STATE ACTOR THREATS IN 2025

Joel J. Luker, Maj, U.S. Air Force

April 2007

Blue Horizons Paper
Center for Strategy and Technology
Air War College

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **APR 2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **State Actor Threats in 2025**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Center for Strategy and Technology,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**162**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US 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.

Abstract

To evaluate properly the utility of a proposed technology, especially one developed for military purposes, one must also understand the context in which the developer will employ that technology. This is because the enemy is always trying to counter one's capabilities and render them ineffective. In addition, the military never operates freely – certain political considerations always govern (and restrain) the use of military force. As a result, when trying to determine the technologies in which the USAF should invest, the context in which they will be employed becomes paramount.

To that end, the paper develops four scenarios surrounding state actor threats in the year 2025. The *Wishful Thinking* scenario describes a state whose military is materials-based and fights the US military in a large-scale, force-on-force conflict. The *Information Immobilization* adversary will also attempt to fight the US on the regular battlefield, but will do so using information-based systems to counter USAF capabilities. The *David and Goliath* scenario postulates a threat where a materials-based military attempts to fight the US using irregular tactics. And, finally, *The Phantom Menace* state is one whose information-based forces will take on the US in an irregular manner.

The analysis indicated *The Phantom Menace* provides the highest potential for a state actor to inflict catastrophic damage to the US. However, experience has shown that, to be prepared properly for any future contingency, the USAF cannot focus its acquisition efforts solely on meeting the requirements of any one or two scenarios; the best return on investment will come from developing capabilities that provide an advantage across the entire threat spectrum.

Contents

State Actor Threats in 2025

Introduction

To evaluate properly the utility of a proposed technology, especially one developed for military purposes, one must also understand the context in which the developer will employ that technology. The recent trend in military circles is to accomplish requirements planning using the same methods as those employed effectively by large corporations; specifically, to determine areas in which it must invest, the United States (US) military has shifted its focus from "threat-based" to "capabilities-based" planning methods.[1] The goal is to develop systems that provide a "tool set" from which military planners can then pull to apply given capabilities to handle various situations. However, there is one key drawback to using this approach when planning for future weapon systems: unlike the case in the business world, when the military attempts to apply its "tool set" of capabilities, the enemy gets a vote.

In any conflict, the enemy is actively trying to oppose an actor's ability to accomplish its objectives; each side will attempt to counteract the capabilities available to the other. Thus, it is not enough to say "We want to be able to do *X*," and develop a set of technologies that appear to enable the desired capability. That "*X*" needs to be placed into context, to see how the enemy may oppose one's ability to accomplish "*X*." For instance, in the years between World War I and World War II (WWII), the US Army Air Corps (AAC) developed and adopted the theory of strategic bombardment. The AAC based the theory, in part, on the assumption that bombers could always "get through" to the target, as would have been the case based upon mid-1920's technology. However, the development of radar and advances in fighter aircraft led to improvements in German air defenses; the result was the high combat loss rates experienced by Allied bombers in WWII.[2] The context had changed from the one the AAC assumed during bomber development, reducing the weapon system's effectiveness. This cycle of cat-and-mouse, developing and countering capabilities, is always present in warfare. As stated by Ben Rich, former director of Lockheed's infamous Skunk Works and the developer of the F-117A Stealth fighter,

> …[T]here are always counters to every new technology. Currently, the French and Germans are trying to create a missile that can shoot down our stealth fighter. It might well take them twenty years to succeed, but ultimately they will find a way. And then we will find a way to counter their way, and on and on – without an end.[3]

Thus, to determine the technologies in which the USAF should invest to develop a certain set of capabilities, one must also look at the potential future situation: what the enemies may look like, how they may act/react, and what capabilities they may possess. In short, context is paramount.

To that end, the Blue Horizons (BH) research team used futures research scenario planning methods to develop descriptions of the threats against which the US Air Force (USAF) may have to employ airpower in the year 2025.[4] The output of the scenario planning effort was eight plausible scenarios that illustrated these threats (this paper developed four of the eight scenarios – those involving state actors[5]). Although the scenario planning focused on what the future threat may look like, the method used differed somewhat from traditional threat-based planning. The emphasis was not on *who* the threat may be, but on what capabilities the threat may possess and how it might employ those capabilities. The scenarios thus provided a contextual foundation for the remaining BH research program, which recommended technologies and capabilities in which the USAF should invest.

When designing this investment strategy, the USAF must ensure the capabilities it develops address the entire threat spectrum. "When 'a military gives excessive focus on dealing with a certain specified type of enemy,' this can possibly result in their being attacked and defeated by another enemy outside their field of vision."[6] Thus, technologies which show promise to be applicable in multiple scenarios will provide the best return on investment.[7]

Background

Scenario Development Method

When attempting to characterize a future threat's capabilities, one must first answer the basic "who, what, why, where, when and how" questions that describe that threat. Traditional planning begins with the "who" and the "why" – who might we fight, and what would drive us into that fight? – and works from there. However, as mentioned above, this may lead to a set of tailored capabilities that are only effective against that one threat. So, for the current effort, the BH team intentionally ignored the specific "who" – which also then let them ignore the "why" – and instead classified the potential threats as one of two main groups: state or non-state actors.

Once they had broadly categorized the "who," the BH team then developed a matrix of potential "drivers" that described various characteristics of the actors and attempted to address the remaining "where," "how," and "with what" questions (the "when" in this case was a given – the focus year of 2025). The authors then made a number of assumptions to compress the matrix down into a manageable number of scenarios (see Appendices A and B).[8] In the case of a state actor, the two main drivers were material- or information-based forces fighting in a regular or irregular manner. Putting these drivers into a 2x2 matrix resulted in four state actor-based scenarios, titled "*Wishful Thinking*," "*David and Goliath*," "*Information Immobilization*" and "*The Phantom Menace*." Figure A-3 in Appendix A shows the location of each scenario in the overall threat space.

The authors developed these scenarios using a combination of classical scenario-planning methods, capabilities-based planning and Center of Gravity (COG) analyses. The output was a description of the capabilities a threat may possess in 2025 and how it might employ those capabilities. Appendix A describes the entire process in detail. Analysis of the scenarios also provided insights for future USAF investments; Appendix D discusses these implications.

Comparison to 2006 Quadrennial Defense Review (QDR)

To ensure the scenarios bounded the threat space as defined in the 2006 Quadrennial Defense Review (QDR), the authors assessed each scenario in terms of its relevance to each of the QDR's four "priority areas:" Traditional, Irregular, Catastrophic and Disruptive Challenges.[9] Appendix C, Figures C-1 and C-2, graphically depict how the scenarios provided coverage for the QDR priority areas. The authors also compared the scenarios to the three objective areas identified in the QDR; Appendix C, Table C-1 summarizes how the scenarios addressed these objectives of Homeland Defense, the War on Terror/Irregular (Asymmetric) Warfare and Conventional Campaigns.[10] The comparisons described above indicated that the scenarios did provide adequate coverage to bound the threats highlighted in the QDR.

General Discussion on State Actor Scenarios

What Makes Up a Capability?

Before discussing the capabilities possessed by an actor, one must first understand the three basics required to create a given capability: materiel/equipment (something to employ); strategy, doctrine and tactics (methods for employing it); and skills (i.e., proficiency in implementing the method).[11] Expressed mathematically,

$$\text{Capability} = \text{Equipment} \times \text{Methods} \times \text{Skills} \qquad \text{(Eq. 1)}$$

This relationship is evident in other militaries' attempts to catch up to the US military's current superiority: "…some farsighted countries… are instead putting more emphasis on raising the quality of military personnel [*skills*], increasing the amount of high technology and mid-level technology in weaponry [*equipment*], and updating military thought and warfighting theory [*methods*]" (clarifications/emphasis added).[12]

Producing an effective capability requires all three components to be present;[13] however, the components are not weighted equally. The methods of employment often play the largest factor.[14] History is ripe with examples of a "less-capable" military defeating a more-powerful one through application of superior strategy.[15] While methods are generally the most important, the relative importance of equipment vis-à-vis training will vary from one scenario to the next. As discussed below, the equipment tends to play a larger role than the training for a materials-based military, while the opposite is true for an information-based force.

Material vs Information-Based Capabilities

States which may pose a threat to US interests in 2025 will have either industrial-age or information-age economies. The economy provides the backbone for the military's equipment and skills, and thus it drives the answer to the "with what will they fight?" question posed above.

Those states with industrial-age economies will field "material-based" forces. That is, these states will be able to produce (or import and then maintain) large amounts of tanks, aircraft, ships, etc. – reflective of products commonly produced in an industrial-age society. The hardware available to the material-based adversary will be the primary driver that determines the capabilities it possesses. A material-based state's military will augment its hardware with some computerized systems and associated technical skills, but these skills will be limited to computer system operation.

In contrast, the states with information-age economies will be able to design, develop and sustain state-of-the-art computer hardware, software and associated network technologies. These states' militaries will use advanced data collection and processing techniques, including artificial intelligence (AI), to exploit rapidly situations on the battlefield. The technical/computer skills possessed by the information-based state's military (as opposed to the hardware it operates) will primarily drive its capabilities. This is not to say that the hardware will be unimportant – advanced computer processors and network systems will play a large part in the state's military capabilities – but the information-based military will achieve the bulk of its advantage because of its computer system design and programming capabilities. Thus, information-based adversaries also boast the largest potential to commit a cyberattack.

In reality, all state actors will possess a mix of industrial-age and information-age capabilities. However, for purposes of scenario development, the author treated the states on an "either-or" basis to simplify the analysis and bound the threat space. The assumption was that, if the USAF develops capabilities to handle each end of the scale, it should be able to handle the full spectrum as well. However, planners must take care to realize that the center of the scale, where an enemy may apply a combination of material- and information-based capabilities in a synergistic fashion, could present the "most dangerous" region of the threat space (see Appendix D for further discussion).

Regular vs Irregular Warfare

The authors answered the question of "how will an adversary fight?" using two broad categories of conflict: regular and irregular warfare. For purposes of this analysis, the authors defined "regular" warfare as conventional, force-on-force conflict – what some called "Big War."[16] "Irregular" warfare included everything else: guerrilla/insurgency-style tactics, terrorist or special forces-type attacks, cyber attacks against non-military targets, information warfare, etc. Specific details of how an adversary would apply these tactics varied from scenario to scenario; the main scenario descriptions include these specific details.

As in the case of material or information-based capabilities, any state may actually blur the lines between fighting using solely “regular” or “irregular” tactics; that is, a state may use both types of tactics in any single campaign. However, for simplification the analysis again examined the extremes in an attempt to bound the overall threat space.

Scenario 1. Wishful Thinking: Regular Warfare Against a Materials-Based Adversary

Scenario Overview: What Does The Adversary Look Like?

The author named this threat scenario *Wishful Thinking* for two reasons. First, it represented a classic World War II-style “force-on-force” battle between nation states – the type of battle many analysts believe the US military prefers to plan, train and equip itself to fight.[17] After finally settling the situation in Iraq and waging 20+ years fighting the Global War on Terror (GWOT), which will be primarily a limited war, the US military will long for a return to its “glory days” of the perfect, relatively easy, rapidly-executed “Big War.” Second, the adversary in the *Wishful Thinking* scenario will believe they will be able to survive (or even win) a force-on-force battle with the US military. Building a force that could challenge US superiority would require large numbers of assets with vastly improved capabilities. Developing such a force would leave a trail that *should* be visible to intelligence assets. Therefore, if US military and political leaders are not asleep at the wheel, they should be able to plan for and counter the adversary’s improved capabilities. Thus, the adversary’s belief that it could “catch up” to the US military will be an unrealized pipe dream. Even so, its belief that it might be able to challenge the US military dictates the need to plan for the threat a *Wishful Thinking* state might one day pose.

The *Wishful Thinking* threat is a state whose economy is primarily based on heavy industry. As a result, its military is dependent on having a lot of “stuff” – physical weapon systems such as tanks, airplanes and ships. It will try to affect the US military using primarily kinetic effects (physical damage to US military hardware). The *Wishful Thinking* state's military possesses modern or semi-modern weapon systems; a strong defense industrial base supports the development and sustainment of these weapons systems. This strong internal defense industry means the *Wishful Thinking* state is at least semi-independent in terms of resupplying its military in the event of a drawn-out conflict. It is not dependent on other states to resupply it with arms; in fact, it is an arms supplier to others. These arms will push the state of the art.

Because its industrial output is sufficient to meet its own defense needs, the *Wishful Thinking* state will be able to invest a significant portion of its military funding into research and development (R&D). This R&D would expand the boundaries in terms of physics, genetics, robotics, nanotechnology, etc. and then apply these advances to new weapon system designs. Thus, the *Wishful Thinking* state has the highest potential for developing a breakthrough, disruptive, <u>materials-based</u> technology. The state's defense industries would then develop these technologies into military-relevant capabilities, guided by their strategic aims and analyses of the US military's Centers of Gravity (COGs) and perceived vulnerabilities.

Objectives, COG Analysis and Enemy Capabilities

The *Wishful Thinking* state will attempt to defeat the US by destroying the US military and breaking the will of the US population. These two objectives are also inter-related: because the *Wishful Thinking* state does not have the power projection capabilities to launch a conventional attack against the US and directly impact the US population (see Appendix B), it will attempt to inflict as many casualties on the US military as possible to turn US public opinion against the conflict. To achieve these strategic objectives, the *Wishful Thinking* adversary will focus its efforts on attacking three Centers of Gravity for USAF operations: US space power, airpower and airmen (USAF personnel).

US space power will be the primary target for a *Wishful Thinking* adversary. The US's space-based systems provide the bulk of its asymmetric military advantages; therefore, any adversary who seriously wishes to challenge the US must neutralize this capability: "it is certain that in a conflict with American forces, any enemy would like to destroy or disable U.S. satellites, so as to deny those forces one of the greatest advantages they enjoy today against other military groups."[18] In addition, existing satellites will be vulnerable to several forms of attack by 2025. The *Wishful Thinking* COG analysis, along with the associated probability and risk determination (see Appendix I[19]), showed the most likely lines of operation for attacking US space power to be the use of kinetic weapons to attack and physically damage satellites, using micro-satellites (microsats) to interfere with satellite operations, and using directed energy (DE) weapons to blind or damage satellite components.

Kinetic anti-satellite (ASAT) weapons could either be terrestrial-based (including air-launched missiles, since the aircraft are ground-based) or space-based. The US, Soviet Union and China have all demonstrated terrestrial-based ASAT weapons, so this technology is already proven, at least for attacking low-earth-orbit satellites.[20] By 2025 the *Wishful Thinking* state could improve the technology to attack satellites in higher orbits as well. And if using a ground-based kinetic weapon against high-orbit satellites proves too difficult, a space-based interceptor would be a feasible alternative.

A space-based kinetic interceptor would basically consist of a satellite that attacks another one. The attack could occur in a number of ways: by ramming the target satellite; by intercepting the target and then detonating an explosive charge to kill it; or by attaching the attacking satellite to the target, thereby changing the target's mass and affecting its ability to operate properly.[21] A more-difficult, yet possible, option would be to surround the target satellite with obstacles (such as microsats) that block the target satellite's sensors, transmitters and receivers, disrupting its performance.[22]

While the above concepts may require some work to become operational, the barriers are manageable. The National Aeronautics and Space Administration (NASA) has already proven the ability for a satellite to autonomously intercept another orbital body,[23] paving the way for an attacking satellite to autonomously intercept its target. And there are no treaties or other policy issues hampering space-based ASAT systems. All of these actions are legal under the 1967 Outer Space Treaty, the only treaty governing the weaponization of outer space.[24] The main drawback to using a kinetic ASAT capability is that the US might be able to track the interceptors; knowing where they originated provides a target against which the US could retaliate. However, microsats (which are difficult to track due to their small size[25]) may nullify this retaliatory capability and remove the main barrier to kinetic ASAT employment.

In addition to its kinetic ASAT systems, the *Wishful Thinking* adversary will also use DE weapons to blind satellite sensors and attack the satellites as a whole. There are a number of types of DE weapons that could disrupt or destroy a satellite's functionality, including lasers, high-powered microwaves (HPM) and Electromagnetic Pulse (EMP) weapons. China recently demonstrated a developmental capability to blind a satellite's sensors using lasers.[26] HPM and EMP weapons go beyond simply blinding the satellite, and provide the ability to "fry" the target satellite's internal circuitry. Another advantage of DE systems is that they can be ground-based and avoid any repercussions associated with "weaponizing" space.

In addition to attacking the US's space assets, the *Wishful Thinking* state will develop an advanced Integrated Air Defense System (IADS) to prevent the US from attaining air superiority. This IADS will improve the *Wishful Thinking* state's ability to execute its "Find, Fix, Target, Track, Engage, Assess" (F^2T^2EA) "kill chain."[27] The key step will be to negate US stealth capabilities, thus improving the F^2T^2 portion of the kill chain. The *Wishful Thinking* adversary will do this using multi- or hyper-spectral sensors. Unlike radar, these sensors can "see" in a broad portion of the electromagnetic (EM) spectrum, reducing the ability of a stealth aircraft to hide.[28] The adversary will improve his engagement capability using mobile air defense batteries armed with DE weapons. This mobility will minimize the USAF's ability to employ Global-Positioning System-guided weapons against the IADS. At the same time, the DE weapons' ability to attack at the speed of light will reduce the target aircraft's ability to react to the engagement; the various types of DE weapons available would also make it difficult to develop adequate countermeasures. Taken together, the multi-spectral sensors and mobile DE air defense batteries will present a very formidable "first layer" in a tiered air defense system.

