this laser, in the first nine months of that year, the U.S. 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, to include some attacks on motorists.⁸²

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, recently decommissioned by the U.S. Department of Defense was a megawatt-class system, roughly one 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, to include stopping a Ford F-150 truck.⁸³

As with pulsed power devices, laser efficiency and effectiveness is continuing to improve. Small hand-held devices powerful enough to blind or kill will soon 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.⁸⁴

Space

The last of the six threat areas the team explored were threats to assets in space. As has been demonstrated by both China and the U.S., satellites in low earth orbit are vulnerable to direct ascent attacks.⁸⁵ Directed energy research is continuing in several countries and will pose a risk to satellite operations in the very near future.⁸⁶ Lasers that can dazzle or destroy satellites, likely all the way to geostationary orbit, will likely 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.

What many may not realize is the important roles that satellites play in the economy or in our everyday lives. Most people intuitively understand that the global positioning system (GPS) provides their location and, in combination with a receiver, can help them locate hospitals or gas stations. What is not widely understood is that the way GPS operates is by triangulating one's position through the use of very precise timing of the receipt of signals from the satellite constellation. So precise is this timing, that GPS time data is now an integral part of traffic control systems to include stoplight timing. They are also crucial for the operation of automated teller machines that enable banking customers to obtain cash when they are not at a branch of their primary banking institution, and are integrated into the machines that process credit and debit card purchases. It controls the sequencing of mobile phone calls through the cellular tower network in many countries. Airlines rely on it for direct-route navigation. It also controls the switching of power networks, and the transfer of electrical power between grids to avoid power surges on power lines as generators are brought on-line or taken off-line as the power load increases and decreases.⁸⁷ This reliance on these signals is rapidly increasing.⁸⁸

The loss of this satellite constellation alone would suddenly stop credit card transactions, produce gridlock in many of the world's cities as traffic lights ceased to operate, take the mobile phone network off-line, and keep bank customers from being able to withdraw cash from their savings or checking accounts unless they dealt directly with a bank teller at their banking institution. The second and third-order effects to peoples' lives and the nation's economy would be considerable.

Other satellites provide us with data essential for weather warnings, provide for long-distance telecommunications, provide us with television signals, and enable rapid transfers of data from distance locations. These systems are all potentially vulnerable as well.

From a military standpoint, military aviation and ground system locations are dependent, at least in part, on GPS positioning. Military operations are affected by the

weather, and satellite pictures and the atmospheric data embedded therein are crucial to modern weather forecasting.⁸⁹

The study team’s research and interviews with a variety of space-reliant companies and government agencies revealed that much like the national critical infrastructure on the ground, our space assets are poorly protected.⁹⁰ As with the ground-based systems, the cost of hardening or making these systems resilient to attack is greater than the cost of insuring them against loss, and as such, a positive financial market disincentive exists to address any current or projected space vulnerabilities.

A Structural Model of Deterrence

In order to evaluate the six technological threats discussed above, the study team had to understand deterrence concepts and deterrence theory. An intensive effort was undertaken to review the literature on both conventional as well as nuclear deterrence theory, and to determine what key elements transcended the writings of the various authors that helped the world develop an understanding of this dynamic.

Based on over 20 works, deliberately selected to span Western and Eastern cultures, the model depicts already acknowledged aspects of deterrence theory and their relationships to each other.⁹¹ As such, it became a framework for thinking and analysis. While the study team considered undertaking an attempt to engage in Bayesian probability modeling as a study methodology, the necessary data was not readily available, and such an analysis could not be conducted within the study deadlines. This model could, however, be used to undertake such efforts, as part of a future research program.

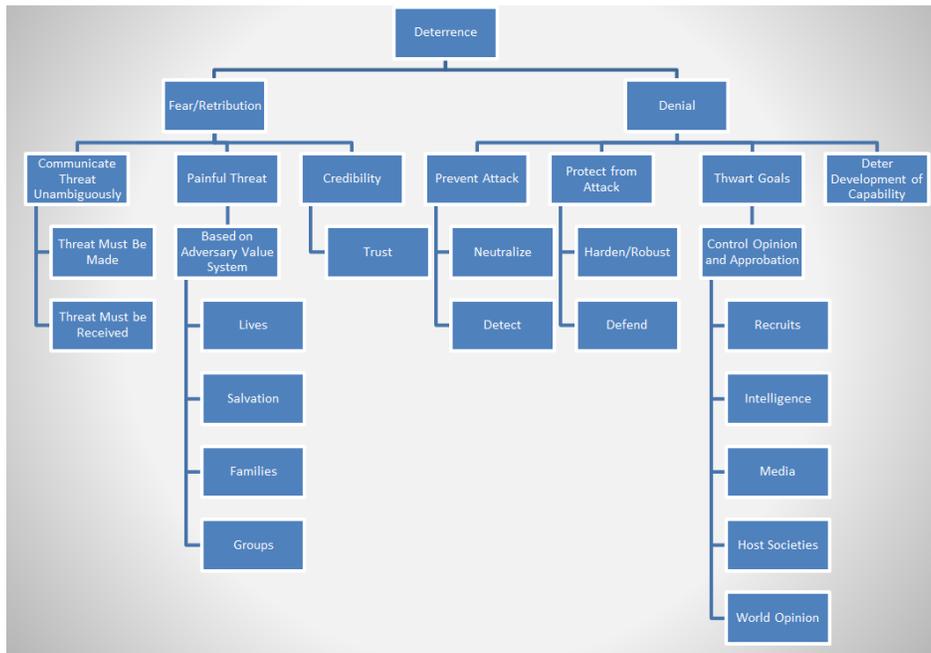


Figure 12: A Structural Model of Deterrence Theory

As the team examined the literature, it became clear that the focus during the Cold War was mainly on the left half of the model – the side labeled “Fear/Retribution.” This thinking made sense, as during this timeframe, the treaties in effect limited each side (the U.S. and the U.S.S.R) to 100 ballistic missile interceptors.⁹² As 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 and 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 only to that which was necessary to ensure that 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.

This study concludes that with regard to many of the future threats, the relative importance of the two sides of deterrence theory changes. It is important to recognize that the theory itself is structurally sound. What is different is that with regard to 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 constitutes a change in the way in which the Department of Defense and the Department of the Air Force need to operate in the future.

In operationalizing the model against the future threat array, many of which are conventional, we turned to an equation verbally described in Mearsheimer’s 1983 book Conventional Deterrence. Mearsheimer argues that the failure of deterrence is specified as a calculus in the mind of the actor to be deterred. Mearsheimer referred to this calculus as “the attacker’s fear to the consequences of...action.”⁹³ While Mearsheimer describes this calculus in great detail, this study turned it into a mathematical expression. An actor is deterred if the following condition holds:

$$\text{Adversary's Assessment of Success (Probability x Value)} - \text{Adversary's Assessment of Failure (Probability x Value)} < 0$$

Figure 13: The Deterrence Equation

Mearsheimer argues that several factors play in this calculus of whether deterrence will succeed. The first term 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 multiplicand of these two elements comprises the potential adversary’s assessment of success (green box in figure 13). Only if a potential adversary’s assessment of failure is greater than this assessment 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 (red

box) is the greater of the two terms, then the value of the equation is less than zero, and the actor is deterred.⁹⁴

There are some assumptions 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 that 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 that underpins it. Secondly, it assumes that one can attribute the attack to the actor who is or will carry it out. While in the nuclear era this was relatively easy, as nation-states launching ballistic missiles in a global thermonuclear war do leave behind a "calling card" of sorts, this has recently proven much more difficult in newly-created artificial domains such as cyberspace.

In fact, it is 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 that the probability of carrying it out successfully likely rises, or at a minimum remains the same. The probability of incurring punishment clearly diminishes as 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 done incorrectly. A failure to properly attribute often leads to simple-minded decisions along the lines of what actors expect.⁹⁵ 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.⁹⁶ These dynamics were tested in exercises conducted by the Center in conjunction with this research, where participants in a wargame were placed in a position of relative uncertainty with regard to adverse conditions experienced by the U.S. and its allies. Even though sufficient data were available to the participants to uncover the actual actors, the dynamics predicted by attribution theory above were present. The vast majority of the participants misattributed the hostile actions to the wrong actor.

In a real world situation, such misattribution can have disastrous consequences. Imagine if, when Japan had sequestered the Chinese fishing vessel for transgressing its territorial waters in the Senkaku Islands on September 8, 2010, a third party state had launched a cyber-attack against the United States via servers within mainland China. Had such an event occurred, and had the U.S. then misattributed the source of the attack to the Chinese, which attribution theory predicts we would have done, the consequences that would have ensued would have been of a type that neither Japan, China, nor the U.S. would have wanted. Getting attribution correct is essential, not only for deterrence, but also to avoid unintended conflict.

Complicating the problem of attribution is 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 oneself to these events, decide on a course of action, and then act on that decision (a cyclical process called the OODA loop) is shrinking.⁹⁷ With several new technologies operating either at or near the speed of light, this decision loop is rapidly shrinking toward a point, requiring much more rapid capabilities to observe and attribute incoming attacks.

We can see this dynamic at work in recent events. On May 6, 2010 at approximately 2:32 pm Eastern Daylight Savings Time, a large mutual fund complex

executed a single sell order for 75,000 E-Mini S&P 500 contracts, a trade valued at approximately \$4.1 billion.⁹⁸ The sell order was programmed to execute sales at a level equal to 9 percent of the rate at which the securities had been sold up to that point in the day, but without regard to price. This was, in essence, an order to sell these contracts at market price. While this was a large order, it was only the third largest such sell order for this security in the preceding 12 months. Nonetheless, after about nine minutes, the existing demand for these contracts had been exhausted, and the price was falling quickly, with the DOW Jones Industrial Average already down nearly 600 points. This caused short-term traders to have to sell shares in the equities markets to cover their losses on the S&P contracts. The result was a sudden fall in the market price of the S&P 500 and other equities within the markets. By 2:46 PM, the Dow Jones average had fallen 1000 points in ten minutes. The investigation into the event showed that the original sell order triggered a trading “tipping point” that had been built into algorithms within the market’s mechanisms. When all automatic trading mechanisms were halted just before 2:46 PM, market prices began to recover.

The investigation as to how this event, called the “Flash Crash” or “The Crash of 2:45 PM” occurred revealed that computer trading had moved so quickly, that the machines were selling and buying shares of stocks and contracts faster than investors could keep up. This is a classic example of a complex dynamic system, sometimes called a chaotic system, in which tipping points that, if crossed, rapidly take the system to a new state.⁹⁹

The nation-states that comprise our global security system are similarly chaotic and capable of rapidly tipping from one state to the next. This is not merely a phenomenon of machines. For example, on June 28, 1914, the assassination of Archduke Franz Ferdinand of Austria triggered a conflict grossly out of proportion to the initial act. More than 9 million combatants would die in the conflict that ensued which eventually involved large sections of the planet. In short, human society also can have tipping points where single acts, or small sets of acts, can cause reactions much larger than would normally be expected.

In the end, the human system in which we must deter is complex and chaotic. It has tipping points. What is changing with automation is the speed with which these events can occur. In the “Crash of 2:45 PM,” roughly ten minutes elapsed between the time a decision to sell contracts was executed and the point at which the stock market had lost trillions of dollars in value. In the case of World War I, a full month elapsed between the assassination of Archduke Ferdinand and the Austro-Hungarian Empire’s invasion of the Kingdom of Serbia. In the modern age, time is disappearing. The decision cycle coined by John Boyd as the OODA Loop is shrinking and rapidly collapsing into an OODA point. As attacks and actions today can be initiated at the speed of light by ever-faster computers and weapon systems, 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 deterrence lay, the study directors conducted a formal and informal Delphi study.¹⁰⁰ The study drew upon participants (called “Oracles” in the Delphi method) who had studied the above six

technologies and had a working knowledge of deterrence theory and military strategy. These respondents were asked to respond in a manner where their anonymity was preserved, but such that their comments, rationale, and ratings were visible to all. After three rounds of the study, we had achieved consistency in the ratings for each of the three questions we sought to explore. Each question explored all of the six technologies discussed above, while also parsing the responses to separate out dynamics that are different between nation-states, groups and individuals.

The first question asked the respondents to rate on a Likert scale of one to five (very easy, easy, neutral, difficult, and very difficult), the level of difficulty of deterring nation-states, groups, and individuals from launching an attack using each of the technologies below. The results in figure 14 show that it is more difficult to deter individuals, regardless of technology explored, than it is to deter nation-states. In addition, we found that the team believed that cyberspace, bio-, and nano-technologies 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.

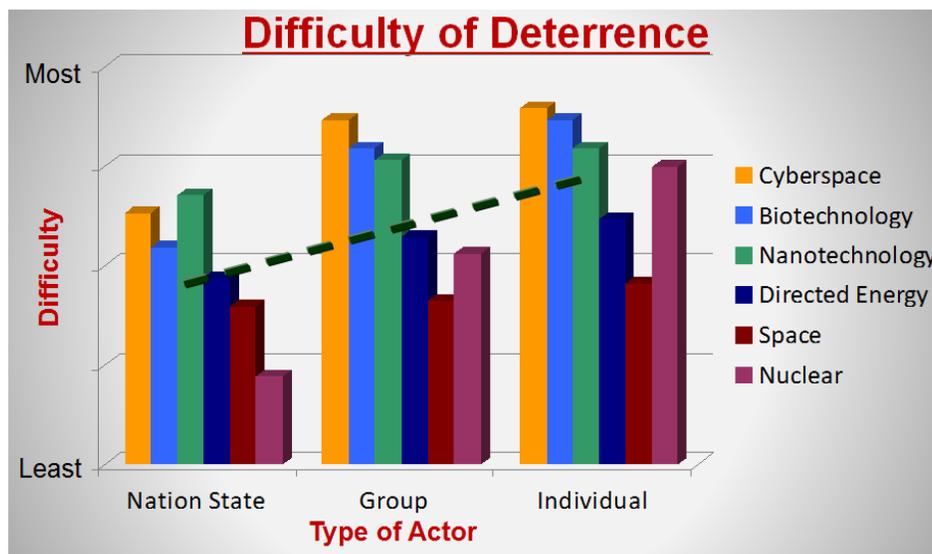


Figure 14: Difficulty of Deterrence Delphi Results

In the anonymous discussions during the formal Delphi sessions, and in the broader discussions which took place during the informal Delphi study, the respondents were asked why this relationship was perceived as it was. In general, the study participants believed that nation-states and groups placed value in their respective reputations. Moral constraints to use force and the results of international approbation act most strongly on nation-states.¹⁰¹ Yet, the ‘Oracles’ believed that for groups, especially the larger ones, the reputational issues were sufficiently strong as to make them easier to deter than small groups and individuals. Individuals, they argued, would be least affected by international norms, and thus the hardest to deter.

The second question we asked the respondents was regarding the difficulty of attribution. As with the question above, this question was parsed both by type of actor as well as the technologies involved.

As is shown in figure 15, the graph takes on the same shape as above, but for different reasons. Here, the individuals were considered the most difficult to attribute,

across all six technologies, as they were the most likely to be able to conduct an attack and avoid leaving a distinguishing trail that would lead to properly attributing the source of the attack. Nation-states, on the other hand, because of their size and the bureaucracies that must approve these actions, often leave traceable indications that they were behind 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 as to make it possible to trace the program.

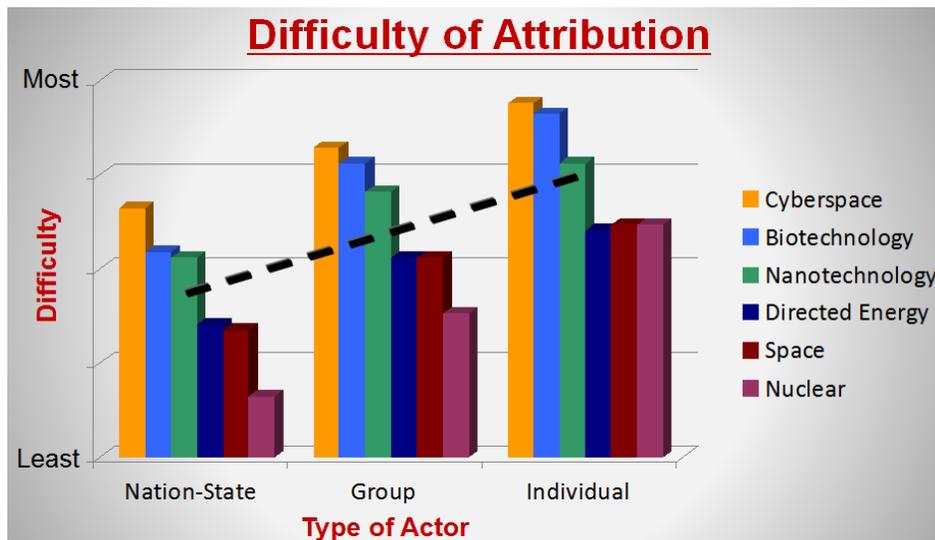


Figure 15: Difficulty of Attribution Delphi Results

Three types of technologies were perceived to be much harder to attribute than the rest. Attacks in cyberspace were considered difficult to attribute as the attacks could, with proper planning, be made difficult to trace and be routed through third party servers. Biological attacks were considered problematic as 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 back to their origins, as the passenger traffic would leave a very large number of potential paths to trace.¹⁰² Nanotechnology threats were also considered difficult as they are small enough in size that they could remain dormant for extended periods, leaving great doubt as to when they were positioned.

The last area in which we collected data via the formal Delphi method was in the area of likelihood of attack. Here, definitions proved important, as we were interested in the likelihood of only very large destructive or catastrophic events. For this segment of the study, a “catastrophic” attack was considered one that “threatens national survival or eliminates the U.S. Air Force’s ability to accomplish its mission.” A “destructive” attack was one that “seriously impacts the U.S.’s ability to function or significantly degrades the U.S. Air Force’s ability to perform its mission.” We asked the respondents to use a betting scheme where each had \$400, and with even odds, we asked them to place bets on where the next destructive or catastrophic attack would occur. Attacks below the destructive threshold were to be ignored for this exercise.

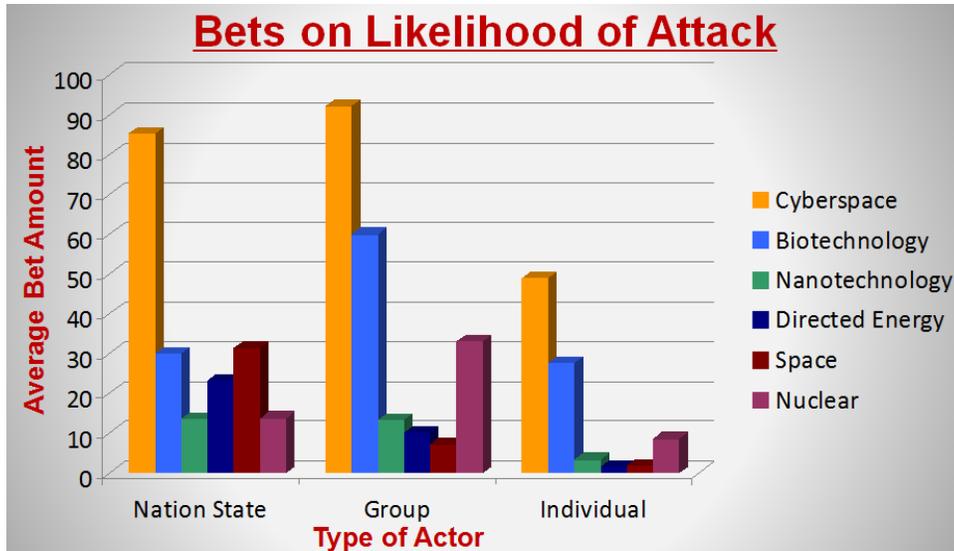


Figure 16: Likelihood of Catastrophic Attack Delphi Results

The results of this exercise are in figure 16 above, which contains three patterns within the data that are worthy of explanation. First, the greatest perceived threats to the functioning of the U.S. or its Air Force were either via biotechnology or in cyberspace. It was in these two areas that the Oracles believed there was significant catastrophic risk to the nation and its Air Force. The respondents believed this danger was significant due to the relatively unprotected nature of the infrastructure to cyberspace attack, and a very incomplete infrastructure to detect novel pathogens or viruses. Second, for three of the six technologies, the graph has a central “hump” with a greater probability of catastrophic or destructive attacks coming from groups than from individuals or nation-states. In all three cases; cyberspace, biotechnology and nuclear weapons; the Oracles believed the nation-states would be somewhat self-deterred due to the reputational issues discussed above. However, they also believed that very few individuals, if any, would be able to garner the resources single-handedly to create an attack of destructive or catastrophic scale. This created a curve for these three technologies 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 better. Lastly, for the remaining three technologies; nanotechnology, directed energy, and space; nation-states were considered the most likely to attack catastrophically, as it was deemed unlikely that even groups would have the resources to attack using these weapons on a massive scale.

The study team then plotted all three of these Delphi results in three-dimensional space to get a better picture of the threat space. Depicted in figure 17, below, this plot shows that cyberspace and biological threats are the most critical, with some nuclear and space issues worthy of highlighting.

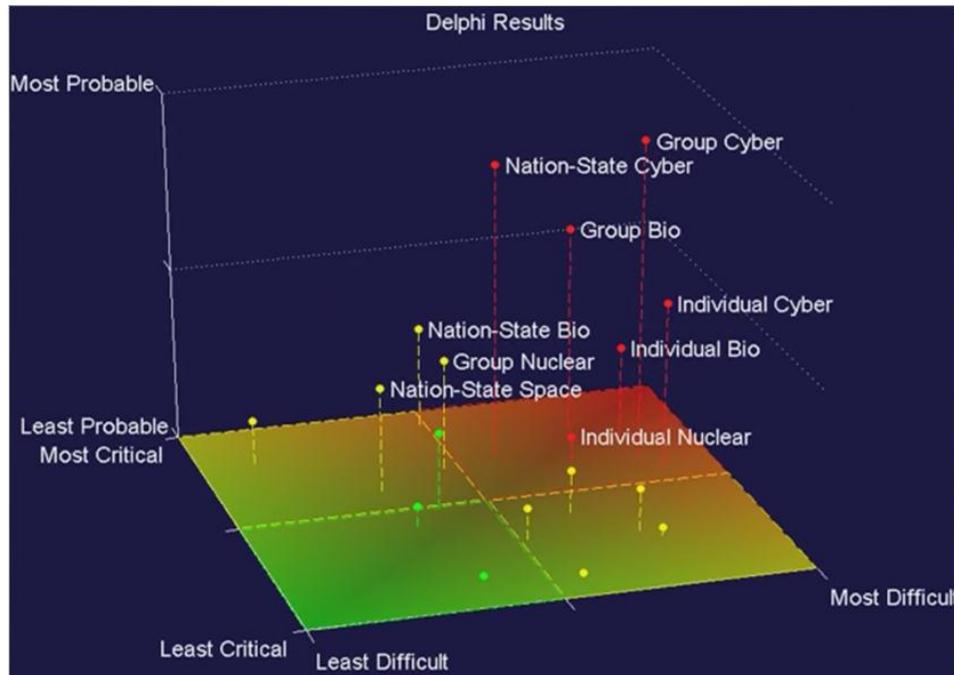


Figure 17: Delphi Study Threat Data in 3-D

Findings & Implications for the U.S. Air Force

The purpose of this study was to discern the role of the U.S. Air Force in deterring future technologies. The report now examines the issues the study team uncovered that are directly relevant to the Air Force.