DE weapons may also provide a second layer of defense if a US aircraft does happen to get through the first. The *Wishful Thinking* state could develop an electronic "force field" to protect high-value targets. This field would nullify or prematurely detonate the electronic fuzes in any incoming weapon, and/or disrupt the incoming weapons' guidance and control systems.[29,30] The end result would be the ability to mitigate the intended effects of the US-led attack.

While blunting the US's aerial attack, the *Wishful Thinking* state will also employ its own capabilities to attack the US from the air; its primary means of doing so will be stealthy micro UAVs. The UAVs' small size and stealthy characteristics will allow them to hide from US air-superiority and air-defense sensors. While stealthy cruise missiles could also provide the *Wishful Thinking* state with an air attack capability, micro UAVs will be more cost effective.[31] The UAVs' low cost means an adversary could field more of them, "swarming" the US forces and overwhelming US defenses using sheer numbers. This fleet of enemy UAVs will negate the USAF's ability to gain and maintain air superiority; as a result, US ground forces will no longer have the luxury of freedom from airborne observation and attack, a freedom to which they have grown accustomed. Future doctrine and training must account for this eventuality.

The US military's emerging doctrine of "non-linear" battlefield operations will also increase USAF personnel's exposure to attack; [32] the *Wishful Thinking* adversary will capitalize on this exposure to increase the number of US casualties in an effort to break American will. Other states have recognized the US's aversion to taking casualties, and the corresponding link to defeating the US military:

> Ever since the Vietnam War, both the military and American society have been sensitized to human casualties during military operations, almost to the point of morbidity. Reducing casualties and achieving war objectives have become two equal weights on the American military scale. Those common American soldiers who should be on the battlefield have now become the most costly security in war, like precious china bowls that people are afraid to break. All of the opponents who have engaged in battle with the American military have probably mastered the secret of success – if you have no way of defeating this force, you should kill its rank and file soldiers.[33]

Thus, the *Wishful Thinking* state will do whatever it can to increase the US casualty count. The "intersection" of the four "GRIN" technologies (genetics, robotics, information and nano-tech[34]), and genetic manipulation in particular, will enable this strategy.

The *Wishful Thinking* state will take advantage of advances in the GRIN technologies – genetic manipulation in particular – and improve its ability to successfully employ biological weapons. Genetic manipulation will allow engineers to modify biological weapons and increase their effectiveness, even creating never-before-seen viruses that have no known antidote.[35]

Genetic manipulation may even allow the development of "targeted" bio-weapons that only affect one race of people while leaving the developer's indigenous population untouched. Engineers will also be able to create improved antibodies to allow inoculation of the *Wishful Thinking* state's own troops, reducing fears of self-contamination and eliminating one of the risks/barriers to the use of biological weapons. And, finally, engineers will increase the weapons' "robustness," enabling easier employment without damaging the payload.[36] In short, genetic manipulation will increase the likelihood of an adversary using biological weapons against US forces to inflict as many casualties as possible.

The *Wishful Thinking* state will also use DE weapons to increase the US casualty count. The large variety of capabilities inherent in DE weapons will make defending against them extremely difficult. Uses for DE weapons will range from precise, lethal strikes with lasers to wide-area denial with HPM weapons.[37] By 2025 humans will have most of the brain's functions mapped out and understood,[38] which could then lead to development of DE weapons that interfere with neural activity, creating effects ranging from immobilization to death of the target. The bottom line is that the *Wishful Thinking* state will employ DE weapons against USAF fielded forces, and the large number of possibilities inherent in DE weapon design (in terms of the broad range of the EM spectrum in which they can operate, as well as the effects they can create) makes defending against them very difficult. As a result, the US must prepare itself for the reality that a conflict against a *Wishful Thinking* state will be extremely bloody.

Scenario 2. Information Immobilization: Regular Warfare Against an Information-Based Adversary

Scenario Overview: What Does The Adversary Look Like?

The *Information Immobilization* state possesses an information-age economy and has experience designing and developing state-of-the-art computer hardware, software and networking systems. Net-centric businesses that trade goods and services (i.e., e-commerce) provide the foundation for the state's economy. As a result, the *Information Immobilization* state possesses a large educated workforce from which it can leverage computer and networking skills. The *Information Immobilization* state's military will put these skills to use and augment its fielded forces with improved computer data processing, networked datalinks and offensive computer network operations (CNO).

While the *Information Immobilization* state's economy is currently in the information age, it most likely evolved there from the industrial age. As a result, it will have at least a modicum of a defense industry that produces military hardware. Similar to the *Wishful Thinking* state, this defense industrial base is necessary to support the *Information Immobilization* state's attempt to fight the US in a "regular" manner. However, unlike the *Wishful Thinking* state, the *Information Immobilization* state will "upgrade" its military hardware with advanced computers, networks and data processing capabilities to achieve "decision superiority."

"Decision superiority" is the ability to make timely, accurate and effective decisions quicker than one's adversary;[39] essentially, it means quicker and better execution of the "Observe-Orient-Decide-Act (OODA) Loop."[40] The *Information Immobilization* state will use datalinks and sensor fusion to "orient" itself better and improve its situational awareness.[41,42] It will also use AI software to analyze the situation; AI's ability to process rapidly huge amounts of data while examining the effects of numerous variables will lead to faster, "smarter" decisions – i.e., decision superiority. The *Information Immobilization* state will then act on these decisions, apply its CNO expertise, and create an asymmetric advantage on the battlefield.

The CNO capabilities available to the *Information Immobilization* state will drastically reduce the information advantage currently enjoyed by the US military, and may in fact tip the balance in favor of the adversary. Before it engages US fielded forces on the battlefield, the *Information Immobilization* state will conduct cyberattacks to disrupt, deny, degrade and/or destroy the US military's information systems. Data streams into command centers and between units operating on the battlefield will either cease entirely, or become suspect to the point where the US military troops can no longer trust the information they see on their displays. For an entire generation of US military officers raised in an era where the "Fog of War" was more akin to a light mist, the result will be a form of decision paralysis, or *Information Immobilization*.

Objectives, COG Analysis and Enemy Capabilities

Similar to the *Wishful Thinking* adversary, the *Information Immobilization* enemy will attempt to neutralize US space and air power; however, it will do so using its information-based capabilities. At the operational level, the *Information Immobilization* state will conduct net-centric warfare against US military targets to reduce the US's information dominance, attacking logistics and communications to disrupt US military operations, and striking support systems (finance, travel, campaign etc.) to distract US military personnel so they cannot remain 100% focused on the planning and conduct of combat ops. Appendix J provides additional details for the *Information Immobilization* objectives and COG analysis.

To attain its objectives, the *Information Immobilization* state will begin by conducting cyberattacks on US military computer systems. Defensively, it will use advanced AI and networked systems to improve air defenses and increase its operational tempo. Together, these offensive and defensive capabilities will increase US casualties, ultimately subverting the US population's will to continue the fight. The *Information Immobilization* state will supplement this subversive effort with a massive information/disinformation campaign designed to reduce US and international popular support for the US-led military action.

Offensively, the *Information Immobilization* adversary will attempt to deny, disrupt, degrade or destroy various US military computer systems. To be effective in doing so, any actions it takes in the cyber domain must have a visible effect in the physical domain: disabling military hardware, disrupting leadership decision capability, etc.[43] The most probable types of assaults are Denial of Service (DOS) attacks and monitoring, disrupting, controlling or spoofing US networked military systems.

A DOS attack is the easiest to execute, but its resulting effects are difficult to predict. Conducting a DOS attack is the easiest because it does not require direct access to the target computer system. For instance, the *Information Immobilization* state could create a virus and distribute it via email. As the virus copies itself and spreads throughout the network, the number of copies (and resulting network traffic) grows exponentially. For instance, one virus "went from nonexistent to nationwide in an hour, lasted for days, and attacked 86,000 computers."[44] Another infected over 500,000 machines within a week.[45] As it spreads, the virus uses up incredible amounts of bandwidth, slowing other network traffic. To slow the virus' spread, system users may need to quarantine (take offline) both infected and non-infected computers. This essentially shuts down the target system. The only problem with a DOS attack is that it is difficult to predict its effects: there is no way to know how fast the virus will spread and what computer systems it will infect.

In contrast to the DOS attack, the other four types of actions (monitoring, disrupting, controlling or spoofing) are more difficult to enact, but produce focused and more-predictable results. These types of attacks are more difficult because they first require the attacker to gain access to the target computer network. Once "inside" the network's security, the attacker can wreak havoc. He can simply monitor what's going on (intelligence collection), or he can disrupt the system by uploading a virus or other destructive code that causes the system to shut down or perform incorrectly. He could also take control of portions of the system, using the existing software and interfaces as if he were sitting at the target computer – for instance, calling up a satellite's existing ground control software and entering new tasking information. Finally, the attacker could upload code that alters the existing software packages to spoof them – make the software programs display inaccurate data even though they appear to be working correctly.

The *Information Immobilization* state would employ all the above methods to degrade US military capabilities, beginning with US space assets. It would gain access to US satellite ground control systems and monitor the various types of communications and Intelligence, Surveillance and Reconnaissance (ISR) data flowing over the network; this will allow the adversary to see what the US sees, reducing the US's space-based ISR advantage. The *Information Immobilization* state would disrupt US satellite operations by uploading computer viruses and/or malicious code that impact the satellite's operations, or it could upload maneuvering instructions that reposition the satellite into an unusable position/orbit (in the extreme, if the satellite has enough maneuvering fuel, it could even initiate a de-orbit burn and cause the satellite to burn up on re-entry into the atmosphere). The *Information Immobilization* state could even go so far as to spoof the data transmitted on the satellites' datalinks, injecting false targets or randomly swapping the enemy/friendly data to create high rates of US fratricide.[46,47]

The *Information Immobilization* state would take similar offensive actions to disrupt US airpower. It would attempt to disrupt or gain control of US UAVs by attacking the UAVs' control systems. It would corrupt data passed over aircraft datalinks to make the data become suspect/untrustworthy. Its network attacks would jam communications links by filling the bandwidth with "garbage" data packet transmissions. Finally, the *Information Immobilization* enemy would attack the US-led coalition's Combined Air Operations Center (CAOC) computer systems to disrupt the CAOC's prosecution of the war.

In addition to attacking the "front line" combat systems, the *Information Immobilization* state's network attacks would also target "rear area" support systems. It would launch a DOS attack to disrupt email systems and other general network traffic. A separate attack would corrupt Department of Defense (DoD) personnel and finance systems to "distract" the military operators and keep them from applying 100% of their focus to prosecuting combat operations. The *Information Immobilization* adversary would impact those combat operations directly by attacking the DoD travel and deployment systems to interfere with troop movement timelines, schedules and plans. Similarly, it will attack and disrupt the US's logistics system, up to and including networks owned and operated by the US defense industry. The US's "Just In Time" logistics system will collapse, and re-supplying US fielded forces will become a nightmare. To make matters worse, as the troops begin to run out of ammunition and supplies, and the casualties begin to mount, the US will find that the *Information Immobilization* state has hacked into and corrupted US military medical and dental records, making it difficult, if not impossible, to administer the required medical care to wounded soldiers.

It is obvious that there are a large number of methods the *Information Immobilization* state could use to attack the US's networked systems; however, the effects generated by these methods are ultimately one and the same: as a result of these network attacks, the US military will have to operate in an information vacuum. The US will find its computer-based/networked information and combat systems (in the case of UAVs) in one of two states: either knocked offline, or corrupted to the point where military personnel cannot trust the data displayed on or retrieved from the system. As mentioned above, for a generation of leaders raised in an era of information overload, the result will be decision paralysis.

In addition to this wide array of offensive actions, the *Information Immobilization* state will also employ its computer hardware and networking skills to improve its air defenses. It will use onboard and network-based sensor fusion to counter the USAF's stealth technology. Onboard sensor fusion would be similar to the techniques currently employed in one USAF F-22 aircraft. In this case, the various sensors that reside on a single platform submit their data to a single central processor that also resides on that platform; the processor then merges the data before displaying the results to the operator.[48] In contrast, networked data fusion would entail using geographically-separated sensors located on independent systems. These sensors would transmit their data over a network to a single central processing location that fuses the data.[49] This effectively creates a hyper-spectral sensor, but it also has another advantage: the networked system allows one radar in an IADS to receive the "ping" sent out from another radar, reducing the radar scattering capabilities of stealth aircraft.[50,51] Advanced computer processors and AI systems will provide the data collection and processing capabilities necessary to make this networked IADS function;[52] and ad-hoc computer networks will ensure the system remains operational despite USAF attempts to destroy its "control nodes."

The *Information Immobilization* enemy will use ad-hoc computer networking and advanced AI to create a "self-healing" IADS system.[53] In previous conflicts such as the Gulf War or 2003 Iraq War, the USAF used a "system analysis" approach to defeat the Iraqi IADS. It destroyed specific "nodes" in the system that, in turn, caused larger portions of the IADS to become ineffectual. For instance, destroying a sector operations center (SOC) could render the IADS in that entire sector moot: "blind the enemy air defense system, and isolate the elements from the brain, and it is no longer a 'system' but individual weapons operating in the dark."[54] However, in the *Information Immobilization* IADS, if the US destroyed a SOC, the IADS' AI systems would recognize that the SOC was no longer functioning; the AI systems would then use the ad-hoc network to transparently re-route the data that flowed to and from the destroyed SOC to an alternate command center. Because the AI systems at the second location are identical to those in the first, there would be no degradation in performance similar to that which would occur if the decision-making responsibility was passed from one person to another with less experience. To the attacker, such an IADS would appear to be "self healing." The *Information Immobilization* state's use of AI is the key that enables this seamless continuity of operations.

The *Information Immobilization* state will also use its AI systems to supplement the decisions made by its military and political leaders, resulting in decision superiority. AI systems will predict US actions and present possible courses of action (COA) to the *Information Immobilization* military commander(s), with an accompanied recommendation for the preferred COA. The human will still be kept in the decision loop, but the AI system will perform the data processing that shapes the human's decisions.[55] By 2025, AI systems will be able to process data at a near-human level, but at a higher "accuracy" rate due to their ability to store, without "forgetting" or "neglecting," large numbers of input variables.[56] As a result, the *Information Immobilization* enemy will be able to make decisions rapidly and more accurately, resulting in "decision superiority."

The *Information Immobilization* state will increase its decision superiority by using an information operation – and, more specifically, an influence operation (IFO) – campaign to shape US political and military decisions.[57] As pointed out by Clausewitz almost 200 years ago, "War is thus an act of force to compel our enemy to do our will."[58] Thus, to achieve victory, one must subvert the enemy's will before he is able to subvert yours. At the dawn of the 20th century, in the middle of the industrial age, airpower theorists proposed using airplanes to bypass the enemy's ground forces, inflict damage upon the adversary's "vital centers," and thus subvert his will to your own;[59] current USAF doctrine still adheres to this theory.[60] In today's information-age societies, global information networks take this concept one step further, providing the means to bypass the armed forces altogether and subvert the enemy's will without even firing a shot. However, the US has not (yet) been effective at conducting and winning IFO campaigns, especially ones directed at its own population.

The US's lack of success in internal IFO campaigns stems from three factors. First, the US Constitution's requirement for Freedom of the Press makes it very difficult to achieve any sort of unity of effort in an IFO campaign. Second, the large number of cable news networks, coupled with their worldwide, 24/7/365 coverage, causes even small events to be blown out of proportion as the networks struggle to fill their air time with anything that will get them ratings. In the press, "Bad news makes good news," so the media tend to focus on events that make it seem like the government is "failing" at whatever it attempts to do. And third, the US population historically mistrusts its own government; as a result, it generally discounts any type of centrally-initiated IFO campaign as "spin" or propaganda. The end result of the US's inability to conduct successful IFO activities is an asymmetric advantage for the *Information Immobilization* state, an advantage it will be happy to exploit.

Scenario 3. David and Goliath: Irregular Warfare Against a Materials-Based Adversary

Scenario Overview: What Does The Adversary Look Like?

The *David & Goliath (D&G)* adversary is a state whose military is materials-based, but knows it cannot defeat the US in a regular war. Such a state is most likely vying for regional prominence and/or is a smaller state who has threatened US security interests in some fashion. It is dependent on foreign military sales to acquire most of its big-ticket military hardware (tanks, airplanes, air defense systems, etc.) but still possesses a limited defense industry that can modify those weapons and/or produce “smaller” military systems. Although the *D&G* state may have enough money to purchase a large supply of military hardware, it would not be a near-peer competitor that might be able to compete with the US in a force-on-force battle. Because it cannot defeat the US in a regular conflict, the *D&G* state will turn to irregular tactics to achieve its strategic goals; during the conflict, it will trade space (ground) for time to allow those irregular tactics to achieve their desired effects.

As the *D&G* state gives up more and more ground to advancing US/coalition forces, the line between the *D&G* and *Guerrillas in the Mist (GITM)* scenarios will become blurred:[61] at what point does the state cease to exist, and its efforts become a resistance against the occupying army or an insurgency against the new government imposed by that army? To delay this transition, the *D&G* state will give up its ground as slow as possible. Before this transition does occur, and even for a period afterwards, several differences will remain between the *D&G* and *GITM* scenarios due to differences in the use of force between state and non-state actors.

Unlike a non-state actor, the *D&G* state actor will limit its application of force in order to conserve as much of its infrastructure as possible. In the case of a government that truly cares about its people, it will attempt to minimize the harm that it inflicts upon them. In the case of a totalitarian regime, it will need to keep critical components of the infrastructure functional to help restore its control over the population should the conflict terminate in such a manner that the regime remains in place.[62] In either case, if it is victorious, the *D&G* state will have to pay to rebuild any infrastructure it destroys. As a result, it will at least hesitate to strike infrastructure targets a non-state actor would not think twice about destroying.

Another difference between the *D&G* state actor and the *GITM* non-state actor is the legitimacy of the state government, and the access that legitimacy provides to other Instruments of Power (IOPs) – such as diplomacy and economics – that are not normally available to a non-state actor.[63] The *D&G* state will use these other IOPs to offset and asymmetrically counter the US's military advantages. For instance, the *D&G* state will use its recognition in international institutions like the United Nations (UN) and attempt to erode international support for the US military action; it will also attempt to degrade the coherence in any US-led coalition.[64] The D&G state will support these diplomatic efforts with an intense, worldwide IFO campaign to sway public opinion. Finally, the D&G state will position itself economically so a military attack against it would have adverse economic repercussions against the US and/or its allies.[65] In short, the *D&G* state will attempt to offset the US's military advantages using non-military IOPs. While these non-military IOPs are crucial to the D&G state's ability to attain its strategic goals, their impact on technology investment for the USAF was minimal and outside the scope of the BH effort, so the author ignored them in the COG and capability analysis detailed below.

Objectives, COG Analysis and Enemy Capabilities

The *D&G* adversary's specific strategic goals could be extremely varied; however, in the end the *D&G* state is simply trying to get the US to leave it alone so it can achieve its objectives, whatever those may be. To reduce US presence/influence in the region, the *D&G* state will erode US public and international support for the US-led military operation.

At the operational level, the *D&G* state will subvert US popular support (i.e., the will of its people) by inflicting as many casualties as possible, drawing out the conflict as long as possible while still maintaining its "statehood," and using its non-military IOPs to offset the US's military advantages. As mentioned above, it will also launch an intense IFO campaign to influence worldwide public opinion. Appendix K details the capabilities the *D&G* state will develop to reach these objectives in support of its overall strategy.

The *D&G* state's primary strategy – to pull back and draw out the fight – is common among nations attempting to fight a superior military force. The Afghani Mujahideen used this strategy in the Afghan-Soviet conflict; their goal was to "trap the Soviets in an attrition war and continue to inflict casualties until the enemy gave up and went home."[66] It was also the strategy proposed by Iraqi Generals to Saddam Hussein before the 2003 Iraq war.[67] The *D&G* state will learn from these examples and engage the US in a drawn-out, high-casualty conflict.

To increase the US casualty count, the *D&G* state will arm its population and create a general militia. The degree to which any state arms its population will vary based upon the state's "trust" of its population not to rise up against the existing government;[68] however, in the worst-case scenario, the *D&G* state will arm its entire population, all of whom will be hostile to US forces. While pulling back, the *D&G* state will leave this well-armed militia behind to surround the enemy (the US) and attack it from the rear. The US's use of swarming tactics on the non-linear/non-contiguous battlefield will exacerbate this access of enemy troops to the rear.[69] However, underlying this predicted modus operandi is the assumption that the US will have to employ ground forces into the *D&G*'s territory; thus, the *D&G* state will take actions to blunt the effects of US airpower and compel the US to employ its ground forces.

The *D&G* adversary will counter US airpower using a number of simple techniques. First, the adversary will disperse his forces to mitigate airborne firepower. Second, he will deploy them or pull back into terrain that helps offset the US's ISR capabilities (mountains, jungle, urban areas, etc.). And finally, he will deploy his forces in or near areas that would appear on a USAF no-strike list: schools, hospitals, places of worship, etc. These techniques should not be surprising; they have been the norm for adversaries operating against the US for the last decade.[70] For instance, in the Kosovo conflict, "the Serbs gave hiding from air attack their highest priority."[71] Improved ISR, low-yield precision-guided munitions and non-lethal DE weapons will help the USAF counter some of these techniques. However, "[i]t is important for the United States to remember to match a particular use of military force to its foreign policy objectives, and not depend solely on victory through airpower."[72,73] In the worst-case scenario, airpower will be unable to coerce the *D&G* adversary, and the US will have to do so using a combination of airpower and boots on the ground. As the US ground forces attack, the *D&G* adversary will pull back and draw them into the lion's den.

To implement its plan, the *D&G* state will supply its military with equipment and skills similar to those described in the *Wishful Thinking* scenario. However, because the *D&G* state is a technology consumer, its equipment may be more limited. In particular, the *D&G* state will have a minimal (if any) capability to launch satellites into space, let alone deploy space-based ASAT weapons. However, it still may be able to disrupt some US space assets using ground-based DE weapons (lasers/dazzlers) or air-launched ASAT weapons. These ASAT weapons will aid the *D&G* state's objective of slowing US/coalition operations.

To enhance its ability to achieve its other operational objective – that of driving up the US casualty count – the *D&G* state will develop and employ small, highly-lethal sidearms and anti-tank/anti-aircraft weapons. One of the factors that makes modern insurgencies increasingly effective is the development of small, cheap, man-portable systems that provide the common foot soldier the ability to counter large systems – systems that normally provide a massive firepower advantage. One person with a rocket-propelled-grenade launcher can destroy a tank or armored personnel carrier.[74] A stinger missile, portable anti-aircraft artillery or other ground fire can take down a multi-million dollar aircraft.[75] Armor-piercing ammunition offsets the advantages normally associated with body armor worn by military troops.[76] These trends will continue, with the development of new, high-yield explosives that provide more killing power per ounce, and, like all technologies, the cost will continue to decrease over time.[77] As a result, the *D&G* state will be able to equip a large militia with extremely deadly weapons.

In addition to arming its militia, the D&G state will also develop and leave behind other surprises for the invading US military. It could disperse nanobots designed to target and "eat" or interfere with US military equipment.[78] Or it could spread a genetically-manipulated virus designed to be ineffective against its own ethnic population (either at the genetic level, or through a prior inoculation program), but yet kill soldiers in the invading army. The possibilities are numerous, but the effects will be similar to deploying a minefield in front of an advancing army: the attacker's casualty count increases while its advance slows as it tries to clear the threat. Thus, these capabilities will help the *D&G* state achieve its two primary operational objectives, of slowing the US advance while inflicting massive casualties. And, when the enemy achieves his objectives at your expense, you would normally call that – in military jargon – defeat.

Scenario 4. The Phantom Menace: Irregular Warfare Against an Information-Based Adversary

Scenario Overview: What Does The Adversary Look Like?

The Phantom Menace is a state whose capabilities are primarily information-based and chooses to fight the US in an irregular manner. Its offensive cyberattack capabilities are similar to those possessed by the *Information Immobilization* state, but it is focused on attacking a different target set. Unlike the *Information Immobilization* state, *The Phantom Menace* does not possess a military capable of fighting the US in a "regular" battle, even when aided by advanced data processing and AI software. As a result, instead of limiting its attacks to US military-related systems, *The Phantom Menace* will expand its attacks to include US economic and infrastructure targets that are vulnerable to a cyberattack. Thus, *The Phantom Menace's* target set will be similar to that attacked by the *Cyber 9/11* non-state actor: US infrastructure and institutions.[79,80] However, just as in the *D&G* vs. *GITM* situation described above, disparities between state and non-state actors drive several key differences between the *Cyber 9/11* adversary and *The Phantom Menace*.[81]

The first difference between *The Phantom Menace* and the *Cyber 9/11* adversary is synchronization of multiple attacks.[82] The *Cyber 9/11* adversary will primarily consist of small non-state actor cells that operate independently from one another; the result is an attack here, a strike there, with time to recover in between the sporadic incidents. In contrast, when *The Phantom Menace* attacks, it will do so in a massive, coordinated fashion to create synergy between the various assaults and minimize the US's ability to recover from one strike before the next one occurs. For instance,

> If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means in gradual stages until the enemy is forced to sign a dishonorable peace treaty.[83]

The result will be a massive collapse of the US economy and disruption to key infrastructure, leading to the US's inability to focus on power projection/overseas military operations.[84] To ensure the US does not have a target against which it *can* focus its military efforts, *The Phantom Menace* state must remain hidden.

The Phantom Menace derives its name from its ability to remain anonymous; its attacks will occur in an untraceable manner (mainly through cyberspace), or at least using methods meant to obscure its true identity. "Stealth and surprise are extremely important."[85] Operating from the shadows in this manner causes a conundrum for the state being attacked:

> The problem is, how does one know for certain which damage is the result of games and which damage is the result of warfare? Which acts are individual acts by citizens and which acts represent hostile actions by non-professional warriors, or perhaps even organized hacker warfare launched by a state?[86]

In addition, "[t]he speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs after the fact, if at all."[87] Maintaining anonymity is crucial for a state actor who wishes to inflict overwhelming damage on the US but who cannot directly counter the US military, because without truly knowing who is attacking it, the US will not be able to retaliate in kind.[88] Thus, *The Phantom Menace's* ability to operate in the shadows will neutralize the US's nuclear triad and vast conventional military arsenal. As a result, *The Phantom Menace* provides the highest potential for a state actor to inflict a catastrophic attack against the US (see Appendix C, Figure C-2).

Objectives, COG Analysis and Enemy Capabilities

As described above, *The Phantom Menace* state's primary objective will be to attack the US, but at the same time remain hidden and reduce the threat of a US nuclear or military counterattack. In short, it will execute "a well-arranged team effort and combined attack to achieve surprise, secrecy and effectiveness. A single full-depth, synchronized action… may be enough to decide the outcome of an entire war."[89] As mentioned above, the primary targets will be US infrastructure and institutions, in an attempt to create chaos within the US mainland. This chaos will then, in turn, hamper the US's ability to project its power (military and otherwise) overseas, allowing *The Phantom Menace* to achieve its (other) strategic objectives, whatever they may be. Appendix L provides additional details on *The Phantom Menace's* strategic and operational objectives, as well as the associated capability analysis.

The Phantom Menace's primary capabilities can be summed up in one word: cyberattacks. The target set of these attacks is extremely varied, and *The Phantom Menace's* methods will differ with each type of computer system it attacks. However, an analysis of the proposed lines of operation revealed a simple recurring theme: the need to protect non-USAF computer systems (including civilian as well as other government agencies) from cyberattack. Appendix D discusses the associated implications for the USAF in its new role as DoD's lead for cyber war.

In addition to conducting coordinated cyberattacks against US infrastructure and institutions, *The Phantom Menace* will also employ advanced IFO capabilities against the US (and worldwide) population. This IFO campaign will have two objectives: first, to reduce the trust of the US population in the media and US leadership; and second, to hamper the US's attempts to put the pieces together and figure out who is conducting the attack. To achieve its objectives, *The Phantom Menace* will use advanced, Hollywood-style computer graphics (CG) programs to create false video footage and the associated news stories. At the rate CG technology is progressing, by 2025 such fabricated footage would be nearly inextinguishable from reality.[90] The *TPM* state would surreptitiously release bogus footage that shows US leaders saying things they never really did; video "documentation" of US troops committing war crimes, etc. It could get the US media to "glom on" to a totally fake story, then later reveal the story to be false, to discredit the media and reduce the public's trust in media broadcasts.[91] Or *The Phantom Menace* could divert attention from itself by creating "evidence" implicating a different actor for the ongoing attacks. The result will be an inability of the US government to gain popular, let alone international, support for a reprisal against *The Phantom Menace* state.

Conclusion

The USAF must continue to invest in technology development to maintain its dominance in the year 2025. This is a daunting task in an era of rapid technological change. To make matters worse, the USAF cannot simply forecast what technologies may be available to increase its own capabilities; it must also understand the technologies available to the enemy, how the enemy plans to employ those technologies, and the skills the enemy will possess to do so. In short, because of the adversarial nature of warfare, the USAF cannot develop an effective capability without first understanding how the adversary may counter that capability. Failure to do so will result in the USAF reacting to advances in enemy capabilities, rather than getting ahead of the power curve and placing its enemies on the defensive.

That being said, the scenarios developed herein provide a basis against which the USAF can compare proposed technologies to determine the technologies' impacts in future warfare. Technologies applicable to multiple scenarios will provide a "broad-spectrum" capability and will most likely deliver the highest return on investment; ultimately, these technologies will provide a robust "tool set" from which USAF planners can pull. Simultaneously developing the skills and methods for employment that go along with these tools will allow the 2025 Air Force to shift rapidly from one mission type to another, effectively employing airpower across the full spectrum of combat operations. This ability to shift effectively between all forms of warfare will be crucial for the United States Air Force, the most lethal military force in the history of warfare, to maintain its dominance. As is often said, "Flexibility is the key to airpower."

NOTES

[1] See United States. Dept. of Defense. Secretary of Defense., *2006 Quadrennial Defense Review* (Washington, DC: 2006), 4.; United States. Dept. of the Air Force. Chief of Staff., *The U.S. Air Force Transformation Flight Plan 2004* (Washington, DC: 2004), 51-52.; United States. Dept. of the Air Force. Chief of Staff., *The Edge: 2005 Air Force Transformation* (Washington, DC: 2005), 6.; United States. Dept. of Defense. Office of Force Transformation., *Elements of Defense Transformation* (Washington, DC: Oct 2004), 3.; and United States. Dept. of the Air Force. HQ USAF/A8X., *Air Force Roadmap 2006 > 2025* (Washington, DC: 2006), 6, 13.

[2] Azriel Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield* (Dulles, Virginia: Brassey's, Inc., 2002), 70.

[3] Ben R. Rich and Leo Janos, *Skunk Works* (New York: Little, Brown and Company, 1994), 321.

[4] For discussion on how to accomplish scenario planning, see Steven Schnaars and Paschalina Ziamou, "The Essentials of Scenario Writing," *Business Horizons* 44, no. 4 (2001).; Jerome C. Glenn and The Futures Group International, "Scenarios," in *Futures Research Methodology--Version 2.0, AC/UNU Millennium Project* (Washington, DC: American Council for the United Nations University, 2003).; Diana Scearce, Katherine Fulton, and The Global Business Network Community, "Scenario Thinking in Practice," in *Leadership, Command and Professional Development; Leadership and the Staff Environment II LB Course*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2004; reprint, from *What If? The Art of Scenario Thinking for Nonprofits*, Chapter 2. Global Business Network, 2002).; and Earl C. Joseph, "Forecasting Change and Developing Futures," (Walden University, 2002).

[5] For a discussion on the non-state actor scenarios, see James "Buster" Myers, Maj., USAF, "Non-State Actor Threats in 2025" (United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007).

[6] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare," (Beijing: PLA Literature and Arts Publishing House, February 1999), 144.

[7] This does not imply the USAF should ignore technologies only applicable to one or two scenarios. If those technologies can drastically reduce the risk associated with a given scenario, they may also provide a good return on investment. But, if a technology is applicable to multiple scenarios, there is simply a higher probability of it being applicable in future conflicts.

[8] The current author uses the plural here simply because this paper will later be published along with its sister paper, being written simultaneously by Maj James “Buster” Myers (see Myers, "Non-State Actor Threats in 2025".). The current author wrote this introduction with the intent that it will later serve as an intro to all eight scenarios once the authors combine the two papers. In addition, the authors co-developed the original driver matrix and the assumptions to cull it down; as a result, Appendices A, B and C are applicable to both papers and were written jointly. The main paper and Appendix D are solely the work of the current author.

[9] United States. Dept. of Defense. Secretary of Defense., *2006 Quadrennial Defense Review*, 19.

[10] Ibid., 36.

[11] Many thanks to Majors James “Buster” Myers and Scott “Grins” Dickson for helping to flush out this line of thought.

[12] Liang and Xiangsui, "Unrestricted Warfare," 44.

[13] Note the multiplication signs in Eq. 1; if any component is zero, so is the result. Therefore, all three components are required to produce an effective capability.

NOTES (Continued)

[14] Kenneth Beebe, Maj, USAF, "The Air Force's Missing Doctrine," *Air & Space Power Journal* (Spring 2006).

[15] See, for example, Jacqueline A. Newmyer, "China's Air-Power Puzzle," *Policy Review* (June & July, 2003): 81. For other examples, reference the American Revolution, the Vietnam War, or the original Star Wars Trilogy.

[16] Colin S. Gray, "Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?," in *Inter/National Security and War, AY07 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, August 2006; reprint, from *Strategic Studies Institute (SSI) Monograph*. US Army War College, March 2006), 277.

[17] See, for example, Liang and Xiangsui, "Unrestricted Warfare," 127.; also Mark Williams, "Technology and the Future of Warfare," *Technology Review (MIT)*, 23 Mar 06, 1.; Gray, "Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?," 279.; Scott Cooper, "Air Power and the Coercive Use of Force," in *Immaculate Warfare*, ed. Stephen D. Wrage (Westport, CT: Praeger, 2003), 16-17.; and Stephen D. Wrage, "Conclusion," in *Immaculate Warfare*, ed. Stephen D. Wrage (Westport, CT: Praeger, 2003), 107.