The study concluded that the answer to the fundamental thesis question of how the Air Force should position itself to deter future threats, begins with its history. The Air Force and its forerunner, the Army Air Corps, pioneered flight. Initially, these flights were in lighter-than-air balloons, and then early aircraft, used to see over the trenches in warfare and to direct cannon and/or created the intelligence to allow for artillery attacks against the enemy.¹⁰³ In more recent years, the Air Force has led in the area of cyberspace. Since its inception, reconnaissance has always been part of the Air Force’s core mission set.¹⁰⁴ In fact, of the targeting chain frequently referred to as F2T2EA (find, fix, track, target, engage, and assess), surveillance and reconnaissance is an integral part of five of its six steps. In short, diminishing the “fog of war”¹⁰⁵ was at the heart of the Army Air Corps creation, was at the heart of the Air Force becoming a separate service, and this remains a crucial role for the Air Force today.

Transparency

The first main finding of this study is that increased “transparency” is necessary in order to facilitate proper attribution and early warning of attack. Transparency has three elements. The first are technical developments that aid in tracking people and

objects through space and time. The second is ongoing innovation in this area, and the last is 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 web sites are updated, or personal data removed, the old data is still available and can still be retrieved.¹⁰⁶ The “Wayback Machine” enables a user to search through over 150 billion web pages archived from the early days of the World Wide Web in 1996 until only a few months before the search is conducted. Should one wish to retrieve information from the past 90 days or so, Google’s “cached” page function takes over.¹⁰⁷ The result is anything that 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 not only raw data, but pictorial information; they archive public (government) as well as private (personal) web postings. Data posted on YouTube, Facebook, MySpace, or other social media sites is readily searchable if such data is made public. As mentioned above, the pictorial data can, itself, be fused together to create 3-dimensional images that can be viewed across the fourth dimension, time.¹⁰⁸ With well over 100 billion pictures already on the internet, and YouTube is surpassing 1 trillion video downloads, with several billion more pictures and videos being posted each month, the internet is morphing into a window to our world that allows us to see anywhere at almost any time.¹⁰⁹ In short, the technological developments are moving us toward transparency.

As this enormous dataset becomes available on the internet, new innovations will be necessary to use it. As mentioned above, nascent versions of some of the necessary algorithms already exist. Photosynth, a readily available Microsoft program, can fuse pictorial data together, as most cell phones now tag the photos with a geographical and chronological stamp. Other algorithms are able to examine patterns of human behavior, and flag for analysis, those activities that are not like the others. Such algorithms can be useful to enable business to foresee the next major consumer product, or for purposes of enhancing security. One such set of algorithms has been developed as part of the Risk Assessment and Horizons Scanning system in Singapore. While analyst intensive, Singapore has developed a process that involves environmental scanning for data, provides indicators of possible activity, enables the conduct of sentiment analysis, and helps them do data fusion and analysis that leads to scenario development and the development of strategies. This system, first put in place in 2004, has undergone several upgrades since its inception. While not fully automated, the system provides “insights to emerging risks and opportunities with national security implications.”¹¹⁰

With a world of data available, and the algorithms to flag events which may be indicators of risks, proper command and control can ensure that risks are properly assessed. Here, the Air Force’s global command and control capability becomes the last element of a new transparency system. As data suggests a risk may be emerging in a part of the world, the command and information exchange systems, in conjunction with well-trained leadership, enables the analysis, further research, and assessment of the risks as they emerge.

The vision for how this transparency system would potentially operate is depicted in figure 18 below. The concept begins with the fusing of several streams of data. Intelligence data gathered through satellites, reconnaissance platforms and other routine methods constitutes the intelligence stream. The public data is data published by news

media, publishing houses, or governmental agencies that seek to make information available to the world. The “private” data may be a slight misnomer, as this includes data on the internet that is publically accessible, to include public personal profiles that can be found in such places as Facebook or MySpace. Most users of these sites allow certain aspects of their profiles to be viewed by people not yet on their list of “friends”.

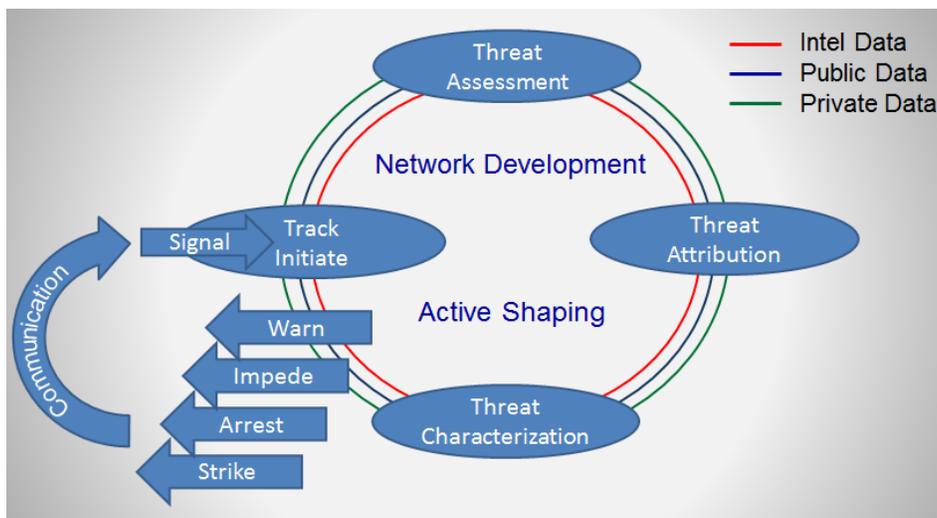


Figure 18: How Transparency Operates

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. On such a signal, tracking by the analyst is initiated. The analyst drills into the data to determine if there is a concern that rises to the level of being a threat to U.S. facilities or interests. If such a threat exists, then additional analytical work is done with the data to attribute this threat to a specific actor or set of actors, and then characterize that threat to include identifying its capabilities, operating procedures, and its location. At this 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 individual 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. Through additional fusing of data, and repeating the above process, other potentially dangerous actors associated with the initially discovered adversary, will also be flagged for further analysis. By repeating this process iteratively, it will soon become obvious to actors who seek to hurt the U.S. that their likelihood of success has decreased, and with it, the deterrence calculus shifts in our favor.

It is important to realize that this process leverages things the Air Force has historically done well. It is a leader in technology, and has an entire laboratory directorate devoted to the creation of new sensor technologies.¹¹¹ It is the Air Force that was and is the service responsible for reconnaissance and information gathering, and it is the Air Force that has developed computerized operations centers where the fusion of

these data can take place. In short, the creation of transparency is an extension of extant Air Force missions, and the Air Force can and should lead in these areas.

From this proposed operational concept, this study concludes that transparency should be thought of as a second pillar of deterrence. From an Air Force standpoint, it has benefits very similar to air superiority, in that it facilitates both attack and defense. More importantly to this analysis, transparency has a deterrent quality all its own. It is important to understand that transparency is about knowledge rather than about control.

Stood alongside the ability to strike globally, transparency has the potential to radically alter an adversary's deterrence calculus. If (s)he believes that their actions will likely be discovered and attributed, and that the punishment from the United States for an attempt to conduct catastrophic or destructive attacks on U.S. interests will be severe, then the deterrence calculus shifts in favor of the attack being deterred. As a result of the development and proliferation of technologies that can create catastrophic effects over the next 10-20 years, this study concludes that by 2030 transparency and the associated concept of attribution will be essential and as a requirement will drive defense procurement spending.

To fully realize the potential of how transparency can assist in deterring future adversaries, a coherent vision, scientific research and development, further development of concepts of operations, and potential organizational changes will all be necessary within the Air Force. The study participants believe that as the service that established the terms of reference for the use of cyberspace, the Air Force is better prepared to lead these efforts than our sister services. As time is short, it is important that we do so.

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 that the adversary will have some level of transparency versus the United States. Figure 19 was a picture pulled by the study team from the internet while the aircraft depicted were still in these parking spaces at Al Udeid Air Base in Qatar. At one end of the ramp are B-1 aircraft are fully loaded. Had these weapons been detonated by an attack on the base, the other aircraft on the flight line, which included roughly one-fourth of the Air Force's entire AWACs and Airborne Command fleets would have been destroyed. Notice that all the data needed to carry out an attack, to include the target elevation and coordinates, were readily available.

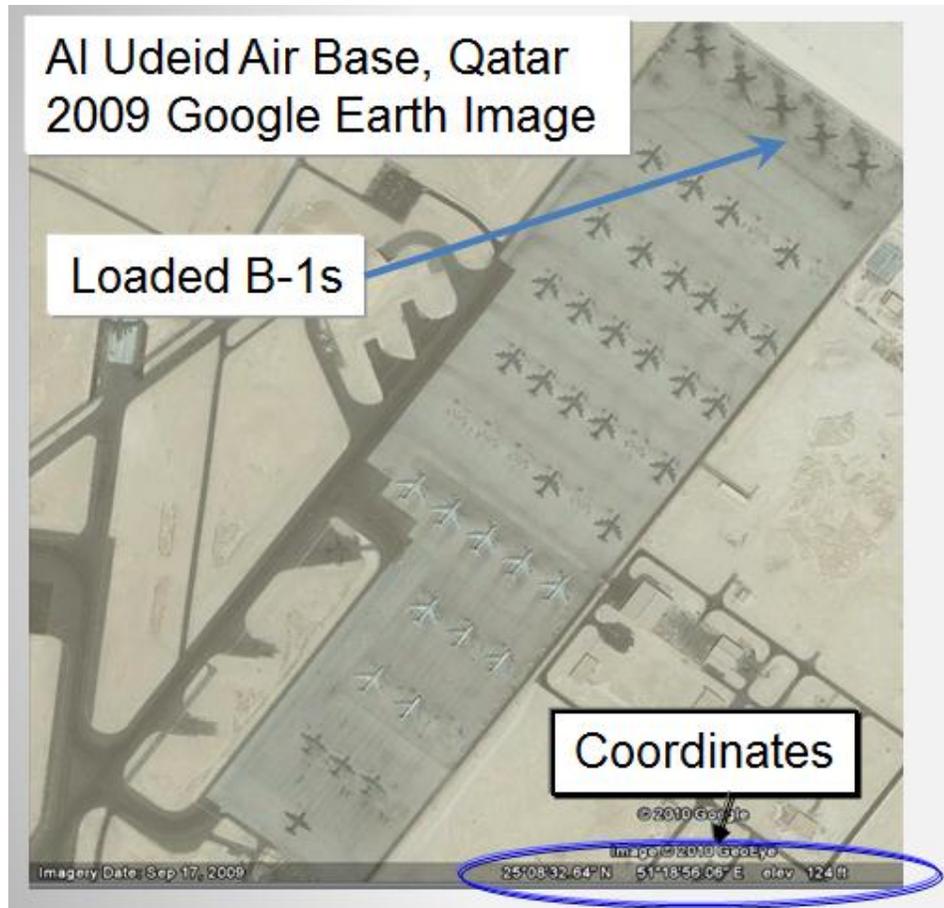


Figure 19: Al Udeid Air Base, Qatar on 17 Sept 2009¹¹²

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. As Bob Pape argues, one must attack a potential adversary's strategy.¹¹³ In short, we need to deny success. To do this, this study argues we need a second concept called "immunization" as well.