[18] Dave Ahearn, "U.S. Military, Commercial Space Assets Vulnerable to Attack: Experts," *Defense Daily* 230, no. 58 (22 June 2006): 1.

[19] Note that the Appendix lettering skips from D to I. This is to plan for the future, when the author merges this paper with its sister paper on non-state actors. Appendices E-H detail the capability development for the four non-state actor scenarios, and are not relevant to this paper, so the author left them out for now. However, he still reserved their “space” in the appendix numbering scheme to reduce the follow-on workload when merging the two papers.

[20] The United States, China and the former Soviet Union have all demonstrated this capability. See Vago Muradian, "Pentagon Turns Attention to Chinese Space Threat," *Air Force Times* 67, no. 30 (2007).; also "Weapons Testing," *Air Force Times* 58, no. 6 (1997).; "Restructuring Plan for Anti-Satellite Program," *Aviation Week & Space Technology* 126, no. 11 (1987).; and "Space Weapons Policy," *Congressional Digest* 63, no. 3 (1984): 67.

[21] While the satellite's orbit would not change (the orbital path is independent of the satellite's mass; see Jerry Jon Sellers, *Understanding Space: An Introduction*, ed. Douglas H. Kirkpatrick, Revised 2nd ed. (Boston, MA: McGraw-Hill, 2004), 141.), changing the object's mass would affect its angular rotation and handling characteristics. As a result, the satellite may not be pointed in the direction it needs to be, and ground controllers would have trouble re-positioning the satellite.

[22] The difficulty to accomplish this, though, arises because of the need for station-keeping relative to the target satellite; a satellite between the target and the earth (blocking the target's sensors or ground-control transmitters/receivers) would have a slightly faster orbit than the target satellite (due to basic orbital mechanics; see Ibid.). However, as energy sources become smaller and with higher energy densities, such a station-keeping capability will become feasible. See Carole Rossi et al., "Solid Propellant Microthrusters on Silicon: Design, Modeling, Fabrication, and Testing," *Journal of Microelectromechanical Systems* 15, no. 6 (2006).

[23] National Aeronautics and Space Administration (NASA), "Deep Impact Kicks Off Fourth of July with Deep Space Fireworks," http://www.nasa.gov/mission_pages/deepimpact/media/deepimpact-070405-1.html.

[24] While technically legal, there are also measures in place to compensate a country if someone harms its space-based assets: “However, the Liability Convention of 1972 establishes procedures for determining the liability of a country that damages or destroys the space objects of another country, while the Registration Convention of 1976 requires the registration of objects launched into space.” See Craig Eisendrath, "Why Is the U.S. Weaponizing Outer Space?," *USA Today Magazine* 135, no. 2740 (2007): 53. However, in warfare, “to the victor go the spoils.” If another country attacks US satellites and ends up defeating the US in battle, who's going to make them pay for the damages??

NOTES (Continued)

[25] Scientists define micro satellites as satellites with masses less than 100Kg (K. Badari Narayana and V. Venkata Reddy, "Thermal Design and Performance of Hamsat," *Acta Astronautica* 60, no. 1 (2007).; and Theresa Hitchens, Michael Katz-Hyman, and Jeffrey Lewis, "U.S. Space Weapons," *Nonproliferation Review* 13, no. 1 (2006): 38.).

[26] Vago Muradian, "China Attempted to Blind U.S. Satellites with Laser " DefenseNews.com, http://www.defensenews.com/story.php?F=2121111&C=america.

[27] Adam J. Hebert, "Compressing the Kill Chain," *Air Force Magazine* 86, no. 3 (2003): 51.

[28] Jimmy Ennett, "The Impact of Emerging Technologies on Future Air Capabilities," ed. Defence Science and Technology Organisation Science Policy Division (Australian Department of Defence, 1999), 39.; and David A. Fulghum, "Sensor Mix Means No Place to Hide," *Aviation Week & Space Technology* 150, no. 3 (1999): 61.

[29] US air-to-surface weapons have begun using electronic (as opposed to mechanical) fuzes due to the increased retargeting flexibility that the electronic fuzes provide (see "Production Fuzion," *Aviation Week & Space Technology* 165, no. 12 (2006): 53.). This increased reliance on electronic fuzes correspondingly increases the ability of an enemy to develop a DE counter.

[30] Such a “force field” has already been demonstrated by troops in Iraq. They use similar technology to jam Improvised Explosive Devices (IEDs) before a convoy reaches the threat. See Michal Fiszer, "Polish Troops in Iraq Getting Counter-IED Devices," *Journal of Electronic Defense* 29, no. 3 (2006).; and Brendan P. Rivers, "US Army Seeks New System to Counter IEDs," *Journal of Electronic Defense* 28, no. 4 (2005).

[31] One JASSM, the USAF’s newest conventional low-observable cruise missile, costs over $400,000 per weapon; a disposable UAV munition would be much cheaper, most likely in the $30K - $60K range (between the cost of a Small Diameter Bomb and a Dragoneye UAV). See Lorenzo Cortes, "JASSM Costs Could Go up 100 Percent If Congressional Cuts Hold, Air Force Says," *Defense Daily*, 10 September 2003, 1.; Global Security.org, "Small Diameter Bomb / Small Smart Bomb," Global Security.org, http://www.globalsecurity.org/military/systems/munitions/sdb.htm.; and Israel Aerospace Industries LTD, "Dragon Eye Miniature UAV," http://www.defense-update.com/products/d/dragoneyes.htm.

[32] United States. Dept. of the Air Force. Secretary of the Air Force., *Air Force Doctrine Document (AFDD) 2-1.3: Counterland Operations* (Washington, DC: Dept. of the Air Force, 12 September 2006), 65-67.; and United States. Dept. of Defense. Office of Force Transformation., *Elements of Defense Transformation*, 8.

[33] Liang and Xiangsui, "Unrestricted Warfare," 93.

[34] Joel Garreau, *Radical Evolution* (New York: Doubleday, 2004), 4-8, 53-54, 115-27.; and Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York, NY: Penguin Group, Sept. 2005), Chapter 5.

[35] Joby Warrick, "Custom-Built Pathogens Raise Bioterror Fears," *The Washington Post*, 31 July 2006, A.1.

[36] One of the current limitations of biological weapons is their frailty, which makes delivering them from standoff weapons (like a mortar, bomb, etc.) extremely difficult without killing the virus/agent. See "Fear and Breathing," *Economist* 360, no. 8241 (2001).

[37] For example, the US already has a HPM system that stimulates a person’s nerve endings to make him extremely uncomfortable, to the point where he simply cannot focus on the work at hand. John P. Geis II, Lieutenant Colonel, USAF, "Directed Energy Weapons on the Battlefield: A New Vision for 2025" (Air University, April 2003).; and Air Force Research Laboratory, *Active Denial System*, United States Air Force Fact Sheet (Kirtland AFB, NM: United States Air Force, August 2006).

[38] Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*, 197.

NOTES (Continued)

[39] Dave Sloggett, "Decision Superiority in Operations Other Than War," *Jane's Defence Weekly* 42, no. 48 (2005).

[40] The OODA Loop is a model that represents the four phases involved with determining and executing a course of action (i.e., making a decision, carrying it out, and then assessing the outcome to ensure the action created the desired effect). See Paul K. Van Riper, "Information Superiority," *Marine Corps Gazette* 81, no. 6 (1997): 58-60.; and Wikipedia.com, "OODA Loop," http://en.wikipedia.org/wiki/OODA_Loop.

[41] Sensor fusion is the merging of data from a large number of sensors prior to displaying them to the operator. For instance, in the F-22 aircraft, "[s]ensor fusion occurs when targeting, detection and tracking information is fused [sic] from multiple sensors to create a single input to the pilot." Boeing, "News Release: Boeing Avionics Help Guide F-22 Missile to Its Target," http://www.boeing.com/news/releases/2001/q3/nr_010924n.htm.

[42] For a discussion on the "orientation" phase of the OODA loop and its impacts on situational awareness, see Col Michael J. Carey, "Integrating Space Capabilities in Support of the USCENTCOM Theater of War a Challenge for the DIRSPACEFOR," in *Joint Air and Space Operations, AY2007*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2006; reprint, from *High Frontier*, vol. 1, no. 4, Space Warfighting. Headquarters US Air Force Space Command.), 220.

[43] Raymond C. Parks and David P. Duggan, "Principles of Cyber-Warfare" (paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001), 123.

[44] George H. W. Bush, "The National Security Strategy to Secure Cyberspace," (Washington, DC: February, 2003), 6.

[45] Gabriel Sherman et al., "Maximum Velocity," *Popular Science*, February 2005.

[46] From the author's personal experience, inserting false targets or changing the target display information on a datalink is relatively easy to do. USAF personnel do this on a daily basis when testing various hardware and software components of the datalink.

[47] The actions of Chechen insurgents demonstrated a case of disrupting information to create fratricide. Because Chechnya was a break-away from the former Soviet Union, the insurgents possessed radios that were compatible with those used by the Russian troops, and knew the Russian tactics/radio procedures as well. The insurgents used the radios to interfere with Russian Forward Air Controllers' calls for close air support, resulting in Russian fratricide. See Maj. J. Takacs, "The Russian Air Force in Chechnya: Have Lessons Been Learnt and What Are the Future Perspectives?," in *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2007; reprint, from Royal Air Force, *Air Power Review*, vol. 4, no. 4. Director of Defense Studies, Winter 2001), 463.; and Maj Marcel de Haas, "The Use of Russian Air Power in the Second Chechen War," in *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2007; reprint, from Royal Air Force, *Air Power Review*, vol. 6, no. 1. Director of Defence Studies, Spring 2003), 482.

[48] Boeing, "News Release: Boeing Avionics Help Guide F-22 Missile to Its Target."

[49] Doug Richardson, *Stealth Warplanes* (Osceola, WI: MBI Publishing, 2001), 179-80.

[50] By controlling the angled surfaces present on a stealth vehicle, engineers minimize the amount of radar energy that "bounces back" towards the transmitting system. Instead, the radar energy bounces off in a different direction, causing it to be "invisible" to the transmitting radar system. But if a different receiver were to detect that energy, and also determine which transmitter sent the energy pulse out, the aircraft would no longer be "invisible." See Bill Sweetman, *Lockheed Stealth* (St. Paul, MN: MBI Publishing, 2001), 36-38.; and Richardson, *Stealth Warplanes*, 34,

NOTES (Continued)

36. Lockheed's "Silent Sentry" currently uses a similar technology, although it is currently only accurate enough for acquisition/early warning, and not target tracking (Richardson, *Stealth Warplanes*, 175.).

[51] David A. Fulghum, "New Radars Peel Veil from Hidden Targets," *Aviation Week & Space Technology* 150, no. 3 (1999): 58.

[52] Ibid.

[53] Ad-hoc networks are "unplanned, self-organizing networks composed of mobile nodes that utilize mesh networking principles for interconnectivity." See Brent Peacock, Maj., USAF, "Connecting the Edge: Mobile Ad-Hoc Networks (Manets) for Network-Centric Warfare" (United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007). In the case of an IADS system, if part of the network went down, the IADS would automatically re-route its information through a different path. This is the way standard internet routers currently work, but ad-hoc networking offers increased flexibility as well as the advantage of using mobile "routers" that are more difficult, if not impossible, to target kinetically.

[54] Tom Clancy and Gen (Ret.) Chuck Horner, *Every Man a Tiger* (New York, NY: Berkley Books, 1999), 341.

[55] This is essentially the case now in the F-22's cockpit due to its sensor fusion algorithms. The computer processes the data and determines what the pilot sees (it shapes the information that lead to his decisions), but the pilot still presses the pickle button to initiate an attack.

[56] Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*, 25, 200.

[57] United States. Dept. of the Air Force. Secretary of the Air Force., *Air Force Doctrine Document (AFDD) 2-5: Information Operations* (Washington, DC: Dept. of the Air Force, 11 January 2005), Chapter 2.; and United States. Joint Chiefs of Staff., "Joint Publication (JP) 3-13: Information Operations," (Department of Defense, 2006), I-10.

[58] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

[59] Alfred F. Hurley, *Billy Mitchell: Crusader for Air Power* (Bloomington, IN: Indiana University Press, 1975), 76. Also William Mitchell, *Winged Defense* (Mineola, New York: Dover Publications, Inc., 1925; reissued in 2006), 4-6.

[60] United States. Dept. of the Air Force. Secretary of the Air Force., *Air Force Doctrine Document (AFDD) 1: Air Force Basic Doctrine* (Washington, DC: Dept. of the Air Force, 17 November 2003), 40.

[61] For a description/analysis of the *Guerrillas in the Mist* scenario, see Myers, "Non-State Actor Threats in 2025".

[62] For example, see Saddam Hussein's decision not to drop the bridges across the Euphrates during the 2003 Iraq war. Michael R. Gordon and Gen (Ret.) Bernard E. Trainor, *Cobra II: The inside Story of the Invasion and Occupation of Iraq* (New York, NY: Pantheon Books, 2006), 505.

[63] Edwina Campbell and Lewis Griffith, "An Introduction to the Instruments of Power," in *Inter/National Security and War, AY07 Coursebook,* ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 19 Apr 2004), 181.

[64] Liang and Xiangsui, "Unrestricted Warfare," 63-64.

[65] Take, for example, the US's current conundrum with Iran and its nuclear development program. Any attack against Iran could disrupt world oil trade, specifically in Europe; the result is a form of protection against a US military attack. International Crisis Group, "Iran: Is There a Way out of the Nuclear Impasse?," (International Crisis Group, Middle East Report No. 51, 23 February 2006), 16.

NOTES (Continued)

[66] James S. Corum and Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists* (Lawrence, KS: University Press of Kansas, 2003), 396.

[67] This was the tactic proposed by the Iraqi General Staff prior to the 2003 Iraq War; however, due to his concerns of a general uprising, Saddam Hussein ignored their advice. Gordon and Trainor, *Cobra II: The inside Story of the Invasion and Occupation of Iraq*, 58-59.

[68] See, for example, Saddam Hussein's debate about whether or not to arm his population and create a state-supported militia. Ibid., 58.

[69] For discussion on the US's emerging doctrine of non-linear, non-contiguous operations, see United States. Dept. of the Air Force. Secretary of the Air Force., *Air Force Doctrine Document (AFDD) 2-1.3: Counterland Operations*, 65-67.; and United States. Dept. of Defense. Office of Force Transformation., *Elements of Defense Transformation*, 8.

[70] David E. Johnson, "Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era," in *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2007; reprint, from *Learning Large Lessons: The Evolving Roles of Grond Power and Air Power in the Post-Cold War Era*, Chapters 3 and 4. RAND, 2006), 168.; also Cooper, "Air Power and the Coercive Use of Force," 16.; Bruce R. Pirnie et al., "Kosovo (Operation Allied Force)," in *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2007; reprint, from *Beyond Close Air Support: Forging a New Ground-Air Partnership*, Chapter 3. RAND, 2005), 396.; and Wrage, "Conclusion," 107.

[71] Pirnie et al., "Kosovo (Operation Allied Force)," 397.

[72] Cooper, "Air Power and the Coercive Use of Force," 8.

[73] Ever since the Kosovo conflict, the USAF and US Army have been locked in debate over whether airpower, once effectively employed against the proper "strategic targets," can "win" a conflict without employment of ground troops. See Johnson, "Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era," 162-69.; also Cooper, "Air Power and the Coercive Use of Force," 10.; Spencer Abbot, "Air Power Strategy and the Problem of Coercion," in *Immaculate Warfare*, ed. Stephen D. Wrage (Westport, CT: Praeger, 2003), 21.; and Pirnie et al., "Kosovo (Operation Allied Force)," 394, 97.

[74] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 391.; also Israel Aerospace Industries LTD, "Rpg-7/Rpg-7v/Rpg-7vr Rocket Propelled Grenade Launcher (Multi Purpose Weapon)," http://www.defense-update.com/products/r/rpg.htm.; and Wikipedia.com, "Rocket-Propelled Grenade," http://en.wikipedia.org/wiki/Rocket_propelled_grenade.

[75] See, for example, Gordon and Trainor, *Cobra II: The inside Story of the Invasion and Occupation of Iraq*, 268-78.; also Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 396-97.; and Pirnie et al., "Kosovo (Operation Allied Force)," 396.

[76] "This ammunition is powerful enough to penetrate metal, ballistic or bullet-proof glass, even armored cars or helicopters." Senator Carl Levin, "Statement of Senator Carl Levin on Armor Piercing Ammunition," in *FDCH Press Releases*.

[77] "Five-Year Plan (FY04 – FY08) for the Manufacturing Technology (ManTech) Program," (Department of Defense, July 2003), B-9.

[78] The difficulty here would be developing the nanobots so they target only the invaders' equipment, while leaving the local infrastructure intact. But, theoretically, it could be possible based on the equipment's characteristics. The

NOTES (Continued)

USAF is already developing systems that discriminate friendly from enemy forces to enable autonomous attack [see "Missile Monitor," *Journal of Electronic Defense* 25, no. 12 (2002): 43.; also "Military," *GPS World* 16, no. 12 (2005): 48.; and "Lockheed Martin Successfully Tests Low-Cost Autonomous Attack System," *Defense Daily* 228, no. 21 (04 November 2005).]. The same type of autonomous targeting/identification could be applied at the nano-level to target the nanoparticles/nanobots against the adversary's equipment while ignoring friendly systems.

[79] Bush, "The National Security Strategy to Secure Cyberspace," viii.

[80] In their treatise "Unrestricted Warfare," Liang and Xiangsui provide an excellent overview of additional irregular warfare tactics a state could employ (and targets they could strike) against an adversary: trade, financial, ecological, psychological, smuggling, media, drug, technological, fabrication, resources, economic aid, cultural and international law, as well as "other types of non-military warfare too numerous to mention." (See Liang and Xiangsui, "Unrestricted Warfare," 50-57.) However, most of them leave a physical trail that would allow a state to take punitive, physical counteraction against the attacker if the results of the attack were truly catastrophic. The current study ignored those that fit this mold.

[81] For a description/analysis of the *Guerrillas in the Mist* and *Cyber 9/11* scenarios, see Myers, "Non-State Actor Threats in 2025".

[82] Liang and Xiangsui, "Unrestricted Warfare," 207-08.

[83] Ibid., 145-46.

[84] In essence, this is the concept of hitting the "side targets" to take out the main target. If the main target (in this case, the US military) is too strong, then instead strike at the "side targets." Ultimately, the main target will then collapse. See Ibid., 163.

[85] Parks and Duggan, "Principles of Cyber-Warfare", 123.

[86] Liang and Xiangsui, "Unrestricted Warfare," 46.

[87] Bush, "The National Security Strategy to Secure Cyberspace," vii.

[88] Timothy Shimeall, Phil Williams, and Casey Dunlevy, "Countering Cyber War," *NATO Review* (Winter 2001/2002): 18.

[89] Liang and Xiangsui, "Unrestricted Warfare," 208.

[90] For example, consider the difference in special effects between the original Star Wars trilogy (released between 1997-1983) and its prequels (1998-2005). Over this 20-year timespan, the CG industry went from non-existent to the point where almost the entire film was manipulated using CG; according to the director, George Lucas, "on one level you could say it was 90% fabricated and only 10% real." (see Scott Chernoff, "George Lucas Interview - the Story Comes First," Star Wars.com, http://www.starwars.com/episode-ii/bts/profile/f20020115/indexp4.html.). And that was on "*Star Wars Episode II*" in 2002; the technology has come even further since that time. As computer processors and CG software continue to advance, the results will become more and more lifelike.

[91] For example, see the decline in CBS news ratings following the Dan Rather scandal. Allison Romano, "CBS Scandal, Local Fallout," *Broadcasting & Cable* 135, no. 3 (2005).

Appendix A: Scenario Development Process

Introduction

This appendix describes the scenario development process used to develop the 2025 threat scenarios for the Blue Horizons (BH) program. First, the authors discuss scenario development in general and highlight the unique way in which they approached the scenario development process. Next, they describe the end-to-end process for generating scenarios, starting with scenario selection and ending with the documentation and utilization of the scenarios. The scenario developers tailored approaches from The Futures Group, as well as from the Millennium Project, to derive the final process that led to mature threat scenarios.[1] The authors focused the process to meet BH objectives at each step, to create scenarios that were relevant, realistic and useful to the investigation of future technology applications.

Scenarios – An Overview

"A scenario is a story that connects a description of specific future to present realities in a series of causal links that illustrate decisions and consequences"[2] Typically, scenarios result in broad textual descriptions of plausible futures, but lack a significant description of the analytical processes that led the creators to one conclusion over another. The scenario generation process often involves groups of individuals, each of whom bring a specialized set of knowledge; they generate ideas in process meetings in which a facilitator asks probing questions to develop the scenario logic.[3] Members of the team are therefore able to check one another for logical consistency, rationality, necessity and completeness. While the investigators for the current threat scenarios enlisted the help of peers and others who might provide quality and sanity checks on the scenario development process, no large group emerged. Most scenarios of similar subject matter were unavailable in open sources, and a few analysts and intelligence experts—those who could provide significant expertise in the subject matter—were tentative, at best.

Wanting to stay in open source literature, but also wishing to produce high-quality scenarios, the authors required more rigor in their scenario development process to develop, justify and explain decisions. Without the luxury of a groupthink forum to cross-check boundaries and applications, the authors found it necessary to inject a standard process that included sufficient documentation for future researchers to understand why the scenarios ended up as published. At the same time, for relevancy and expediency for authors citing the scenarios, they tried to use existing tools and techniques to record and clarify scenario building blocks. This is not to say that the investigators abandoned scenario development principles, for they followed the three step process outlined by The Futures Group International and documented by Jerome Glenn, explained in the Process Section below.[4]

The result of the work was a set of textual explanations about scenarios, but backed by significant documented analysis to explain what led the authors down those paths. Indeed, the process brought out many unforeseen capabilities and issues, while at the same time illuminating and eliminating personal biases and constraints. While perhaps not equivalent in quality to the sanity check provided by groups of experts, the process enabled a free flow of ideas and avoided common pitfalls such as loss of focus, unjustified rejection of scenario elements, or inadvertent omission of critical blocks.[5] At the same time, technology researchers from the BH program offered feedback to help guide the scenarios to a more useful and relevant level; while not necessarily experts, these were the primary customer base for the effort.

One other key way in which these scenarios differed from others was that the investigators avoided threat-based planning. The emphasis was not on *who* the threat may be, but on what capabilities the threat may possess and how he would employ those capabilities. This led the scenarios away from story-based descriptions of plausible futures and toward analysis-based illustrations of ways and means by which future adversaries may fight to achieve their ends. The process used to develop the scenarios integrated multiple analytical elements to generate scenarios that were relevant, realistic and useful for the BH effort.

The sections below describe the process the authors used to generate the BH scenarios. For accuracy, the authors included descriptions of each step in the process verbatim from Jerome Glenn's treatise on scenario development, accompanied by an explanation of how they adapted the process for the BH effort. The three main steps in the process were Preparation, Development, and Reporting and Utilization.[6]

Preparation

Purpose

> *Define the scenario space. A scenario study begins by defining the domain of interest.*[7]

The authors interpreted this to mean they had first to understand the purpose of developing the scenarios. The purpose of this effort was to provide the BH team with a set of threat scenarios and capabilities against which each researcher could compare his or her technologies. It was important to note that this purpose neglected "natural" threats or disasters, such as a catastrophic failure of the economy, loss of vital resources, etc., that would not have been caused by an enemy. While these factors could dramatically affect the US military's abilities to wield influence, analyzing them was beyond the scope of the investigation. The authors therefore limited the investigation to an examination of potential adversaries because military technologies (as well as tactics and processes used to employ those technologies) are meant to counter those of our enemies. In addition, it was impossible to understand or capture all the factors from all sources that could threaten the US. Futures research, and scenario development in particular, has generally shown that "defining a large number of alternative worlds is often neither necessary nor desirable," so the authors reduced the scope to focus on potential threats generated by adversaries.[8] Understanding that the purpose of the work was to provide common context regarding potential adversaries, the investigators developed objectives to guide scenario selection.

The authors defined two primary objectives to guide the scenario-development process: 1) bound the plausible threat space in 2025; and 2) develop scenarios that clearly illustrated the benefits of novel technology employment. In other words, they sought to make the scenarios reasonable, relevant and useful to the BH effort. Any scenario must be plausible, but not necessarily probable, in that it is not likely that any one particular scenario will happen exactly as described.[9] However, the combination of scenarios should allow planners to "clearly see and comprehend the problems, challenges, and opportunities that such an environment would present."[10] Thus, the chosen scenarios provided extreme cases in which adversary capabilities stressed the system under investigation (in this case, future US Instruments of Power) in different ways. The intent was not to accurately predict any one scenario, but rather to bound the potential threat space, for a "set of choices that encompass the range of major challenges and opportunities usually suffices."[11] The second objective ensured that the scenarios provided a sounding board for BH technologies; the researchers considered relevance to technology application in each step of the scenario development process. The results ultimately helped the authors define driving factors to describe and discriminate future adversaries.

Driving Factors: The Matrix

> *Given a clear statement of the domain, analysts list key driving forces thought to be important to the future of the domain…If three such forces were defined, the*

> *space would be three-dimensional. With two forces, scenario space is two-dimensional.*[12]

How does one define an adversary? This has proven to be the hardest part of the scenario selection process. There is no standard for how military planners attack this question, despite numerous works on the nature of war, the history of warfare, and planning campaigns. In fact, the authors found few attempts to characterize adversaries in other than broad terms, such as irregular versus regular (in fact, one of our axes). Therefore, the authors went back to basics and attempted to describe potential threats in broad terms by answering the following set of questions:

Who will fight the US?
With what will they fight?
Where will they fight?
When will they fight?
Why will they fight?
How will they fight?

The authors developed a list of potential factors that addressed the above basic questions, with the exception of "when?" and "why?" The BH team charter dictated the "when" – the target year of 2025. Answering the "why" involved a complex dynamic that would be situation- and adversary-specific; therefore, it was discussed in the scenarios as a contextual element where required. In addition, when trying to determine the technologies/capabilities in which the USAF should invest, the key was to focus on what an adversary may possess and how they may employ those capabilities against the US, in order to develop counters to the potential threat. From this perspective, *why* the adversary had chosen to use these capabilities against the US was not important. Therefore, the authors dismissed the "why" as a discriminating factor. The focus on the remaining four questions allowed the investigators to develop a set of potential factors, or drivers, for the initial scenario matrix. Table A-1 below lists these factors. The authors chose the factors in Table A-1 through a combination of brainstorming and research; the curriculum at Air Command and Staff College also provided a benchmark for the accumulated wisdom and experience of senior USAF leadership, indicating what they deemed relevant. Table A-1 also lists some of the additional sources that led the investigators to the choice of these factors.

Table A-1. Initial Set of Factors

Question	Factors		Sources
How	Irregular Combat	Regular Combat	Gray,[13] United States,[14] Waxman[15]
How	Geographically Centered	Geographically Dispersed	Stephenson,[16] Johnson,[17] O'Sullivan[18]
Where	On Foreign Soil	On Our Soil	None—two possibilities
Who	State	Non-state	Mansbach,[19] Arts,[20] Strange[21]
Who	Coalition	Lone Actors	None—two possibilities
Who	Technology Developers	Technology Consumers	None—two possibilities
With What	WMD	Non-WMD	Hutchinson,[22] Alibek,[23] Larsen[24]
With What	Evolutionary Technical Capability	Revolutionary Technical Capability	Phaal,[25] Lorber,[26] Barley[27]
With What	Materials Dominant (bombs, lasers, etc)	Information Dominant (cyber, public opinion)	Alberts,[28] Cebrowski,[29] Cohen[30]

While the factors shown in Table A-1 provided a solid foundation on which to begin describing the threat space, it rapidly became apparent that the resulting scenario matrix would be too large. Therefore, the authors' next step was to cull the matrix down to a manageable level.

The Matrix: Reloaded

> *A smaller set of choices that encompass the range of major challenges and opportunities usually suffices. A few possibilities may need to be excluded as illogical or insufficiently plausible over the planning horizon. The final selection of worlds should be sufficient to present a range of opportunities and challenges, but should be small enough in number to handle. Four to five "worlds" seems ideal to capture a range of future challenges and opportunities.*[31]

In scenario development, "[u]sually some 6 to 30 variables affecting the future situation are nominated. This list is then winnowed down by eliminating redundancies."[32] For the list in Table A-1, there were 2^9, or 512 possible scenarios, one for each possible combination of factor pairs. Therefore, compressing the matrix became a priority to make the scenarios manageable.

The authors compressed the matrix by eliminating redundancies and making a number of assumptions, ultimately reducing the matrix to eight scenarios.

Eliminating Redundancies

Geographically-Centered vs Geographically-Dispersed

By default, any state actor is somewhat geographically-centered; if necessary, one knows where the state is and can generate a set of fixed strategic targets. The authors considered this to be part of what constituted a "regular" fight. In addition, saying a state actor is "geographically-centered" does not mean it will mass its forces in one location. Since the mid-90's, even state actors have made it a point to disperse strategic and tactical targets to hide them from U.S. intelligence collection and make them more difficult to target.[33] However, any discussion of irregular warfare would cover these types of tactics, since non-state actors (i.e., terrorist organizations) typically operate in geographically-dispersed "formations" or cells. Therefore, the authors deemed geographic dispersion and regular/irregular warfare to be somewhat redundant. Thus, they eliminated the geographic dispersion factor.

Coalition vs Lone-Actor

In a similar fashion, the authors were able to eliminate a second factor by reasoning that whether an adversary acts alone or in a coalition is redundant to whether it is a state or nonstate actor. Logically, if two or more nonstate entities band together, they would form either a pseudo-state or a larger nonstate. Likewise, if two states (or a state and a nonstate actor) banded together, it would be the same as confronting a larger, more capable single state. The challenges associated with confronting these complex situations were thus subsets of the discussion regarding facing off against state or nonstate actors. In short, the threat space was sufficiently bound without the coalition/lone actor discriminator.

Key Assumptions

As one can see, eliminating the redundancies in the original matrix only eliminated two potential axes. Thus, the authors made several assumptions to further compress the matrix; Appendix B provides additional supporting documentation for these assumptions.

Evolutionary vs Revolutionary Technical Capability

The authors eliminated this driver by making a simple observation based upon insurgent activities in Iraq: even evolutionary technologies can be applied in revolutionary ways. For instance, the Iraqi insurgents have used standard cell phones as detonators for IEDs.[34] They took two common technologies and combined them in a revolutionary manner. The global reach of the internet allows rapid transfer of the know-how and ingenuity of one or two people who generate simple ideas like these to other potential enemies throughout the world. Thus, the USAF can expect future enemies to rapidly adapt as they discover what does and does not work against our forces.

As a result, the USAF must be flexible and able to respond to a revolutionary effect of technology's application, independent of whether that effect was generated using evolutionary or revolutionary technology. Knowing this, the authors ignored the Evolutionary vs Revolutionary Technical Capability driver, and simply assumed that all effects could be revolutionary.

Technology Developer vs Consumer

The authors eliminated the technology developer/consumer pair with an assumption, developed in Appendix B, that the rate of technology proliferation will accelerate at or well beyond its current rate. The assumption dictated that the timing gap for new, breakthrough technologies to proliferate to either open or black markets will continue to close through 2025. In other words, in 2025 there will be virtually no difference between the technical capabilities of technology producers and consumers, and the discriminator was therefore moot. With this assumption, the latest technologies would be available to all actors almost immediately after production, allowing for worst-case considerations within the scenario. The individual scenarios discussed nuances associated with eliminating this driver pair, such as the ability of an adversary to obtain, retain, and replenish technologies based on funding and level of sophistication.

Availability of WMD

As discussed in Appendix B, the authors assumed all potential threats will have access to WMD; a corollary to this assumption was that any actor can choose to use WMD. This assumption allowed WMD use to be an adversary capability in all scenarios (to different degrees, of course, as determined by the driving attributes of the scenario). With this assumption, the driver pair became irrelevant.

Fighting on US or Foreign Soil using Regular or Irregular Warfare

The assumptions discussed up to this point, along with the elimination of redundancies, allowed the authors to compress the matrix to the four driver-pairs shown in Table A-2 and in Figure A-1 below.

Table A-2. Final Set of Factors

Question	Factors	
How	Irregular Warfare	Regular Warfare
Where	On foreign soil	On our soil
Who	State	Nonstate
With What	Materials dominant	Information dominant

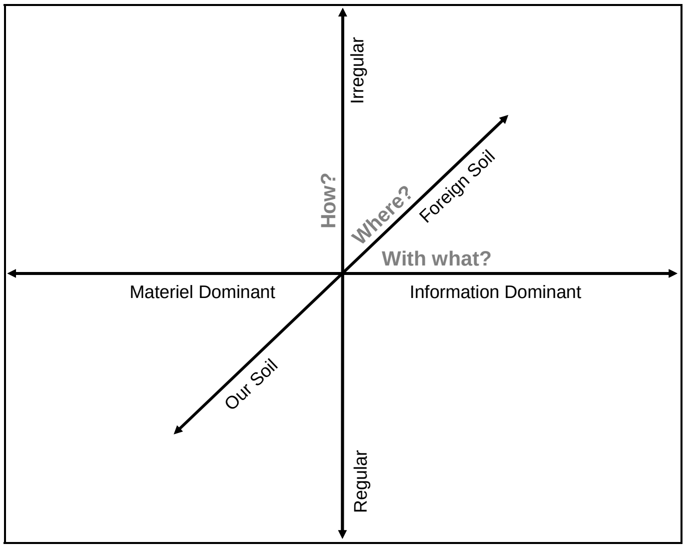

Figure A-1: The Scenario Factors for State and Nonstate Adversaries

This four-dimensional space would have generated 16 possible scenarios, which was still too unruly. Therefore, the investigators prioritized the factors, with state versus nonstate being the most important discriminator; each would have eight potential scenarios. However, the authors made certain specific assumptions about state actors, and others about non-state actors, to cut the number of scenarios in half.

For state scenarios, the authors assumed that in 2025, state adversaries would still lack the power projection capability to invade the United States. One could argue that a state might sponsor groups of irregulars or use Special Operations forces to conduct operations on American soil; however, the nonstate scenarios covered the challenges of that kind of event. Thus, the state actor scenarios reduced with the assumption that any conflict with a state actor would not occur on US soil. For nonstate scenarios, as was mentioned above, the authors deemed all such conflicts to be irregular, by definition.