Immunization

Immunization as it applies to the U.S. is analogous to an individual getting the annual influenza vaccine. It is a protective measure that reduces an attack's effectiveness. Properly immunized against the flu, one can be coughed upon all winter long and not feel any adverse effects. Similarly, a nation-state properly immunized against attack will not suffer significant damage, even if an attack is launched against it.

For nation-states like the U.S., this immunization process involves implementing physical safeguards around pieces of critical infrastructure that would protect them in the event of an attack. This involves creating back-up methods of operation and functional resilience that result in little or no denigration to operations should an attack happen, creating strategies that enable the flexible selection of options to mitigate the effects of an attack, and the development of cognitive resilience within the populace and the military

so that even if an attack occurs, there is not a disproportionate psychological reaction to the strike.

As threats become more numerous and span ever increasingly large technological sets, immunization will require time, resources and practice to attain. The methods of immunizing computer systems will be different than the methods of immunizing the populace against a biological pathogen. Nonetheless, the country must be prepared to do both, as well as secure our interests from attacks of other types. If we can achieve a level of immunization where the gains to be won by attacking the U.S. and its interests abroad are minimized, then again, 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. 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.

As such, there are several implications for the Air Force. To begin, immunization will require people and materiel. It is not free. The Air Force has experience with hardening facilities from attack by several of these weapon types, and the methods of hardening against traditional attacks will, in many cases, work for the new threats.

The panoply of new threats increases the requirements for the services to work together to create effective immunization and resilience. As we do this, we need to understand not only who is theoretically responsible for certain mission sets, but also who is really going to accomplish them. For example, the U.S. Army is required to defend U.S. Air Force bases from guided rockets, artillery, mortars and munitions (G-RAMM). Yet, when the survey team conducted interviews with several senior U.S. Army leaders and programmers regarding the steps the Army is taking to accomplish this task, found little action being taken. For the Air Force, this means that making the assumption that the bases will be defended may carry with it serious risk.

These interdependences and risks, some of which have not been assessed, may force the re-examination of how the U.S. Air Force presents forces. The current expeditionary method of operations uses canvas as a protective material for personnel, command centers, computer systems and operations centers. The range of threats emerging in the future is such that mere canvas as a protective layer will almost certainly be insufficient for the task. The Air Force will need to consider threats to its bases, logistics, and communications; and will need to examine new technologies and methods to shield aircraft, command centers, and personnel from attacks that may range from conventional guided munitions to electronic or pulsed electromagnetic attack. It will need to explore new and existing technologies to provide resiliency to aircraft, airfields, command and control facilities, and base infrastructure after attacks. Further, these same protection and resiliency considerations need to be extended to our assets in space, as well.

As the team looked across the implications of these future threats, it was acutely aware that these considerations challenge the myopia that has been allowed to permeate the Department of Defense over the last decade. Today, the United States remains focused on unconventional conflict as a result of having spent the last 20 years involved

in wars in the Middle East. While President Obama has announced timelines for handing over the region to the indigenous governments, these timelines are ill-defined and may stretch out years.

While it is perfectly appropriate for warfighters to concentrate on the battle they are currently fighting, the consequence of this concentration is that America's military has been strictly focused on developing-nation unconventional warfare for a generation, and will remain focused on this mission, at least in part, for several more years. 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 are now engaged, and we are not ready. Further, technology is changing at a pace where those who fail to make a concerted effort to stay abreast of new developments find their thinking quickly rendered obsolete. The scope of the threats which we may face from the above technologies is disturbing.

The good news is that one of the Air Force's great strengths has been a tradition of looking ahead, challenging current strategic assumptions, and embracing new technologies. This type of thinking is critical to the Air Force. While not a named "core competency," it has been the Air Force and its predecessor, the Army Air Corps, who have foreseen where technology was leading, and what the next new strategic leaps would be.

Recommendations

Based on the research and findings above, the study team has two sets of recommendations for the Air Force as it moves toward the 2030s. These two sets of recommendations deal with the development of a global vigilance strategy, and the assessment of and addressing the Air Force's immunization needs. 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 have to be endured.

A Global Vigilance Strategy for 2035

To develop a global vigilance strategy for 2035, the Air Force must first re-establish itself as a leader in electronic warfare with increased research and development of equipment as well as increased training. This is essential to be able to handle threats that emerge in cyberspace, and echoes the CSAF General Norton Schwartz' 2010 Vector Statement recommendations.¹¹⁴ The Air Force, however, needs to broaden beyond mere electronic warfare, and become a leader in the field of intelligence, surveillance and reconnaissance. In these areas, the Air Force is the traditional lead service, and so we should be again.

While the Air Force has made great strides in integrating remotely piloted aircraft (RPA), space and cyberspace operations, this integration needs to move toward completion. Real-time sharing, fusing, and cross-cueing from information in each of these realms must be achieved.

As General Schwartz recommended in July 2010, the study also found and recommended that the Title 10 Futures Game should focus on vetting new technologies,

innovative ideas and future concepts of operations, and finding novel ways to institutionally integrate RPAs, space, cyberspace, and real-time data fusion into new ways of conducting business. This creates a pre-requisite that all Title 10 Futures Wargames be fully and completely staffed by and run by visionary leaders who are knowledgeable about emerging technologies and their potential capabilities. This will involve much more careful selection of game players and senior mentors than has been the case in the past. Only by ensuring those creating, playing and running the games are conversant in these technologies and their potential, can one be able to create the new concepts of operations that will be needed to propel the Air Force into the future.

As the global vigilance strategy is developed and as it unfolds over time, the Air Force should constantly re-examine its organizational structures to determine if or when changes are needed to optimize the integration of global vigilance into all facets of its operations. While reluctant to posit precisely what these changes may be, the study team unanimously believed that existing organizational structures would be inadequate to handle transparency at the necessary levels in the 2030 timeframe, and that the Air Force leadership would need to examine organizational structures as the transparency strategy evolved over time.

Lastly, the study team, upon its out-brief, recommended that an informal interagency study group be formed to define the capabilities, capacities, organization, authorities and systems needed to fully enable transparency. As this study's details became more widely known and coordinated, the National Security Staff became aware of and began to work on some of the issues embedded in this report. Presidential Policy Directive 8 (PPD-8) is an outgrowth of the National Security Staff's efforts in these matters. As a result of PPD-8, an interagency group has already been formed, and should present its conclusions to the President later this year (2012). This study believes that interagency cooperation and coordination will be necessary to optimally use precious taxpayer-provided resources to achieve a global vigilance strategy for 2035.

Immunization

As mentioned above, potential adversaries in the future will have access to many of the same transparency-creating technologies that we will have, and as a result, implementing the concept called "immunization" is necessary. To do this, one must have a full assessment of immunization needs and understand where the service is already taking grave risks.

Unfortunately, a full assessment of all the risks the Air Force is taking with regard to its basing, current and future adversary threat laydowns, short-falls in other services' efforts such as the lack of any funding for G-RAMM defense, and interagency issues such as the lack of protection for the national critical infrastructure; has never been done. This leaves the Air Force in a position where the problem set itself remains inadequately defined. Our recommendations here, therefore, take a problem-solution format.

The first step is to fully define this problem, and the Air Force should embark on this step immediately. Several Air Force missions in the future will be at risk due to the variety of threats that will be fielded by potential adversaries, as well as due to underfunding of needed capabilities by ourselves and/or other agencies and services. Increased transparency will mean that the locations of our forces will be known to our

adversaries. The technologies listed above will also be in their hands. This combination places our combat capability at grave risk and will reduce, potentially to zero, our ability to achieve surprise. In an era of precisely targeted conventional missile attacks, directed energy weaponry, and cyber domain warfare, our doctrine of operating from bare bases in an expeditionary manner may put us at unacceptable risk in some theaters. Add potential biological attack, and attacks to our communication and space assets, and one begins to paint a multi-dimensional trade space that has never been fully mapped. The Air Force needs to create and understand this risk map to make mission risk visible, both based on our own funding outlays, and those of other services, agencies, or allies upon which we depend.

Once this risk analysis is complete, then, and only then, can we target research and development in the laboratory system to address the key vulnerabilities. Research and development to improve our ability to harden combat systems, personnel deployment locations, and support infrastructure will be needed to ensure the Air Force is able to survive to operate in future combat environments. This research will likely need to target new material science and communications technologies to deny adversaries the ability to disable our Air Force via an attack.

Only by creating an Air Force that is capable of operating without significant degradation in the face of a potential adversary attack, can we deny success. If we are able to achieve this level of immunization, then an adversary's gains to be won by attacking become so trivial that a rational actor will choose to not strike in the first place. This is part of how deterrence succeeds.

Issues for Other Departments

Because of the breadth of challenges that will confront the United States in the decade of the 2030s, this is much more than a Department of Defense problem. There are issues for the Departments of Homeland Security, Transportation, Health and Human Services and Commerce, as a minimum. There are likely others this study has not stumbled upon as well.

The Department of Homeland Security is responsible for the defense of our national infrastructure and our air transport system. As such, they need to understand the potential impact that directed energy will have on our electrical and banking systems.

Of importance here is that while adversaries can be deterred, our sun cannot. The good news is that when the sun attacks, it gives warning, and the protection of the national infrastructure with warning is a rather trivial problem, assuming a plan is in place to do it.¹¹⁵ Sadly, no such plan exists, and no agreed upon threshold to take action vis-à-vis solar flares exists. While the Department of Commerce looks at weather effects, and NASA looks at solar flares, there is no means by which their respective analyses are combined to make decisions on how to protect the utility systems upon which we all depend. Until there is, we will all remain at risk of a major flare destroying our electrical grid in a manner that could keep the lights out for years.

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 back-lash against limitations such as the 3 ounce bottle limits on commercial aircraft, this problem is about to become 5-10 fold

worse. 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 just nano-engineered 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 nano-explosives is something that must be guarded against as well.

The one potential extinction level event discussed above is biological attack. In the Blue Horizons III study, a major project was recommended to enable rapid detection and decoding of new genomic structures along with the ability to quickly prototype and produce vaccines. We stated then, and reiterate now, that a major project is needed on biogenetics to be able 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 took to develop a vaccine for the H1N1 influenza in 2010. This study concludes that this recommendation remains valid and must be pursued. However, its implementation lies within the purview of the Centers for Disease Control and the National Institutes of Health.

In short, the future technologies studied have the potential to threaten our lives, livelihoods, and infrastructure. Many aspects of protecting these do not lie in Title 10, and must be addressed by the responsible agencies. If they fail to do so, then our ability to deter an adversary by denial may exist within our Air Force, but not within our nation as a whole. Deterrence is a team sport. It is one all the federal agencies must play together.