These assumptions reduced the matrix to the one shown graphically in Figure A-2. The assumptions described here lead to the state actor scenarios collapsing to the vertical plane, while the non-state actors collapse to the horizontal plane. For clarity, Figure A-3 and Figure A-4 break these planes out for state and nonstate actors, respectively. The figures also include the names given to each of the corresponding scenarios.

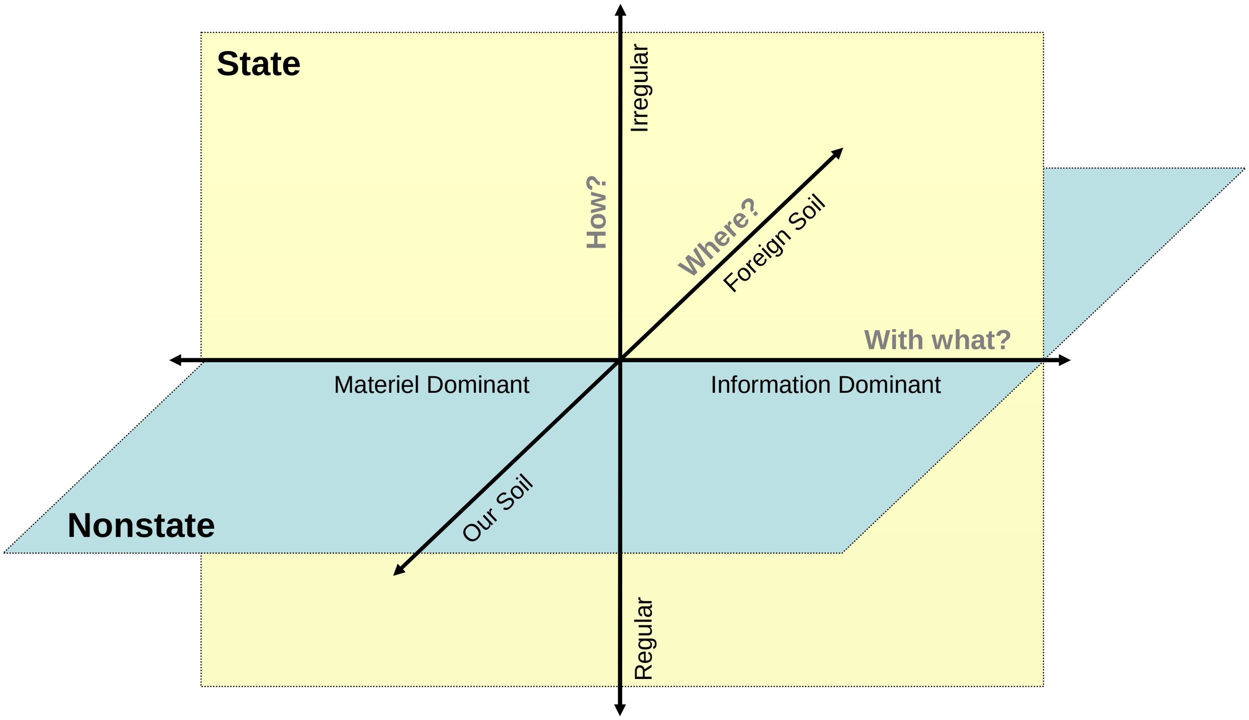

Figure A-2: Scenario Matrix

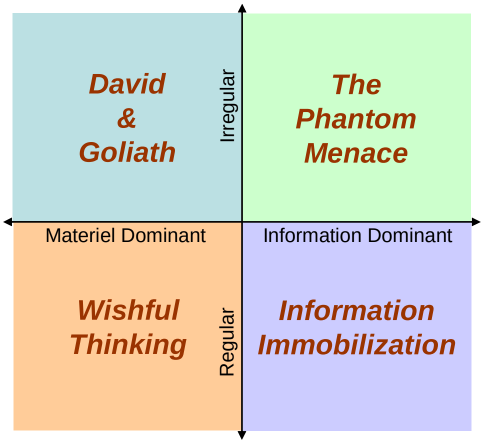

Figure A-3: State Actor Scenarios

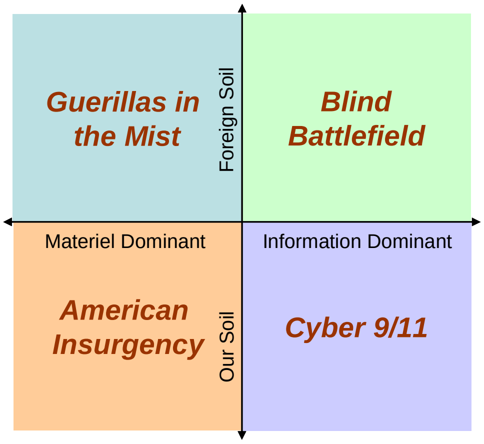

Figure A-4: Nonstate Actor Scenarios

Quality Control: Validating the Driver Selection

The final step in scenario selection was a quality check, a way to ensure the selected scenarios were both necessary and sufficient to meet the purpose and objectives of Blue Horizons. Of primary concern was whether the factors chosen were indeed factors that would be relevant in the 2025 period. The authors also had to determine whether the set of factors was complete. To accomplish this task, the authors used environmental scanning and a literature review of previous futures studies.

Environmental Scanning

Environmental scanning is a method that provides a trend analysis on a set of subjective data, looking for "weak signals" that indicate plans should change.[35] Investigators usually limit the subjective data they poll to products of subject matter experts, such as scholarly literature reviews, expert panels, periodical reviews, expert essays, conference presentations, etc. By sampling these data for trends in key words, one can quickly identify emerging topics before they hit the mainstream. For example, if chocolate had never been a topic at confectioner conventions for 20 years, but then had a growing number of citations in the next 3, the increase would be an indicator that chocolate was about to make a breakthrough. Like all futures methodologies, there is risk in assuming that these weak signals are not anomalies. However, the method will uncover all real weak signals in addition to the false alarms; it is left to the researcher to determine which ones are relevant. Besides uncovering weak signals of growth, environmental scanning can also reveal the weakening of previously-strong factors. If experts start publishing less works about a given topic, it could be an indicator of the topic's potential demise.

To test the factors for viability in 2025, the authors conducted environmental scanning on scholarly publications using the factors as key words. They simply tracked the number of citations on those key words for the last 30 years, from 1965 to 2004, using Google's Scholar Search.[36] Figure A-5 shows the results of the scans.

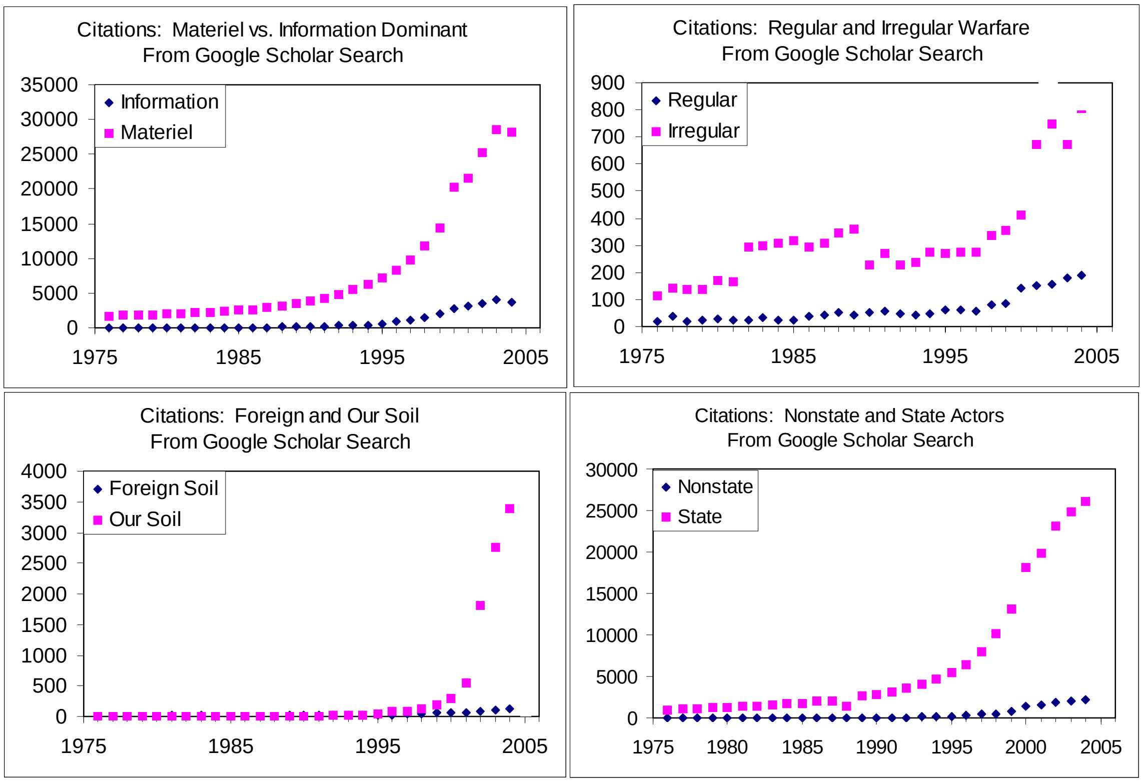

Figure A-5: Environmental Scan of Scenario Factors

The authors analyzed these scans to validate their choice of driving factors. The data indicated there was steady and significant growth for all the factors under investigation. In one case, the materiel data decreased in 2003, believed to be due to the saturation of warfighting technology publications and to the surge in the focus on information and cyber warfare. Interesting signals appeared in the irregular warfare scan. There was a surge in citations following the 1982 bombing in Beirut and a decline with the fall of the Soviet Union. A disconcerting, unexplained decline occurred in 2003; however, the trend recovered in the next year. In all the keyword pairs, citations on one of the two poles grew by more than 100% in the last 10 years. In the same period, these factors also displayed nonlinear growth. The bottom line was that there was no unexplained weak signal to indicate a decline in relevance for the chosen factors. This did not prove relevancy in 2025; however, when coupled with the recent cited sources listed in Table A-1, it demonstrated plausibility that these factors would continue to be important. The final question, then, was whether the set of factors was complete enough to sufficiently bound the threat space.

Overview of Previous Futures Research Studies

In any futures research, one cannot truly test for completeness because of the large number of factors that could exist to shape the future; however, the authors attempted to minimize any "holes" in the current scenario matrix by comparing the chosen drivers to previous military-related futures studies. While this method did provide some insights, for the most part it was like comparing apples and oranges, because of the way the authors defined the current scenario development process.

While most existing studies and forecasts focused on developing a politico-socio-economic context for what the world would look like, the scenarios developed herein attempted to describe what a future threat might look like, the capabilities it might possess, and how it might employ those capabilities. As a result, there was not a one-to-one correlation between previous scenario development efforts and the current desired end state. However, comparing previous scenario drivers did inspire some thought/discussion because politico-socio-economic factors ultimately shape the capabilities possessed by an actor, as well as how it might employ them. Thus, the paragraphs below provide a brief overview of the most pertinent futures studies examined in the literature, as well as a discussion of how the drivers used in their scenario development related to the current effort.

AF 2025

The most pertinent set of pre-existing scenarios was the AF 2025 study, published in 1996.[37] In this study, the research team developed eight scenarios based on three drivers: The rate of technological change (ΔTeK), the scope of the world power grid (was the concentration of power still primarily with the US, or was its influence diluted/counteracted by other events/ alliances?) and the American Worldview (global or domestic). As one can see, none of these drivers really described the "who, what, why, where or how" associated with a future threat, and were therefore not directly applicable as drivers for the BH scenarios.

However, while the AF 2025 drivers were not directly applicable to the manner in which the BH team cast their drivers of a future threat, they did raise some important concepts that the current authors incorporated into their assumptions, ultimately shaping the Blue Horizons scenarios. First, as described in Appendix B, the authors assumed the rate of change of technology (ΔTeK) would continue. Second, the events of 9/11/01 essentially altered the strategic scope for the US, forcing it to have a global worldview; it simply cannot afford to revert to an isolationist mode. And finally, the authors determined that the global power distribution was simply not the right "fit" with the "who, what, why, where and how" that described a potential adversary. In addition, it was somewhat irrelevant. As discussed in Appendix B, if it needs to employ its forces against any adversary, the US will have to fight as part of a coalition effort. If the US possesses all the "global power," it will still need a coalition to legitimize its offensive military operations so it does not appear to be the "bully" who is forcing everyone else to do its bidding. If the global power is dispersed, then the US would need to form a coalition to consolidate enough power to implement its proposed actions. In either case, the US must prepare itself to fight as part of a coalition. The bottom line is that the three drivers used in AF 2025 were not outright used as drivers in the BH scenario development, but they indirectly affected the final product by influencing the baseline assumptions underpinning the BH scenarios.

SpaceCast 2020

The SpaceCast 2020 effort created eight scenarios that described contextual factors relevant to US space-planning strategy. The SpaceCast 2020 team based its scenarios on three key drivers: the number of actors playing a role in space; the will of the actors to use space; and the technological proliferation and growth and economic vitality of the actors (also called "technomic capability").[38] Like the AF 2025 drivers, these were not directly applicable to the Blue Horizons effort.

There was one main reason the SpaceCast 2020 drivers were not applicable to the BH effort: they were too space-centric. The Blue Horizons team was looking at technology applications across the entire portfolio of USAF missions: air, space and cyberspace. As a result, the SpaceCast 2020 drivers created a scenario set that was simply too restrictive.

Alternative Futures Conference

The final military-related scenario set examined was a product of the National Intelligence Council's "Alternative Global Futures: 2000-2015" conference (held in 1999).[39] Similar to the AF 2025 study, the drivers in this study resulted in four scenarios that described a geo-political context of future worlds. As a result, the drivers and scenarios were not directly applicable to the direction the BH team wanted to pursue in its scenario development. The bottom line was that, as mentioned above, the BH team took a fairly different approach to its scenario development process. Instead of developing a set of scenarios to describe future "worlds," they used the scenario development methods to describe the characteristics of potential future threats.

Other Projects

In addition to the three projects discussed above, the authors also had access to a large number of other futures research projects. However, after scanning the three above, it rapidly became apparent that the scenario focus in the current effort was vastly different from what had been done in the past. Therefore, the authors decided to just press ahead to proceed with the actual scenario development.

Development

Key Measures

> *Within each scenario, certain key measures are described. These measures might include forces such as economic growth, legislative environment, technology diffusion and proliferation, or competitive capability, among others. The key measures need to be selected with care. They should have the potential for great impact on the outcome of the scenario…Every scenario in the set will include projections of the same measures.*[40]

Militaries project and use force. As has been explained, the authors deemed that who the threat might be was less important than how it might wield that force, what tools it would use, where it would fight, and when it launches its attack. Thus, a threat's capabilities and how it might employ them are the critical elements for understanding how to counter the threat. As a result, the U.S. military has shifted its focus from "threat-based" to "capabilities-based" planning methods.[41] Therefore, when the authors discuss various threats, they mean capabilities, (including the method of employment); these are the only key measures for the scenarios.

Developing Capabilities

To generate capabilities and understand employment methodologies, the authors emulated the adversary for each scenario. While it is possible to generate a list of capabilities ad hoc, the inevitable results would be multiple omissions, biases, and inaccuracies. The authors, again without the benefit of large teams of experts, engaged in a step-by-step analysis starting with understanding the enemy objectives, and ending with the development of a most-likely capabilities list for each scenario.

Table A-3. Generating a Capabilities List

General Approach	Basis
Identify the adversary's strategic objectives	Operational Planning
Identify the centers of gravity (COG) to achieve strategic objectives.	Effects-Based Operations, Operational Planning
For each COG, identify operational objectives and perform a critical element analysis	Effects-Based Operations, Operational Planning
For each critical vulnerability, identify decisive points.	Effects-Based Operations, Operational Planning
For each COG, identify capabilities that can affect the decisive points.	Capabilities-Based Planning
For each capability, develop a risk assessment (probability versus impact)	Risk Management
Determine most likely capabilities (probability> 60%)	Risk Management, Capabilities-Based Planning
Discuss most likely capability set (see outline below)	Scenario Thinking

Strategic Objectives

The first step for getting into the adversary's head was to understand his motivations; to the military planner, this means to understand his strategic objectives. What is it that the adversary wants to achieve? What is his desired end-state? Each scenario carried its own unique strategic objectives in accordance with the drivers that defined the adversary. The authors used analogies to current or past conflicts to help project relevant end states into the target timeframe.

Centers of Gravity

For these scenarios, the authors defined centers of gravity (COGs) as “physical or moral entities that are the primary components of physical or moral strength, power, and resistance. They do not just contribute to strength; they are the strength.”[42] In this case, the COGs of interest were friendly COGs, because the authors needed to understand what the adversary could affect to achieve his strategic objectives. Understanding the relationships between the COGs was just as important. Often, enemy tactics were derivable from the ways in which cascading or culminating effects resulted from actions against multiple COGs simultaneously.

Critical Element Analysis

In order to understand capabilities, strategic objectives and COGs were necessary but insufficient, so the authors chose to drill down to lower levels to gain a full understanding of the enemy. They first drilled down from strategic objectives into operational objectives for each COG, a way to understand the adversary’s goals for affecting each center. From the lower-level objectives flowed logical lines of operation, to ensure the investigators were not constrained by biases or historical examples. The authors viewed each COG as a system of systems and defined those areas in which operations might be effective in the target timeframe as logical lines of operation. In essence, lines of operation were to the scenario planning what first principles are to physicists – a way to start the analysis from the ground-up.

Once they had defined lines of operation, the authors conducted a critical element analysis to determine how an enemy might attack the COG. A critical element analysis is a way to break lines of operation into critical capabilities, requirements, and vulnerabilities, allowing researchers to identify what provides lines of operation, and henceforth COGs, their foci of power. Critical capabilities describe the elements within a COG that put fear into the adversary’s heart in the context of achieving his strategic objectives.[43] Critical requirements are the "conditions, resources, and means that are essential for a COG to achieve its [critical capabilities]."[44] Critical vulnerabilities are simply critical requirements that are susceptible to defeat by adversary action, leading to the concept of decisive points.

Decisive Points

On the march to generating a capabilities list for each scenario, one must understand what the adversary plans to use its capabilities against. The definition of COGs, lines of operation, and critical vulnerabilities allowed the authors to drill down to the lowest level possible. Decisive points for scenarios were generic target sets that, if affected by the adversary's capabilities, weakened the friendly centers of gravity. In joint operational planning, decisive points are very specific elements of specific systems, such as an integrated air defense system; however, it is neither necessary nor desired to go to that level to develop a capabilities list. Instead, it was sufficient to understand what kinds of things the enemy could affect (facilities, people, data, etc.). As a result, the authors interchangeably referred to decisive points as "targets." If the adversary knows the target sets that influence COGs, in turn contributing to his operational and strategic objectives, he could start to build a list of useful capabilities.

List of Capabilities

The generation of capabilities was by far the most subjective aspect of the scenario development process. Authors relied on research into past and current conflicts, projections about military tactics, technologies, and procedures, and peer inputs to arrive at a list of capabilities for the decisive points in each scenario. All viable and relevant ideas remained on the list, regardless of probability of use or technological availability; the authors then considered these aspects in subsequent analyses.

Risk Analyses

The scenario developers leaned heavily at this point on a research paper by Lt Col Thomas Goss entitled “Building a Contingency Menu: Using Capabilities-based Planning for Homeland Defense and Homeland Security.” Despite the title, his methodology provides a toolset that was well suited to future threat scenarios not related to homeland protection issues. For each line of operation, Lt Col Goss assessed each capability for impact and likelihood, plotting them on a line to illustrate which of the capabilities appeared likely while simultaneously carrying a high consequence.[45] While he did not dwell much on naming the process, it was equivalent to a risk analysis in accordance with the integrated risk management framework (IRMF), but treating each capability as an independent risk.[46]

The goal of the IRMF is to produce a numerical comparison of risk by multiplying a quantitative probability of a risk by its consequence. By plotting the result on a matrix (as illustrated in Figure A-6), one is able to see the overall risk category for each risk, as well as its individual probability and impact values.

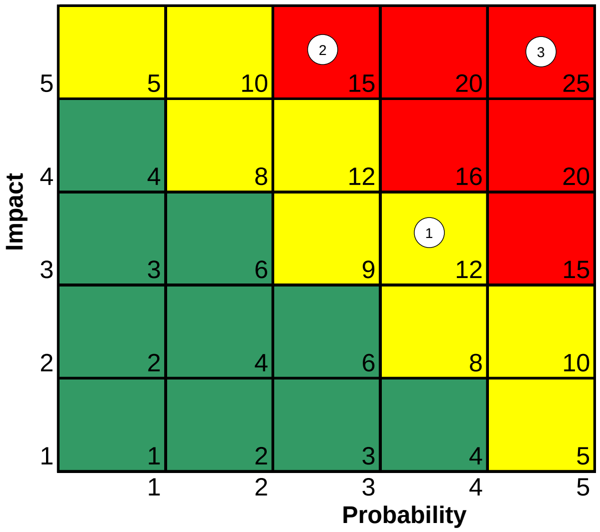

Figure A-6: IRMF Risk Matrix

In the example in Figure A-6, one can see that risk 1 is more likely than risk 2, but that risk 2 has a greater overall risk because it also has a higher impact. Instead of plotting the capabilities in a single line, the authors chose to perform a risk analysis to see the full picture of the risk associated with each capability.

To avoid a completely subjective, unexplained view of the risks associated with each capability, each scenario required the development of criteria to define probability and impact. For example, in one scenario the author based the probability criteria on technology availability in the target timeframe, cost (in terms of materiel and human capital), and probability of detection before the attack. In the same scenario, author based the probability criteria on the area of effect and the level of objectives (tactical, operational, or strategic) achieved. Some capabilities provided direct effects to contribute to, or in some cases even achieve, strategic objectives; others failed to achieve even limited tactical objectives.

Because each scenario used different criteria to determine the impact of a capability, the risks were not directly comparable across the scenarios. For instance, a single capability could have a higher impact in one scenario than another, so it would have a different risk. More importantly, although the risk mapping showed the relative risks within a scenario, a risk rating of “20” in one scenario was not directly comparable to a risk rating of “20” in another scenario. Thus, one should refrain from saying “scenario 1 presents a higher risk than scenario 2” based simply on the numbers in the risk matrix. Thus, instead of a quantitative comparison based on the risk numbers, the authors qualitatively compared the scenarios to one another using criteria from the 2006 Quadrennial Defense Review. Appendix C, Figures C-1 and C-2 show these comparisons for state and nonstate actors, respectively.

Most Likely Capabilities

Most likely capabilities emerged from the risk analysis. The authors defined those above the 60% probability line (falling in the last two columns of Figure A-6) as being highly probable. Admittedly, the cut line was completely arbitrary; in this case, 60% reduced the field, but did not eliminate what the investigators felt were critical capabilities. The only task that remained was the compilation of a single list of the most-likely capability set.

Reporting and Utilization

Documentation

> *In most cases, the best documentation is a simple series of charts and narratives describing the future history represented by each scenario. As thinking surrounding the scenarios is driven farther down in the organization, several levels of documentation for each of the scenarios is often useful.*[47]

The scenarios culminated in a textual summary of the key contextual elements surrounding the nature of the adversary and the capabilities he had available. The authors compiled those elements most relevant and useful for technologists to consider into each scenario script. In addition to each scenario description, individual appendices offered the supporting data the authors used to produce the scenarios in accordance with the scenario development process. The appendices provided further detail to justify the scenario results.

Contrast Scenarios

> *Contrast the implications of the alternative worlds. How different are the business decisions and planning goals you would pursue considering each alternative world? What actions and commitments offer your organization the most resilience in the face of these uncertainties?*[48]

Comparing and contrasting the alternative worlds was beyond the scope of the investigation, since the scenarios met the objectives for the BH program.

Testing Policies

The range of scenarios can be used to test policies.[49]

The authors left this step for the remainder of the BH team to accomplish. Each individual technology researcher will test his technologies against the scenarios. These assessments considered a technology highly valuable if it either addressed aspects of multiple scenarios, or if it uniquely addressed high consequence adversary capabilities within a given scenario.

Conclusion

The developers for the 2025 threat scenarios used a mixture of analytical tools to tailor standard scenario development processes to meet the objectives of the Blue Horizons team within the constraints of the environment. These tools, in addition to eliminating personal biases, provided the bases for each scenario, documented each step, and explained the decisions each author made during scenario construction. Overall, the focus of the effort was to allow technologists a common context on which to compare future technologies; this required relevancy, realism and utility.

NOTES

[1] Jerome Clayton Glenn et al., *Scenarios*, Version 2.0. ed., Futures Research Methodology (Washington, DC: American Council for the United Nations University the Millennium Project, 2003), 4.

[2] Ibid.

[3] Ibid., 9.

[4] Ibid., 9-10.

[5] Ibid., 10-11.

[6] Ibid., 9-10.

[7] Ibid., 9.

[8] Ibid.

[9] Glenn and The Futures Group International, "Scenarios," 4.

[10] Ibid., 9.

[11] Ibid.

[12] Glenn et al., *Scenarios*, 9.

[13] Colin S. Gray, "Another Bloody Century -- Future Warfare," in *Inter/National Security and War, AY07 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, August 2006; reprint, from *Another Bloody Century*. London: Weidenfield & Nicholson, 2005).

[14] United States. Dept. of Defense. Secretary of Defense., *2006 Quadrennial Defense Review*.

[15] Matthew C. Waxman and Project Air Force (U.S.), *International Law and the Politics of Urban Air Operations* (Santa Monica, CA: Rand, 2000).

[16] Michael Stephenson, *Battlegrounds : Geography and the History of Warfare* (Washington, D.C.: National Geographic, 2003).

[17] Ronald M. Johnson and U.S. Army Command and General Staff College., "Application of Aspects of Unconventional Warfare : Tools for Engaging the Current and Future Threat Trends of the Post-Cold War Environment" (U.S. Army Command and General Staff College, 1999).

[18] Patrick O'Sullivan, "A Geographical Analysis of Guerilla Warfare," *Political Geography Quarterly* 2, no. 2 (1983): 11.

[19] Richard W. Mansbach, Yale H. Ferguson, and Donald E. Lampert, *The Web of World Politics : Nonstate Actors in the Global System* (Englewood Cliffs, N.J.: Prentice-Hall, 1976).

[20] Bas Arts, Math Noortmann, and Bob Reinalda, *Non-State Actors in International Relations*, Non-State Actors in International Law, Politics, and Governance Series (Aldershot, Hants, England ; Burlington, VT: Ashgate, 2001).

NOTES (Continued)

[21] Susan Strange, *The Retreat of the State : The Diffusion of Power in the World Economy*, Cambridge Studies in International Relations ; (New York: Cambridge University Press, 1996).

[22] Robert Hutchinson, *Weapons of Mass Destruction : The No-Nonsense Guide to Nuclear, Chemical and Biological Weapons Today*, Cassell military paperbacks ed., Cassell Military Paperbacks (London: Cassell, 2004).

[23] Ken Alibek and Stephen Handelman, *Biohazard : The Chilling True Story of the Largest Covert Biological Weapons Program in the World, Told from the inside by the Man Who Ran It*, 1st ed. (New York: Random House, 1999).

[24] Jeffrey; Wirtz Larsen, James J.; Croddy, Eric A., *Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology, and History*, ed. James J. Wirts (Abc-Clio Inc, 2004).

[25] R.; Farrukh Phaal, Clare, Probert, David R., "Technology Roadmapping--a Planning Framework for Evolution and Revolution," *Technological Forecasting and Social Change* (2003).

[26] Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield*.

[27] S.R. Barley, "What Can We Learn from the History of Technology?," *Journal of Engineering and Technology Management* 15, no. 4 (1998): 19.

[28] David S. Alberts, John Garstka, and Frederick P. Stein, *Network Centric Warfare : Developing and Leveraging Information Superiority*, Ccrp Publication Series (Washington, DC: National Defense University Press, 1999).

[29] Arthur K.; Garstka Cebrowski, John J., "Network-Centric Warfare: It's Origin and Future," *Proceedings*, no. January 1998 (1998).

[30] Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* (1996).

[31] Glenn et al., *Scenarios*, 9.

[32] Glenn and The Futures Group International, "Scenarios," 6.

[33] John Arquilla, David Ronfeldt, and Michelle Zanini, "Information-Age Terrorism," *Current History* (2000): 179-85.

[34] U.S. Army Training and Doctrine Command (TRADOC), "A Military Guide to Terrorism in the Twenty-First Century: TRADOC DCSINT Handbook No.1," (Ft. Leavenworth, KS: United States Army, 2005), E-7.

[35] Jerome Clayton Glenn et al., *Environmental Scanning*, Version 2.0. ed., Futures Research Methodology (Washington, DC: American Council for the United Nations University the Millennium Project, 2003), 1.

[36] "Googlescholar.Com," http://www.scholar.google.com.

[37] Col Joseph A. Engelbrecht Jr. et al., "Alternate Futures for 2025: Security Planning to Avoid Surprise," in *Air Force 2025* (Maxwell AFB, AL: Air University, April 1996), 10-12.

[38] Air University, *Spacecast 2020*, vol. 1 (Maxwell AFB, AL: Jun 1992), 3.

[39] Dr. Peter Dombrowski, "Alternative Futures in War and Conflict: Implications for U.S. National Security in the Next Century," in *An Occasional Paper of the Center for Naval Warfare Studies* (Newport, RI: Naval War College, Strategic Research Department Center for Naval Warfare Studies, April 2000).

NOTES (Continued)

[40] Glenn et al., *Scenarios*, 9.

[41] See United States. Dept. of Defense. Secretary of Defense., *2006 Quadrennial Defense Review*, 4.; United States. Dept. of the Air Force. Chief of Staff., *The U.S. Air Force Transformation Flight Plan 2004*, 51-52.; United States. Dept. of the Air Force. Chief of Staff., *The Edge: 2005 Air Force Transformation*, 6.; United States. Dept. of Defense. Office of Force Transformation., *Elements of Defense Transformation*, 3.; and United States. Dept. of the Air Force. HQ USAF/A8X., *Air Force Roadmap 2006 > 2025*, 6, 13.

[42] Jack D. Kem, *Campaign Planning : Tools of the Trade*, 2ND ED ed. (US ARMY COMM & STAFF COLL, 2006), 19.

[43] Ibid., 46.

[44] Ibid., 47.

[45] Thomas J. Goss and Naval Postgraduate School (U.S.). "Building a Contingency Menu : Using Capabilities-Based Planning for Homeland Defense and Homeland Security" (Naval Postgraduate School, 2005), 4-7.

[46] Canada. Treasury Board., *Integrated Risk Management Framework = Cadre De Gestion Intégrée Du Risque* ([Ottawa]: Treasury Board of Canada Secretariat, 2001).

[47] Glenn et al., *Scenarios*, 10.

[48] Ibid.

[49] Ibid.

Appendix B: Assumptions

Introduction

This Appendix summarizes and justifies the key assumptions used to compress the scenario driver matrix (see Appendix A) and support the general scenario development.

General Assumptions

The general assumptions are those that applied to all eight (including both state and non-state actor) scenarios.

US's Ability to Project Power Overseas

One of the main drivers affecting the scenario development was the "where will the US fight?" axis (see Appendix A, Figure A-2). The authors "answered" this question using two broad categories: on US soil or on foreign soil. Implicit in this choice of driver-pair was the assumption that the US would still be able to project power overseas if/when required. Admittedly, a major catastrophe, economic crash, change in national mood (to an isolationist period), disruption in the international arena that causes the US to lose its allies (and thus basing and/or overflight rights), or other severe discontinuity in the infrastructure that supports and permits US power projection could render this assumption null and void. However, based on the last 100 years of history, and the US's ability to project power almost at will, the authors deemed the probability of such a disruption to be remote. As a result, the authors judged the assumption that the US would be able to project power overseas to be valid.

US Military Will Fight as Part of an Ad-Hoc Coalition

When the US does wish to project its power overseas, it will do so as part of an ad-hoc coalition. It must surround itself with other like-minded allies to bring legitimacy to its actions.

Even though it is the world’s remaining superpower, the US cannot simply throw its weight around every time it wants to influence world events. To do so would be no different than the schoolyard bully picking on the smaller children. But, eventually, the smaller kids will band together and teach the schoolyard bully a lesson. The same occurs in international politics. If the US continually abuses its power and status, eventually the other nations will “gang up” on the US to counter its power. To avoid this outcome, “the United States always tries to get as many followers as possible, in order to avoid becoming a leader with no support, out there all alone.”[1] Such a coalition will endorse the action and prevent a large international backlash.

On the other hand, if the US happens to fall from power, it will still need to fight as part of a coalition. In this case, the US, by itself, would not have enough military power to accomplish its objectives. As a result, the US will build a team to help increase the overall military power available for the operation. A good example would be the Global War on Terror. Even though the US is currently a major world power, its military is still not large enough to fight Al-Qaeda simultaneously across the entire globe. “No one country has either the resources or the credibility to do the job alone. We need direct and long- term engagement by other major countries, including a credible multilateral military force, and we need it fast.”[2] The bottom line is that, independent of the amount of relative military power possessed by the United States, it will fight as part of an overall team effort.

When the US does employ its military forces, the allies that join the effort will not become involved due to traditional alliances; rather, they will join in the cause as part of an ad-hoc coalition. The term “ad-hoc” indicates that the team members will change from one crisis to the next. In the current “globalized” international arena, the players find themselves interconnected, intertwined and tangled in a web of various networks.[3] This web can amplify the impact of seemingly minute details, or make the outcome nearly impossible to predict. As a result, a state's allegiances may seem to shift from one crisis to the next, because the particulars for each crisis are slightly different. States will refrain from signing treaties that bind them into actions that may not always be in their best interests, and instead opt to join an ad-hoc coalition if and when they choose.[4] This phenomenon began with the first Gulf War and has been the modus operandi for international military operations since that time:

> "The appearance of the 'overnight' alliance brought an era to a close. That is, the age of fixed-form alliances which had begun with the signing of the military alliance between Germany and Austria-Hungary in 1879."[5]

The bottom line is that the US may be able to identify and work with several "standard" coalition partners (close allies that share many common interests), but in most cases the allies with which it finds itself operating will vary from one military operation to the next. As discussed in Appendix D, this raises several problems when dealing with capability development; it affects interoperability of equipment, training and tactics – every one of the three components required to create an effective capability.[6]

All Actors Will Have Access to State-of-the-Art Technologies

The authors assumed that, as actors develop new technologies, these technologies will proliferate to all actors nearly instantaneously. Traditionally, one may think that only technology "developers" will have sole access to state-of-the-art technology. This is because, traditionally, an actor wants to retain its competitive edge over others in the same field. This generally has been the case for both state and non-state actors. A state may not want to sell its top-of-the-line equipment to another state,[7] or a business wants to retain its edge in the marketplace. However, this axiom may no longer hold true.