Summary

The U.S. Air Force Center for Strategy and Technology was asked to examine how the U.S. Air Force could best deter attacks in space and cyberspace, or attacks using biotechnology, nanotechnology, directed energy, and/or nuclear weapons. The Center discovered that these threats, as one looks out toward the year 2035, create a potentially dangerous future for the U.S. and many of our allies and partners around the world.

This study concludes that the threats in these six areas range from very dangerous to the potentially catastrophic, with the nexus between bio and nanotechnology holding the gravest risk of all. The study finds that little has been or is being done to protect America’s citizens or their infrastructure from these threats, but also finds that technologies to mitigate these threats either already exist, or can be developed with time.

Deterrence theory, as originally constructed, is found to be still valid. The basic theory still holds in the future, but the way it must be applied will change. New technologies are susceptible to being deterred through denial, not merely through retribution as was the case with nuclear weapons during the cold war. As such, new strategies, specifically in the areas of transparency and immunization are required.

In summary, we’ve shown that deterrence is based on changing an adversary’s assessment of whether the gains to be won from an attack outweigh the risks (s)he incurs. To do this, one can affect both sides of the deterrence equation, by denying the adversary the opportunity and tools to initiate a successful attack and ensuring the gains to be won are small; as well as by punishing the attacker for the attack once an attack is launched. To achieve the capability to deter by denial and by punishment in the 2030s, the Air Force will need a new vision for global vigilance and a new strategy for immunization.

To achieve the latter, we will need to map the risks that are inherent in our systems and doctrine, and begin researching and developing work-arounds to mitigate these risks. If we do these things, then the adverse consequences and the likelihood of attack using modern conventional and nuclear systems in the 2030s can be significantly reduced, and the threats we fear most, need never materialize.

To achieve this outcome, cooperation is required across the whole of government. While the Air Force has an important role to play, and will inevitably lead in some areas, it is not structured, nor is its mission to accomplish this task alone. Deterrence is a team sport, and every cabinet agency has a position to play on this team. Only when our nation unites to achieve deterrence of these new technologies as a common goal, will it be achieved.

The Center for Strategy and Technology was established at the Air War College in 1996. Its purpose is to engage in long-term strategic thinking about technology and its implications for U.S. national security.

The Center focuses on education, research, and publications that support the integration of technology into national strategy and policy. Its charter is to support faculty and student research; publish research through books, articles, and occasional papers; fund a regular program of guest speakers; and engage with collaborative research with U.S. and international academic institutions. As an outside funded activity, the Center enjoys the support of institutions in the strategic, scientific, and technological communities.

An essential part of this program is to establish relationships with organizations in the Air Force as well as other Department of Defense agencies, and identify potential topics for research projects. Research conducted under the auspices of the Center is published as Occasional Papers and disseminated to senior military and political officials, think tanks, educational institutions, and other interested parties. Through these publications, the Center hopes to promote the integration of technology and strategy in support of U.S. national security objectives.

For further information on the Center for Strategy and Technology, please contact:

Colonel Thomas D. McCarthy, Director
Harry A. Foster, Deputy Director
Grant T. Hammond, Deputy Director, Global Strike
Theodore C. Hailes, Air University Transformation Chair
Lt Col Christopher A. Bohn, Chief Scientist

Air War College
325 Chennault Circle
Maxwell Air Force Base, Alabama 36112
(334) 953-6996/6460/2985

Titles in the Occasional Paper Series

1

Reachback Operations for Air Campaign Planning and Execution
Scott M. Britten, September 1997

2

Lasers in Space: Technological Options for Enhancing U.S. Military Capabilities
Mark E. Rogers, November 1997

3

Non-Lethal Technologies: Implications for Military Strategy
Joseph Siniscalchi, March 1998

4

Perils of Reasoning by Historical Analogy: Munich, Vietnam, and the American Use of Force Since 1945
Jeffrey Record, March 1998

5

Lasers and Missile Defense: New Concepts for Space-Based and Ground-Based Laser Weapons
William H. Possel, July 1998

6

Weaponization of Space: Understanding Strategic and Technological Inevitables
Thomas D. Bell, January 1999

7

Legal Constraints or Information Warfare
Mark Russell Shulmann, March 1999

8

Serbia and Vietnam: A Preliminary Comparison of U.S. Decisions to Use Force
Jeffrey Record, May 1999

9

Airborne and Space-Based Lasers: An Analysis of Technological and Operational Compatibility
Kenneth W. Barker, June 1999

10

Directed Energy and Fleet Defense: Implications for Naval Warfare

William J. McCarthy, February 2000

11

High Power Microwaves: Strategic and Operational Implications for Warfare

Eileen M. Walling, March 2000

12

Reusable Launch Vehicles and Space Operations

John E. Ward, Jr., March 2000

13

Cruise Missiles and Modern War: Strategic and Technological Implications

David J. Nicholls, March 2000

14

Deeply Buried Facilities: Implications for Military Operations

Eric M. Sepp, March 2000

15

Technology and Command: Implications for Military Operations in the Twenty-First Century

William B. McClure, July 2000

16

Unmanned Aerial Vehicles: Implications for Military Operations

David Glade, July 2000

17

Computer Networks and Information Warfare: Implications for Military Operations

David J. Gruber, July 2000

18

Failed States and Casualty Phobia: Implications for Force Structure and Technology Choices

Jeffrey Record, December 2000

19

War as We Knew It: The Real Revolution in Military Affairs/ Understanding Paralysis in Military Operations

Jan S. Breemer, December 2000

20

Using Lasers in Space: Laser Orbital Debris Removal and Asteroid

Deflection

Jonathon W. Campbell, December 2000

21

Weapons for Strategic Effect: How Important is Technology?

Collin S. Gray, January 2001

22

*U.S. Army Apache Helicopters and U.S. Air Force Expeditionary Forces:
Implications for Future Military Operations*

Brad Mason, June 2001

23

The End of Secrecy? Military Competitiveness in the Age of Transparency

Beth M. Kasper, August 2001

24

Prompt Global Strike Through Space: What Military Value?

Larry G. Sills, August 2001

25

*Precision Engagement at the Strategic Level of War: Guiding Promise or
Wishful Thinking?*

Timothy J. Sakulich, December 2001

26

Infrared Systems for Tactical Aviation: An Evolution in Military Affairs?

George B. Hept, January 2002

27

*Unmanned Undersea Vehicles and Guided Missile Submarines:
Technological and Operational Synergies*

Edward A. Johnson, Jr., February 2002

28

Attack Operations for Missile Defense

Merrick E. Krause, May 2002

29

*Death by a Thousand Cuts: Micro-Air Vehicles in the Service of Air
Force Missions*

Arthur F. Huber II, June 2002

30

Sustained Space Superiority: A National Strategy for the United States

Larry J. Schaefer, August 2002

31

Hyperspectral Imaging: Warfighting Through a Different Set of Eyes

Paul J. Pabich, October 2002

32

Directed Energy Weapons on the Battlefield: A New Vision for 2025

John P. Geis II, April 2003

33

Homeland Security and the Coast Guard: Postured for Technology Improvements

Arthur C. Walsh, June 2003

34

Non-Lethal Weapons: Setting our Phasers on Stun? Potential Strategic Blessings and Curses of Non-Lethal Weapons on the Battlefield

Erik L. Nutley, August 2003

35

Aircrew Performance Cutting Edge Tech

Kris M. Belland, September 2003

36

Centralized Control with Decentralized Execution: Never Divide the Fleet

Daniel F. Baltrusaitus, May 2004

37

The Decision Maker's Guide to Robust, Reliable and Inexpensive Access to Space

Gary N. Henry, July 2004

38

Global Mobility: Anywhere, Anytime, Any Threat? Countering the MANPADS Challenge

Jacqueline D. van Ovost, July 2005

39

Strategies For Defeating Commercial Imagery Systems

Stephen Latchford, July 2005

40-51

Netted Bugs and Bombs: Implications for 2010

Edited by Marsha J. Kwolek. December 2005

Part I: Network Centric Operations: Promises and Pitfalls

Network Warfare Operations: Unleashing the Potential
Richard A. Lipsey

Network-centric Operations: Challenges and Pitfalls
Eric E. Silbaugh

Network-enable Precision Guided Munitions
Benjamin F. Koudelka Jr.

Lowering the High Ground: Using Near-Space Vehicles for Persistent C3ISR
Andrew J. Knoedler

Part II: UAVs in 2010: Lean and Lethal

Unmanned Combat Aerial Vehicles: SEAD and EW for the Future
James C. Horton

Small Power: The Role of Micro and Small UAVs in the Future
James M. Abatti

Pesky Critters
Kirk M. Kloepple

Pandora's Box Opened Wide: UAVs Carrying Genetic Weapons
Daryl J. Hauck

Part III: Silver Bullets in Search of a Six Shooter

Perfecting War: Searching for the Silver Bullet
Eric J. Schnitzer

Who Pushes the Pickle Button?
John E. Marselus

Leveraging Simulation Against the F-16 Flying Training Gap
Shaun R. McGrath

Electronic Pulse Threats in 2010
Colin R. Miller

52

Ground Truth: The Implications of Joint Interdependence for Air and Ground Operations
L. Ross Roberts, March 2006

53

"Heads, Not Tails:" How To Best Engage Theater Ballistic Missiles?

Ronald C. Wiegand, February 2006

54

Transcendental Terrorism and Dirty Bombs: Radiological Weapons Threat Revisited
Chad Brown, February 2006

55

International Armament Cooperative Programs: Benefits, Liabilities, and Self-inflicted Wounds---The JSF as a Case Study
Stephen G. DiDomenico, February 2006

56

War Without Oil: A Catalyst For True Transformation
Michael J. Hornitschek, May 2006

57-59

Streamlining DOD Acquisition: Balancing Schedule With Complexity
Edited by Lt Col James Rothenflue and Marsha J. Kwolek,
September 2006

A System as the Enemy: A Doctrinal Approach to Defense Force Modernization
Benjamin A. Drew

Impact of Weapons Systems Complexity on Systems Acquisition
Robert A. Dietrick

Faster is Better...Can the USAF Acquisition Process be SAIV'D?
James L. Chittenden

60

The Seductive Effects of an Expeditionary Mindset
Michael Arnold, March 2007

61

The Air Force in SILICO – Computational Biology in 2025
Christopher Coates, December 2007

62

Biofuels: An Alternative to U.S. Air Force Petroleum Dependency
Mark S. Danigole, December 2007

63

Air Force and the Cyberspace Mission: Defending the Air Force's

Computer Network in the Future
Shane P. Courville, December 2007

64

Next Generation Nanotechnology Assembly Fabrication Methods: A Trend Forecast
Vincent T. Jovene, Jr., January 2009

65

*Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030:
Executive Summary*
John P. Geis II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster, and David Blanks,
July 2009

66

Resurgent Russia in 2030: Challenge for the USAF
Theodore C. Hailes, Ronald Buckley, David Blanks, Mark Butler, Phillip Preen and
Michael Tarlton, September 2009

67

Failed State 2030: Nigeria – A Case Study
Christopher J. Kinnan, Daniel B. Gordon, Mark D. DeLong, Douglas W. Jaquish and
Robert S. McAllum, February 2011

68

Discord or Harmonious Society? China in 2030
John P. Geis II, Scott E. Caine, Edwin F. Donaldson, Blaine D. Holt, and Ralph A.
Sandfry

69

Finding the Shape of Space
Christopher C. Shannon, Scott J. Scheppers, Dustin P. Ziegler, Brian C. McDonald,
David Suh Hoon Menke, John P. Geis II, Amanda S. Birch and Tosha N. Meridith, July
2011

NOTES

¹ Memorandum of Agreement entitled “Strategic Studies (Blue Horizons) Special Interest Item,” signed by General John D. W. Corley, Vice Chief of Staff of the United States Air Force, on May 17, 2006.

² Moseley, T. Michael and the Air Force Center for Strategy and Technology, *Blue Horizons 2007: Horizons 21 Project Report*, (Headquarters U.S. Air Force: Washington DC) 2008, 86 pp.

³ Friedman, Thomas L., *The World is Flat*, (Farar, Straus, and Giroux: New York, NY), 2005, 488 pp.

⁴ Geis, John P. II, Harry A. Foster, Theodore A. Hailes, and Christopher J. Kinnan, *Blue Horizons III: The Age of Surprise*, (Maxwell AFB, AL: Air University Press), 2012. Center for Strategy and Technology Monograph # 70.

⁵ Mosely, *Blue Horizons 2007: Horizons 21 Study Report*, and Geis, John P. II, Christopher J. Kinnan, Ted Hailes, Harry A. Foster and David Blanks, *Blue Horizons II: Future Capabilities and Technologies for the Air Force in 2030* (Maxwell AFB, AL: Air University Press) 2009.

⁶ This phrase is often used by the Chief Scientist of NASA’s Langley Research Center, Dennis Bushnell to title some of his presentations.

⁷ The Center for Strategy and Technology has collaborative research relationships with all ten research directorates of the Air Force Research Laboratory, Sandia National Laboratory, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, as well as the National Aeronautics and Space Administration. As needed, the Center reaches out to scientists and engineers from industry, the academy and additional laboratories to complete its research. Specific debts of gratitude are owed to the following individuals who contributed to this study and who were willing to be named: John Mearsheimer (University of Chicago), Robert Pape (University of Chicago), Jacek Kugler (Claremont Graduate University), General (ret) Mike Hayden, General (ret) John Shaud, Dennis Bushnell (NASA Langley Research Center), Peter S. Hamilton (Sandia National Laboratories), Larry A. Schoof (Sandia National Laboratories), Lt Col Joel Almosara, Colonel David P. Blanks, Lt Col Darren Buck, Lt Col Patrick C. Burke, Colonel Christopher Kinnan, Lt Col Thomas Coglitore, Lt Col Miguel J. Colon, Commander Peter R. Falk, Colonel Michael Finn, Major General Maury Forsyth, Lt Col John W. Gloystein., Colonel Christopher P. Hauth, Colonel William P. Jensen, Major General Robert Kane, Mark J. Krause, Lt Col Douglas J. Mellars, Lieutenant General Allen Peck, Colonel Stella T. Smith, Lt Col Robert S. Spalding, Lt Col Michael J. Stephens, Lt Col Edward L. Vaughan, Colonel Ancel B. Yarbrough

Many others contributed, but were too modest to let us list them here.

⁸ There is nothing in this work, nor any source used to compile this work which is or draws upon classified material.

⁹ The majority of researchers visited Sandia National Laboratories in Albuquerque, New Mexico and Los Alamos National Laboratories in Los Alamos, New Mexico. The faculty advisors and principle authors also visited with scientists and researchers at Lawrence Livermore National Laboratories in Livermore, California.

¹⁰ Dalkey, Norman, and Olaf Helmer. “An Experimental Application of the DELPHI Method to the Use of Experts.” *Management Science*, Vol. 9, no. 3: 458-467. Norman and Olaf discuss the method in depth, as well as its origins in RAND’s Project DELPHI. In this case the formal Delphi method was used as described in Norman and Heimer. This study then used an informal variant of the Delphi method to see if the results were robust to multiple methodological approaches. For more on this method, see: Linstone, Harold A., Murray Turrff, and Olaf Helmar. *The Delphi Method: Techniques and Applications*. (University Heights, NJ: New Jersey Institute of Technology), 2002.

¹¹ Graph compiled by authors using data from Intel. See “The Evolution of a Revolution” The Intel Corporation, available at: <http://download.intel.com/pressroom/kits/IntelProcessorHistory.pdf> as of November 17, 2011

¹² Geis, et. al, *Blue Horizons III: The Age of Surprise*

¹³ Data from Internet Systems Consortium, “Internet Host Count History,” available on-line at: <http://www.isc.org/solutions/survey/history> as of November 17, 2011.

¹⁴ Petersen, John L., “Punctuations” *FUTUREdition*, Vol 15, No. 8, April 30, 2012.. Petersen’s article will be published as the forward in *Infinite Energy Technologies*, forthcoming.

¹⁵ Ibid. See also, Kurzeil, Ray, *The Singularity is Near* (New York, NY: Penguin Books), 2005, pp. 10-50

¹⁶ Moseley, *Blue Horizons 2007: Horizons 21*. These numbers have not changed much since 2007, as verified in a 2012 Study by Battelle. See Wadsworth, Jeffrey, *2012 Global R&D Funding Forecast*,

(Battelle Corporation: Washington DC), December 2011, pp. cover through p. 3. Wadsworth points out that U.S. R&D spending will top \$420 billion, but only \$128 billion will be driven by the government – a total of 29 percent. The U.S. continues to hold about 30 percent of the global R&D share.

¹⁷ Among the examples of this research conducted recently are: Coates, Christopher, *The Air Force in SILICO: Computational Biology in 2025*, John P. Geis II, ed. (Maxwell AFB, AL: Air University Press), December 2007; Courville, Shane, *Air Force and the Cyberpspace Mission: Defending the Air Force's Computer Network in the Future*, (Maxwell Air Force Base: Air University Press), December 2007; Danigole, Mark S., *Biofuels: An Alternative to U.S. Petroleum Dependency*, John P. Geis II, ed. (Maxwell AFB, AL: Air University Press), December 2007; and Jovene, Vincent T., *Next Generation Nanotechnology Assembly Fabrication Methods: A Technology Forecast* (Maxwell AFB, AL: Air University Press), January 2008.

¹⁸ Information Technology Associates, "Educational Score Performance – Country Rankings," *World Fact Book*, available on-line at http://www.geographic.org/country_ranks/educational_score_performance_country_ranks_2009_oecd.html as of May 12, 2012. Original data from the 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).

¹⁹ Porter, Alan L., Nils C. Newman, Xiao-Yin Jin, David M. Johnson and J. David Roessner, *High Tech Indicators: Technology-based Competitiveness of 33 Nations – 2007 Report*, (Technology Policy and Assessment Center: Georgia Institute of Technology) January 22, 2008, p. 23. Report available at: http://www.au.af.mil/au/awc/awcgate/nsf/nsf_hi_tech_indicators_33_nations.pdf as of May 12, 2012.

²⁰ Friedman, *The World is Flat* pp. 48-222

²¹ The fastest computer process of 30 years ago, the 8088, operated at a clock speed of not more than 4.7 megahertz. Today, computer chips in standard cell phones routinely exceed 2 gigahertz, or roughly 500 times faster and at lower prices than the first 8088 based computers.

²² Moore's Law posits that computer processor capabilities will double every 18 months. This yields 20 doublings in a 30 year period or an increase of approximately 1.048 million fold.

²³ Moseley, *Horizons 21*.

²⁴ Estimates of the numbers of these groups vary widely. The lowest estimate the authors encountered in their research was 13,425, which is cited by the United Nations. Mainstream estimates are in the range of a few tens of thousands, with some upper end estimates around 60,000. For more data, see: *The United Nations Today*, (New York, NY: United Nations Department of Public Information), October 2008. See also, Anheier, Helmut, Marlies Glasius and Mary Kaldor, "Introducing Global Civil Society," *Global Civil Society Yearbook*, (Oxford, UK: Oxford University Press), pp. 2-38

²⁵ Two computers have already successfully passed a version of the Turing test – the test where a computer mimics human behavior so closely that in a blind test observers cannot discern which actor in a line-up is the computer. The first such event was in was Elbot, which successfully convinced two judges out of three after a five minute interview that it was a human as opposed to the other humans in the test, one of whom fared more poorly. Elbot won the Loebner Prize in 2008. Saygin, A.P., "Comments on Computing Mathincer and Intelligence by Alan Turing," in Epstein, R.; Roberts, G; Poland G., *Parsing the Turing Test*, (Dordrecht, Netherlands: Springer), 2008. The other such computer is Watson. See: Kurzweil, Raymond, "The Significance of Watson," *Kurzweil Accelerating Intelligence Blog*, February 13, 2011, available at: <http://www.kurzweilai.net/the-significance-of-watson> It is worth noting that Kurzweil believes the Loebner threshold for passing the Turing test is too low, and that genuine human intelligence will be reached by 2029.

²⁶ "U.S. and World Population Clocks," U.S. Census Bureau, available on-line at: <http://www.census.gov/ipc/www/idb/worldpoptotal.php> as of May 12, 2012

²⁷ Ridley, Matt, "Humans: Why they Triumphed," *The Wall Street Journal*, May 22, 2010, available on-line at: <http://online.wsj.com/article/SB10001424052748703691804575254533386933138.html> See also: Ridley, Matt, *The Rational Optimist: How Prosperity Evolves*, (New York, NY: Harper Collins) 2010.

²⁸ Hallam, A., and P. B. Wignall, *Mass Extinctions and their Aftermath*, (Oxford, England: Oxford University Press), 2002. Based on Hallam and Wignall's calculations, the combined extinction loss from the five major extinction events (End-Ordovician [84%], Late Devonian [83%], End Permian [95%], End Triassic [80%] and End Cretaceous [76%]) would be 99.994%. 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.

²⁹ Geis, et.al., *Blue Horizons III: The Age of Surprise*.

³⁰ Schwartz, Peter, *The Art of the Long View*, (New York, NY: Doubleday), 1991, pp. 17-169.

³¹ Schwartz, Peter, *Inevitable Surprises: Thinking Ahead in a Time of Turbulence*, (New York, NY: Gotham Books), 2003, pp. 1-236.

³² “Protecting the National Infrastructure: Idaho’s Test Range,” Fact Sheet issued by the Department of Energy, available at:

http://www.inl.gov/nationalsecurity/factsheets/docs/critical_infrastructure_test_range.pdf as of May 14, 2012.

³³ The precise area of attack appears to remain classified, so the authors cannot say what system or set of systems was affected to result in the catastrophic failure of the generator. That the generator catastrophically failed is known and was aired on CNN News, and is also available via other media including You-tube. For the original article on the test, see: Meserve, Jeanne, “Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid,” *CNN.com*, September 26, 2007, available at:

http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US as of May 14, 2012.

³⁴ Photograph courtesy of the Department of Homeland Security

³⁵ Slay, J. and Miller, M. “Lessons Learned from the Maroochy Water Breach,” *Critical Infrastructure Protection*, Vol 253, November 2007, pp. 73-82. For a broader discussion of these events, see also, Tsang, Rose, “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks” unpublished paper from the University of California Berkeley, available at:

http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf as of May 14, 2012.

³⁶ “Teen Hacker Faces Federal Charges,” *CNN Interactive* on-line at

<http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html>, March 18, 1988.

³⁷ Tsang, “Cyberthreats, Vulnerabilities, and Attacks on SCADA Networks,” and “Cracks in the System,” *Time*, January 9, 2002.

³⁸ Geis, et.al, *Blue Horizons III: The Age of Surprise*

³⁹ The program to smoothly and seamlessly stitch pictures together was developed by Microsoft and is called “Photosynth.” Available on the Internet for free, the program enables compilation of images across space and time to produce the ability to conduct three-dimensional walkthroughs of any facility ever photographed. For more, see: Geis, John P. II, Ted Hailes and Grant Hammond, “Technology and the Comprehensive Approach: Part Problem, Part Solution,” *Capability Development in Support of comprehensive Approaches: Transforming International Civil-Military Relations*, Derrick Neal and Linton Wells, ed., (Washington DC: National Defense University Press), 2011, pp. 69-86

⁴⁰ Ibid.

⁴¹ Human Genome Project Information website. See:

http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml as of May 14, 2012.

⁴² Miller, Michael B., “How tall of a stack of paper would we need to print out an entire human genome?” Division of Epidemiology and Community Health, University of Minnesota, October 15, 2005, available on-line at: http://bio4.us/biotrends/human_genome_height.html

⁴³ Human Proteome Organisation (HUPO) Homepage and Website available at:

<http://www.hupo.org/research/hpp/> last updated March 21, 2012 as of May 14, 2012.

⁴⁴ More specifically, these medications are called tyrosine-kinase inhibitors which inhibit reproduction by inhibiting the enzymes involved in signal transduction cascades by adding a phosphate group to the appropriate protein. For some of the latest in developments on the leukemia medications, see: DiBella, Nicholas J., “First-line Treatment of Chronic Myeloid Leukemia: Imatinib versus Nilotinib and Dasatinib,” *Community Oncology*, Vol 8, No. 2, February 2011, pp. 65-72

⁴⁵ Interview by authors with the leading biological scientists at Los Alamos National Laboratory, August 26, 2010, and on subsequent dates. See also: Geis, et.al, *Blue Horizons III: The Age of Surprise*.

⁴⁶ “Mouse Pox or Bioweapon?” *BBC World Service*, January 17, 2001, available on-line at:

http://www.bbc.co.uk/worldservice/sci_tech/highlights/010117_mousepox.shtml as of May 15, 2012.

⁴⁷ Bains, William, *Biotechnology from A to Z*, (Oxford, England: Oxford University Press), 2004, p. 52.

⁴⁸ The dictionaries the authors were issued by the Federal government are among those that do not yet contain an entry for nano-technology.

-
- ⁴⁹ Hall, J. Storrs, *Nanofuture: What's Next for Nanotechnology*, (Amherst, NY: Prometheus), 2005, pp. 15-22
- ⁵⁰ Definition synthesized from Hall, *Ibid.*, pp. 15-51
- ⁵¹ Los Alamos National Laboratories interview.
- ⁵² Gutkowski, W. and T.A. Kowalewski. *Mechanics of the 21st Century*. Netherlands: Springer, 2005, p. 379; Vasyilkiv, Oleg, Yoshio Sakka and Valeriy V. Skorokhod. "Nano-Blast Synthesis of Nano- Size CeO₂-Gd₂O₃ Powders," *Journal of American Ceramic Society*, No. 89, 2006.
- ⁵³ Cole, John W., Isaac F. Silvera and John P. Foote. "Conceptual Launch Vehicles Using Metallic Hydrogen Propellant." Space Technology and Applications International Forum 2008. *American Institute of Physics Conference Proceedings*, Vol. 969, January 2008.
- ⁵⁴ It is interesting to note that a yield increase of 1000-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.
- ⁵⁵ Yarbrough, Ancel, The Impact of Nanotechnology Energetics on the Department of Defense by 2035, Master's Thesis, February 17, 2010, available on-line at <https://www.afresearch.org/skins/rims/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=bc60df64-ed43-443c-a738-bb5a063bf362> as of May 24, 2011
- ⁵⁶ Baird, Henry D., Steven D. Acenbrack, William J. Harding, Mark J. Hellstern and Bruce M. Juselis, "Spacelift 2025: The Supporting Pillar for Space Superiority," *Air Force 2025 Volume 2*, (Maxwell AFB, AL: Air University Press), 1996, pp. 117-150
- ⁵⁷ "Nanoparticles and their Applications," available at <http://nanogloss.com/nanoparticles/nanoparticles-and-their-applications/#more-178> as of May 16, 2012. Of course, nanotechnology, like biotechnology above, can cut both ways. The same basic science that can create nano-corrosives can also create nano-coatings that would make systems resist corrosion. There are over 30,000 scholarly articles on this subject. Among the more heavily cited are: Radhakrishnan, S., C.R. Sije, Debajyoti Mahanta, Satish Patil and Giridhar Madras, "Conducting Polyaniline-nano-TiO₂ Composites for Smart Corrosion Resistant Coatings," *Electrochimica Acta*, Vol. 54, No. 4, January 2009, pp. 1249-1254; Benea, Lidia, Pier Luigi bonora, Alberto Borello, and Stefano Martelli, "Wear Corrosion Properties of Nano-Structured SiC-Nickel Composite Coatings Obtained by Electroplating," *Wear*, Vol 249, No. 10-11, pp. 995-1003; and Kendig, Martin, Melitta Hon, and Leslie Warren, "'Smart' Corrosion Inhibiting Coating," *Progress in Organic Coatings*, Vol 47, No. 3-4, September 2003, pp. 183-189.
- ⁵⁸ Nanogloss.com, *ibid.*
- ⁵⁹ The study participants believe the U.S., Russia, China, the United Kingdom, France, India, Pakistan, Israel, and North Korea are nuclear states. Iran and Myanmar appear to be attempting to join the ranks, though this is not knowable with certitude.
- ⁶⁰ A discussion of the chain reaction necessary and how to detonate a nuclear weapon can be found in: Shortley, George and Dudley Williams, *Elements of Physics, 5th Edition*, (Englewood Cliffs, NJ: Prentice Hall), 1971, pp. 924-927. This book was used for high school physics at Brookfield East High School, in Brookfield, Wisconsin, in 1979. As this was the book's fifth printing, the authors make the assumption that it was likely being used in several other learning institutions simultaneously.
- ⁶¹ Wood, Lowell, *Effect of Electromagnetic Pulse Attacks*, Testimony before the House of Representatives Committee on Armed Services Subcommittee on Military Research and Development, October 7, 1999, prepared statement, pp. 1-3. See also: Geis, John P. II, *Directed Energy Weapons on the Battlefield: A New Vision for 2025* (Maxwell AFB, AL: Air University Press), April 2003, pp. 8-11
- ⁶² Geis, *Ibid.*, and Wood, Lowell, William Graham, Michael Bernardin, and Stanley J. Jakubiak, *Effects of Electromagnetic Pulse Attacks*, Testimony before the House of Representatives Committee on Armed Services Subcommittee on Military Research and Development, October 7, 1999, response to questions from Representative Roscoe G. Bartlett (R-MD), p. 120. Available on-line at: http://commdocs.house.gov/committees/security/has280010.000/has280010_0.HTM as of May 16, 2012.
- ⁶³ Pittock, A.B., T. P. Ackerman, P. J. Crutzen, M.C. MacCracken, C. S. Shapiro and R. P. Turco, "Direct Effects of Nuclear Detonations," in *Environmental Consequences of Nuclear War, Volume I*, (New York, NY: John Wiley and Sons), 1986, pp. 1-23.
- ⁶⁴ Geis, *Directed Energy Weapons on the Battlefield*, p. 9
- ⁶⁵ Pittock, et.al, pp. 17-20 and Geis, *Directed Energy Weapons on the Battlefield*, 11-14..

-
- ⁶⁶ For a complete discussion on the precise thresholds of field strength to cause certain levels of damage, see Geis, *Directed Energy Weapons on the Battlefield*, pp. 11-15.
- ⁶⁷ 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.
- ⁶⁸ Ibid.
- ⁶⁹ Kopp, Carlo, "The Electronmagnetic Bomb – A Weapon of Electrical Mass Destruction" *Air and Space Power Journal Chronicles*, May 10, 2012. Available at: <http://www.ausairpower.net/ASPC-E-Bomb-Mirror.html> as of May 16, 2012.
- ⁷⁰ "Italy Readies Beam to Knock Out Pirate Engines: Electromagnetic Attack Overloads Voltage," *Defense News*, February 28, 2011, p. 1.
- ⁷¹ Ibid and Geis, *Directed Energy Weapons on the Battlefield*, pp. 11-15
- ⁷² Interview with Dr. Paul Kintner, Professor of Electrical and Computer Engineering, Cornell University. Dr. Kintner served on the science board of the National Academies and was regarded as one of the nation's leading scientists on the impacts of space weather on both space and terrestrial systems. He was also the Director of the Global Positioning Systems Laboratory at Cornell. Dr. Kintner died shortly after the interview due to pancreatic cancer.
- ⁷³ Dayton, Leigh, "Solar Storms Halt Stock Market as Computers Crash," *New Scientist*, September 9, 1989. Dayton also quotes Canadian scientists as attributing rushes of computer failures across the country, to include individual's personal computers at home, to the solar flare activity of March 1989.
- ⁷⁴ "Solar Shield – Protecting the North American Power Grid," *NASA Science News*, October 26, 2010
- ⁷⁵ *Severe Space Weather Events – Understanding Societal and Economic Impacts*, Workshop Report by the Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, National Research Council of the National Academies, (Washington DC: National Academies Press), 2008. Available on-line at: <http://www.nap.edu/catalog/12507.html> as of May 17, 2012. Also, Author interview with Dr. Paul Kintner, September 17, 2009. The National Academies estimate the economic impact at over \$1 trillion and perhaps as much as \$2 trillion, or a loss of roughly 10 percent of GDP, which is the economic definition of a depression. Some of the over 130 million people who would lose electricity in such a scenario would have to wait the entire 6 years before the lights came back on, though restoration to others via rolling blackouts could happen more quickly.
- ⁷⁶ *Space Severe Weather Events*, p. 78
- ⁷⁷ Bell, Trudy E., and Tony Phillips, "A Super Solar Flare," *NASA Science News*, May 6, 2008, available at: http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/ as of May 17, 2012.
- ⁷⁸ Interview with Paul Kintner.
- ⁷⁹ Emails between the authors and Michael Walters and Kenneth Friedman of the Departments of Homeland Security and Energy respectively. In email and telephonic conversations, both confirmed that there are no plans in place to address the challenges posed to the national critical infrastructure by solar flares or other like effects. Emails and phone conversations occurred from May 9-13, 2010.
- ⁸⁰ 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: http://www.wickedlasers.com/lasers/Spyder_III_Pro_Arctic_Series-96-37.html In recent months, a new company has begun marketing an even smaller laser that is much more powerful than the Spyder. Their laser creates temperatures of up to 850 degrees at the point of lasing. See: <http://www.awesomelasers.com>
- ⁸¹ The authors searched for importation restrictions on lasers across the world. While it is possible some were missed in the search, after an exhaustive search, only the country of Malta had laws we could locate that prevented the importation of a category IV device.
- ⁸² Author presented early findings at the Aircraft Survivability Conference in Berlin, Germany, on October 13, 2010. In discussions with members of the German Parliament who were present, concern was expressed over recent lasing incidents on the autobahn. These government leaders were unaware of the newly marketed handheld device.
- ⁸³ Potter, Mathew, "Boeing Video of Advanced Tactical laser Aircraft," *Defense Procurement News*, October 2, 2009, available at: <http://www.defenseprocurementnews.com/2009/10/02/boeing-video-of-advanced-tactical-laser-atl-aircraft/> as of May 25, 2011.
- ⁸⁴ Geis, *Directed Energy Weapons on the Battlefield*.

⁸⁵ Covault, Craig, “Chinese Test Anti-Satellite Weapon,” *Aviation Week and Space Technology*, January 17, 2007, available on-line at:

http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/CHI01177.xml
accessed May 25, 2011

⁸⁶ Diehl, William, *Continued Optical Sensor Operations in a Laser Environment*, Master’s degree paper, n.p., accessed February 16, 2011.

⁸⁷ “GPS Applications,” April 10, 2012, available at <http://www.gps.gov/applications/> as of May 18, 2012.

GPS.gov is the official U.S. governmental GPS website. The reader should note that the uses of GPS listed here is not exhaustive, and many others can be found on the site.

⁸⁸ Daly, P., “Navstar GPS and GLONASS: Global Satellite Navigation Systems,” *Electronics and Communication Engineering Journal*, Volume 5, Number 6, December 1993, pp. 349-357

⁸⁹ “GPS Applications,” and “NOAA’s Geostationary and Polar-Orbiting Weather Satellites,” *NOAA Satellite Information System*, available at: <http://noaasis.noaa.gov/NOAASIS/ml/genlsatl.html> as of May 18, 2012.

⁹⁰ Hardening efforts remain stable but at low levels. In late 2010, Honeywell introduced a radiation hard 64 megabyte memory for satellites. This is the state of the art, which greatly lags chip sets and memory for terrestrial-based personal computers. For more, see; McHale, John, “Radiation-Hardened Electronics Technology remains Stable Amid Steady Demand in the Space Market,” *Military and Aerospace Magazine*, May 21, 2010, available at: <http://www.militaryaerospace.com/articles/2010/05/radiation-hardened-electronics.html> as of May 18, 2012, and “Megarad-level Rad-hard 64 Megabit Solid-State Memory Introduced by Honeywell for Military Satellites,” *Military and Aerospace Magazine*, December 10, 2010, available on-line at: <http://www.militaryaerospace.com/articles/2010/12/megarad-level-rad-hard.html> as of May 18, 2012.

⁹¹ While not an exhaustive list, the following scholars and works were among the primary ones used to derive the model: 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,” in *World Politics*, Vol. 36, No. 4, Jul, 1984, 496; Lawrence Freedman, *Deterrence*, (Cambridge: UK, Polity Press, 2004);

Christopher Layne, “From Preponderance to Offshore Balancing,” in *The Use of Force: Military Power and International Politics*, ed Robert J. Art and Kenneth N. Waltz, (Oxford: Rowman and Littlefield Publishers, 1999); 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); Keith B. Payne, *The Fallacies of Cold War Deterrence*, (Lexington, KY: The University Press of Kentucky, 2001); Graham Allison and Philip Zelikow, *Essence of Decision; Explaining the Cuban Missile Crisis*, (New York, NY: Longman, 1999); John P. Geis, II, PhD, Colonel, USAF, Scott E. Caine, Lieutenant Colonel, USAF, Edwin F. Donaldson, Colonel, USAF, Blaine D. Holt, Colonel, USAF, Ralph A Sandfry, PhD, Lieutenant Colonel, USAF, *Discord or “Harmonious Society”?* *China in 2030*, Occasional Paper No. 65, Center for Strategy and Technology (Maxwell AFB, AL: Air University Press, February 2011); Bruce Russett and Alan C. Stam, “An Expanded NATO vs Russia and China,” in *The Use of Force; Military Power and International Politics*, ed Robert J Art and Kenneth Walz, (Oxford: Rowman and Littlefield Publishers, 1999); Thomas 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, “History of Russia’s Anti-Ballistic Missile System,”

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,” *Strategic Insights* Volume IV, Issue 9 (September 2005), Center for Contemporary Conflict, Naval Postgraduate School, Monterey CA, <http://www.CCC.nps.navy.mil/si/2005/Sep/yaoSep05.asp> ; Kenneth N. Waltz,

“Nuclear Myths and Nuclear Realities,” in *The Use of Force: Military Power and International Politics*, ed Kenneth N Waltz and Robert J Art, (New York: Rowman and Littlefield, 1999); Bob Gourley, *Towards a Cyber Deterrent*, (draft paper for the Cyber Conflict Studies Association, 29 May 2008),

<http://www.ctovision.com/cyber-deterrence-initiative.html> ; Thomas Barnett, “Deterrence in the 21st Century,” in *Deterrence 2.0: Deterring Virtual Non-State Actors in Cyberspace*, Study prepared for USSTRATCOM Global Innovation and Strategy Center’s Strategic Multi-Layer Analysis Team, eds Carl Hunt and Nancy Chessner, 10 January 2008; Mansfield, Edward D., *Power Trade and War*, (Princeton, NY: Princeton University Press, 1994); Mearsheimer, John J. , *Conventional Deterrence*, (Ithica, NY:

Cornell University Press, 1985) ; Levy, Jack S., “The Causes of War: A Review of Theories,” *Behavior, Society and Nuclear War, Volume 1*, Philip E. Tetlock, Jo L. Husbands, Robert Jervis, Paul C. Stern and Charles Tilly, eds. (Oxford: Oxford University Press, 1989) pp. 209-333; Organski, A.F.K., and Jacek Kugler, *The War Ledger*, (Chicago, IL: University of Chicago Press, 1980
 Doyle, Michael W. *Striking First: Preemption and Prevention in International Conflict*, (Princeton, NJ: Princeton University Press, 2008); *Complex Deterrence*, Paul, T.V., Patrick M. Morgan, and James J. Wirtz, eds.(Chicago, IL: University of Chicago Press, 2009); and *Proceedings: Deterrence in the Twenty-First Century*, Cain, Anthony C., ed., (London: Air University Press, 2009)

⁹² *Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*, (Washington DC: United States Department of State) available at: <http://www.state.gov/t/isn/trty/16332.htm> as of May 18, 2012.

⁹³ Mearsheimer, *Conventional Deterrence*, p. 23

⁹⁴ This calculus can be traced back to Thucydides who wrote in Book V of his *History of the Peloponnesian War*, when he laments that in war “one side believes the gains to be won outweigh the risks to be incurred, and the other is willing to accept danger rather than face an immediate loss.”

⁹⁵ Kelly, Harold H. 1973. “The Process of Causal Attribution,” *American Psychology*, Vol. 28, No. 2, pp. 107-128; Tversky, Amos & Daniel Kahneman 1974. “Judgment under Uncertainty: Heuristics and Biases,” *Science*, Vol. 185, No. 4155, pp. 1124-1131 and Nisbett, Richard & Lee Ross, 1980. *Human Interference: Strategies and Shortcomings of Social Judgment*, (Englewood Cliffs, NJ: Prentice Hall).

⁹⁶ Janis, Irving L. & Leon Mann 1977. *Decision-Making: A Psychological Analysis of Conflict, Choice and Commitment*, (New York: Free Press); Heradstveit, Daniel & G. Matthew Bonham, “Decision-Making in the Face of Uncertainty: Attributions of Norwegian and American Officials,” *Journal of Peace Research*, Vol. 23, no 4. December 1986, pp. 339-356

⁹⁷ The Observe, Orient, Decide, Act cycle, or OODA-Loop was coined by: Boyd, John R., *A Discourse on Winning and Losing*, available at <http://www.ausairpower.net/APA-Boyd-Papers.html> as of May 22, 2012.

⁹⁸ *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues*, September 30, 2010, p. 2. Available at: <http://www.sec.gov/news/studies/2010/marketevents-report.pdf> as of May 21, 2012.

⁹⁹ Gleick, James, *Chaos: Making of a New Science*, (New York, NY: Penguin Books), 1987.

¹⁰⁰ Dalkey, Norman, and Olaf Helmer. “An Experimental Application of the DELPHI Method to the Use of Experts.” And Linstone, Harold A., Murray Turriff, and Olaf Helmar. *The Delphi Method: Techniques and Applications*

¹⁰¹ Rogers, William D., “The Principles of Force; The Force of Principles,” in *Right vs. Might: International Law and the Use of Force*, (New York, NY; Council on foreign Relations), 1991, pp. 95-108

¹⁰² This type of thinking can also be found in: Karami, Ali, “Pandemics and its Consequences for the Future of Asia,” *Imaging Asia in 2030: Trends, Scenarios, and Alternatives*, Ahey Lele and Namrata Goswami, Ed., (New Delhi, India: Academic Foundation Press) 2011, pp 153-165 and Woodward, Angela, “Biological and Chemical Terrorism,” *Imaging Asia in 2030: Trends, Scenarios, and Alternatives*, Ahey Lele and Namrata Goswami, Ed., (New Delhi, India: Academic Foundation Press) 2011, pp. 323-335

¹⁰³ “Artillery” *Brassey’s Encyclopedia of Land Forces and Warfare*, (Washington DC: Brassey’s) 1996, p. 99

¹⁰⁴ Today, this is considered a subset of “Information Superiority” as one of the Air Force’s six distinctive capabilities. “Air Force Home Page” available at <http://www.af.mil/main/welcome.asp> as of May 22, 2012.

¹⁰⁵ Clausewitz, Carl von, *On War*, Michael Howard and Peter Paret, ed., (Princeton, NJ: Princeton University Press), 1989, pp. 117-121

¹⁰⁶ “Wayback Machine,” available at: <http://archive.org/web/web.php> as of April 24, 2012

¹⁰⁷ GoogleGuide: Cached Pages, available at: http://www.googleguide.com/cached_pages.html as of April 24, 2012

¹⁰⁸ Microsoft’s “Photosynth” is one such program that can enable this fusing, and it is free of charge on the internet. See: “Photosynth – Capture Your World in 3-D” at <http://photosynth.net> as of May 22, 2012.

¹⁰⁹ “Internet 2011 in Numbers” available at: <http://royal.pingdom.com.2012/01/17/internet-2011-in-numbers/> available as of May 22, 2012. The numbers for 2011 were, in most cases, several fold higher than the numbers for 2010.

¹¹⁰ Among the leaders in the development of this software is Singapore. See: RAHS Programme Office, “Our Processes Website” available at: <http://app.rahs.gov.sg/public/www/content.aspx?sid=2954> as of April 24, 2012, and

RAHS Programme Office, “Organisation Structure Website” available at <http://app.rahs.gov.sg/public/www/home.aspx> as of April 24, 2012.

¹¹¹ “Sensors Directorate” home page. Published by the Air Force Research Laboratory and available at <http://www.wpafb.af.mil/afrl/ry/> as of May 22, 2012.

¹¹² Picture was discovered on the Internet using Google’s GeoEye in early 2010. The aircraft were still based at Al Udeid when the picture was found.

¹¹³ Pape, *Bombing to Win*, pp. 1-34

¹¹⁴ Schwartz, Norton A., “CSAF Vector Statement,” July 4, 2010, available at: <http://www.afa.org/grl/pdfs/CSAFVECTOR2010b.pdf> as of May 24, 2012.

¹¹⁵ To protect transformers and generators from the electric currents generated inside power lines by a solar flare, one need only disconnect them from the grid. This need not even be done elegantly. Power companies almost always have spare line; they almost never have spare transformers or generators, thus even quickly achieved and sloppy cuts to the lines can be repaired later.