Recent trends indicate that, at least in the case of state actors, developers are not waiting as long to proliferate their state-of-the-art technologies. For instance, during the 2003 war in Iraq, the Iraqis purchased top-of-the-line Russian Global Positioning System (GPS) jammers to counter the US's GPS-guided weapon systems.[8] The near-instantaneous spread of new technologies is most likely due to the increasing rate of technological development: in order to make money on a product before it becomes obsolete, a developer must sell the technology nearly immediately after it becomes operational. And there's no shortage of buyers. Anyone that has enough money can get their hands on the latest hardware: "The easy accomplishment of raising funds guarantees that [any actor] will be able to attain and master large amounts of high technology means."[9]

In any event, the authors wanted to bound the potential future threat space and ensure they addressed the worst-case scenario. And in the worst case, any actor can get its hands on any available technology. The authors dealt with any scenario-specific technology availability issues within each scenario.

All Actors Will Have Access To WMD

Similar to technology in general, all actors will have access to Weapons of Mass Destruction (WMD); the current rate of proliferation of nuclear weapons supports this assumption. The rate of proliferation has remained fairly constant over time (see Figure B-1).[10] There are two trend lines applied to the data in Figure B-1; the solid black line is a linear fit and the curved, dashed red line is a second-order polynomial. Mathematically, the polynomial is a better "fit" and shows the rate of increase slightly tapering off. However, this does not make intuitive sense for two reasons.

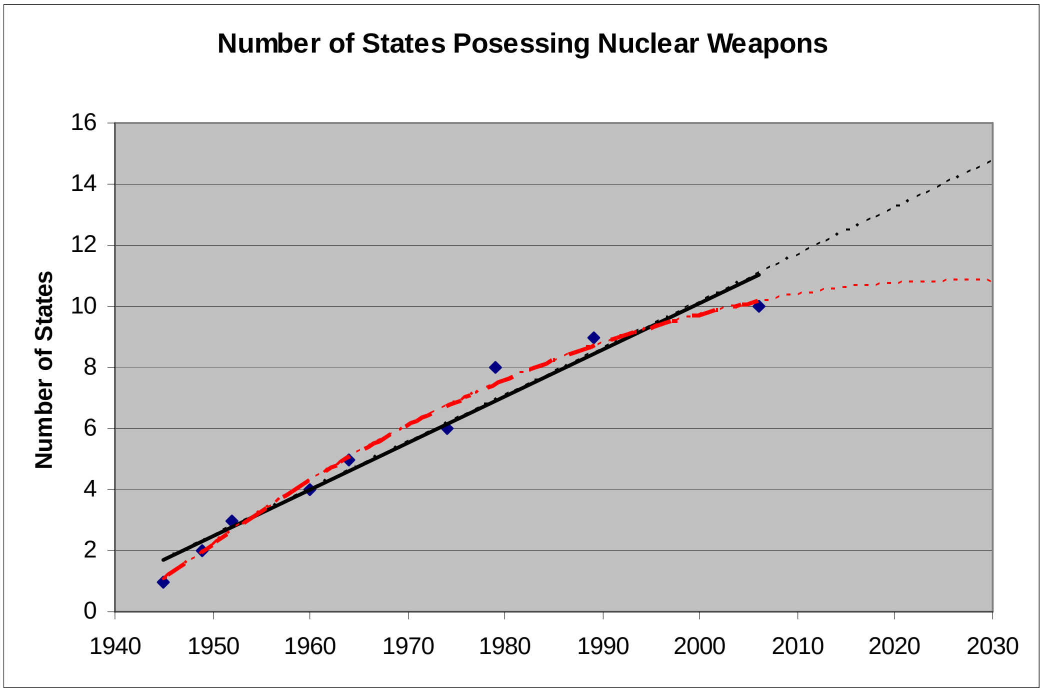

Figure B-7: Number of States Possessing Nuclear Weapons

First, the polynomial fit predicts only one more country acquiring nuclear weapons by 2025, yet several sources indicate Iran may possess the technology by 2010-2015,[11] and Saudi Arabia is also suspected of having a clandestine development program.[12] In addition, as more and more states acquire nuclear weapons, particularly "rogue" nations that repeatedly buck accepted norms of international conduct, the ability to monitor and control the spread of nuclear weapons will decrease. For instance,

> "Iran is already a major 'secondary proliferator' of weapons of mass destruction (WMD), and worse is still to come because its radical new president, Mahmoud Ahmadinejad, has publicly signaled his willingness to provide nuclear assistance to other Muslim states."[13]

As a result, one could expect the rate the technology spreads to other countries to increase, not taper off. Thus, the higher rate shown by the linear extrapolation shown in Figure B-1 may actually be more accurate (or possibly even conservative). In short, by 2025 one could thus reasonably predict that 11-14 states would possess nuclear weapons.

The second reason one could expect the rate of weapon proliferation to continue is that, as the number of states possessing nuclear weapons increases, it will become more difficult to control their spread. There is simply a higher probability that something will "slip through the cracks." This is one of the reasons that the rate of proliferation was relatively unaffected by the 1974 Nuclear Non-Proliferation Treaty (NPT). The inability of the NPT to stem the spread of nuclear weapons is also an indicator that the weapons will continue to spread despite diplomatic attempts to curb their proliferation.

This same logic also applies to chemical and biological weapons, which are generally easier to manufacture than nuclear weapons.[14] In addition to simply being easier to produce, the raw materials and equipment required are not nearly as exotic. Many of the chemicals required to manufacture chemical weapons are dual-use, with legitimate civilian applications.[15] Similarly, "[b]acteriological weapons can be produced in very small labs that are easy to hide″[16] because "the equipment required for most procedures is available since legitimate researchers require them as well."[17] As a result, the ability of a state to acquire chemical and biological weapons will surpass its ability to acquire nuclear weapons, and the number of states with chemical and biological weapons will continue to grow.

The above discussion has focused on the ability of a state actor to acquire WMD, but the same arguments apply to non-state actors. As more states, including potential "rogue" nations, acquire WMD, the probability increases that one of them could transfer the technology to a non-state actor.[18] And, unlike a state actor, the non-state actor is not as threatened by the US's military and other Instruments of Power (IOPs), so there is no deterrent that makes a non-state actor think twice about using WMD.

State Actor-Specific Assumptions

Catastrophic Attacks and US's ability to Respond in Kind

When dealing with a state actor and its potential employment of WMD (or any other method to create a catastrophic attack), the US currently possesses an effective deterrent – the "I know where you live and can hit you with a *very* big stick that will make you glow in the dark" factor. If another state were to severely threaten the US, the US could always respond with nuclear force. Thus, for most state actor scenarios, the authors assumed that, even though other states might have access to WMD, they will not employ these weapons directly against the United States. And this argument/assumption goes beyond simply deterring the use of WMD; it extends to another state's ability to inflict catastrophic damage against the US, independent of the means. That being said, there are two methods an adversary could use to negate this ability to respond in kind.

Another state may be able to negate the US's threat of massive retaliation by simply "hiding" its actions. If the US is attacked by someone, but it can't tell who the culprit is, the US won't have the ability to respond with overwhelming force. Examples of such an attack would be a coordinated Special Operations Forces (SOF)-type attack against points in the homeland (for example, simultaneous detonations of handheld "suitcase" nukes ala CBS's *Jericho* television show[19]), a cyberattack against key information systems, or possibly an attack against a space-based asset by an undetermined source. In all these cases, unless the US can find a way to prove definitively who attacked it, the principle of massive retaliation is worthless.

The other method to counter the massive retaliation principle is to develop a method to defend against/negate the US's nuclear arsenal. An example would be a "shield" to intercept incoming intercontinental ballistic missiles (ICBMs). However, the diversity in delivery options currently available to the US – ICBMs, submarine-launched missiles, and aircraft-launched cruise missiles[20] – seriously hampers an enemy's ability to counter effectively the entire US nuclear arsenal.

The bottom line is that, for all the state actor scenarios *except* for *The Phantom Menace*, the authors assumed that the US's nuclear arsenal would provide a deterrent against another state inflicting catastrophic damage on the US. In the case of *The Phantom Menace*, the adversary's ability to remain hidden removed this restriction.

Other States' Ability to Project Power onto the US Mainland

The final assumption made for the state actor scenarios was that, by 2025, no other state would have the ability to project military power onto the continental United States (CONUS). As a result, the authors were able to simplify the scenario driver matrix and assume that all state-vs-state military confrontations would take place on foreign soil (see Appendix A for further discussion).

At the current time, the two most likely candidates that would be in a position to project power onto CONUS are China and Russia. China poses the largest future threat to the US, but they still cannot project force for sustained combat operations.[21] China is currently increasing its military spending in an effort to modernize, and its programs *will* provide it with a regional power projection capability,[22] but the modernization program falls short of supporting large-scale expeditionary operations.[23] Russia's military power projection capability is in even worse shape. Russia is still attempting to recover from the collapse of the Soviet Union, and its trends in military spending and development are headed in the wrong direction to support major power projection efforts.[24]

While no other state would be able to project sustained combat power into the CONUS, this is not to say that another state could not threaten the US homeland. Inter-continental ballistic missiles (ICBMs) still pose a potential threat, as would a SOF-type attack with WMD. However, as discussed above, the US's own nuclear triad provides a deterrent to the ICBM threat. It also provides a lesser deterrent to the SOF attack, because there's always the chance of intercepting/capturing some of the SOF personnel and determining their country of origin. A SOF-style attack would also be extremely similar to a materials-based non-state actor attacking the US homeland using irregular tactics, a case covered in the *American Insurgency* scenario.[25]

The bottom line is that the authors deemed the threat of conventional forces operating on the US homeland to be negligible, and therefore made the assumption that conventional military conflicts between the US and other states will take place on foreign soil. However, before closing this subject, one should note the above discussion pertained solely to conventional military force power projection (deploying large numbers of forces into the CONUS).

Information technology, and cyberspace in particular, offers a means for an information-based adversary to project power into the US homeland without ever deploying a single troop. Granted, this is not "military" power projection in the traditional sense, but it is still important for two reasons. First and foremost, the USAF's new role as DoD's cyberspace lead assigns it responsibility for offensive and defensive cyberspace operations. And second, as Clausewitz stated, "War is thus an act of force to compel our enemy to do our will."[26] The opposite is also true: *any action taken to compel an enemy to our will could be considered by them to be an act of war*. Because actions taken in the cyber domain can affect the will of the general US population, they are thus acts of war, and the US should treat them as such. *The Phantom Menace* scenario discusses this situation in more detail.[27]

NonState Actor-Specific Assumptions

There were no nonstate actor assumptions applicable across multiple nonstate actor scenarios. The authors covered any assumptions pertaining to individual nonstate actor scenarios in those scenarios themselves.

NOTES

[1] Liang and Xiangsui, "Unrestricted Warfare," 184.

[2] John Kornblum, "Help Wanted in Iraq," *The Washington Post*, 27 June 2006, A.21.

[3] "Globalization" is "the process of establishing and developing interactive, multi-member networks that operate across transnational distances." Dr. Lewis Griffith, "Defining Globalization," (Maxwell AFB, AL: 2006), 3.

[4] Liang and Xiangsui, "Unrestricted Warfare," 62-65.

[5] Ibid., 64.

[6] Joel J. Luker, Maj., USAF, "State Actor Threats in 2025" (United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007), 4.

[7] Take, for example, the recent statements by the US that it will not export the F-22. Cameron Stewart, "US Rules out Deal on F-22," *The Australian*, 14 February 2007.; and James Dunnigan, "F-22 Secrets Too Precious to Sell," http://www.strategypage.com/dls/articles/2007227221547.asp.

[8] "CENTCOM, Pentagon Confirm Destruction of GPS Jamming Equipment," *Defense Daily* Vol.217, Iss. 57 (26 March 2003): 1.; and Frank Vizard, "Attempts to Jam U.S. GPS-Based Weapons and Navigation Systems in Iraq Were a Reminder of Just How Vulnerable the Technology Is " Scientific American.com, http://www.sciam.com/article.cfm?articleID=00079DD3-DAA0-1E96-8EA5809EC5880000.

[9] Liang and Xiangsui, "Unrestricted Warfare," 134.

[10]. Wikipedia.com, "List of States with Nuclear Weapons," http://en.wikipedia.org/wiki/List_of_states_with_nuclear_weapons. Also, the author should highlight that Figure B-1 does not account for the fact that South Africa voluntarily gave up/destroyed its existing nuclear weapons stockpile, the only known instance of this occurring. The author ignored this fact because it is irrelevant to the ability of a state to acquire nuclear weapons, and the rate that ability is changing.

[11] Sharon Squassoni, "Iran's Nuclear Program: Recent Developments," CRS Report for Congress (Library of Congress Congressional Research Service, 23 November 2005), CRS-4.; and International Crisis Group, "Iran: Is There a Way out of the Nuclear Impasse?," 24.

[12] Wikipedia.com, "List of States with Nuclear Weapons."

[13] Ilan Berman, "How to Eliminate Iran's Nuclear Weapons: A Symposium," The Claremont Institute, http://www.claremont.org/writings/crb/spring2006/symposium.html.

[14] Anne Marie Helmenstine, Ph.D., "Chemical Weapons and Warfare Agents," About.com, http://chemistry.about.com/cs/chemicalweapons/a/aa040303a.htm.

[15] George J. Church, "Disarmament: How to Hide an A-Bomb," *Time* 08 July 1991, 40.

[16] Ibid.

[17] Federation of American Scientists, "Introduction to Biological Weapons: Biological Weapons Production," FAS.org, http://www.fas.org/biosecurity/resource/bioweapons.htm.

[18] George H. W. Bush, "National Strategy for Combating Terrorism," (2003), 9-10.; and Warrick, "Custom-Built Pathogens Raise Bioterror Fears," A.1.

NOTES (Continued)

[19] In the *Jericho* TV show, the US is hit with about 20-30 simultaneous nuclear weapons detonations all across the country. The weapons were smuggled into the country and then detonated.

[20] Jim Garamone, "Review Changes Status of Nuclear Deterrent," *Pentagon Brief* (January 2002): 7.

[21] United States. Dept. of Defense. Office of the Secretary of Defense, "Annual Report to Congress: Military Power of the People's Republic of China (2006)," (2006), I.

[22] Ibid., 10-11.

[23] Ibid., 30.

[24] Dr. Marcel de Haas, "'Russia's Military Strategy: Preparing for the Wrong War?," Power and Interest News Report (PINR), http://www.pinr.com/report.php?ac=view_report&report_id=478&language_id=1.

[25] Myers, "Non-State Actor Threats in 2025".

[26] von Clausewitz, *On War*, 75.

[27] Luker, "State Actor Threats in 2025", 26-30.

Appendix C: Comparison to Key QDR Planning Areas

Introduction

The 2006 Quadrennial Defense Review (QDR) identified four "priority areas" and three "Force Planning Construct Objective Areas" to focus DoD planning and investment strategies.[1,2] The Blue Horizons (BH) team compared its eight scenarios to these planning areas to ensure they (the scenarios) adequately addressed the QDR's concerns.

Comparison to QDR Priority Areas

The 2006 QDR defined four "Priority Areas:" Irregular Challenges, Catastrophic Challenges, Disruptive Challenges and Traditional Challenges. The BH team qualitatively assessed each of the eight scenarios for its applicability to each of the four Priority Areas. Figure C-1 graphically depicts how the State Actor Scenarios relate to each of the four areas; Figure C-2 does the same for the Non-State Actor Scenarios.

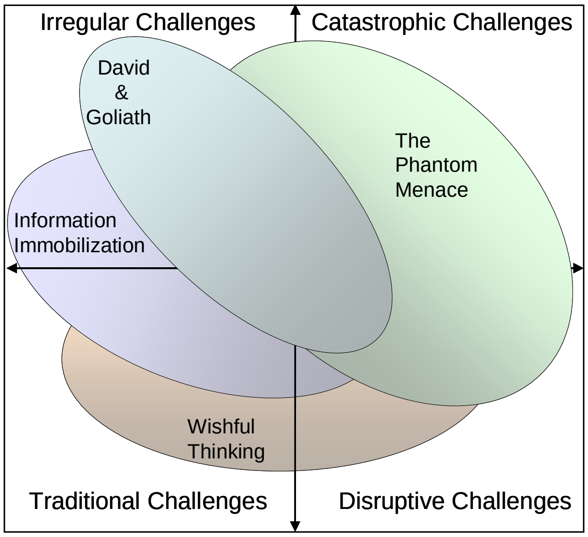

Figure C-8: State Actor Scenario Comparison to QDR Priority Areas

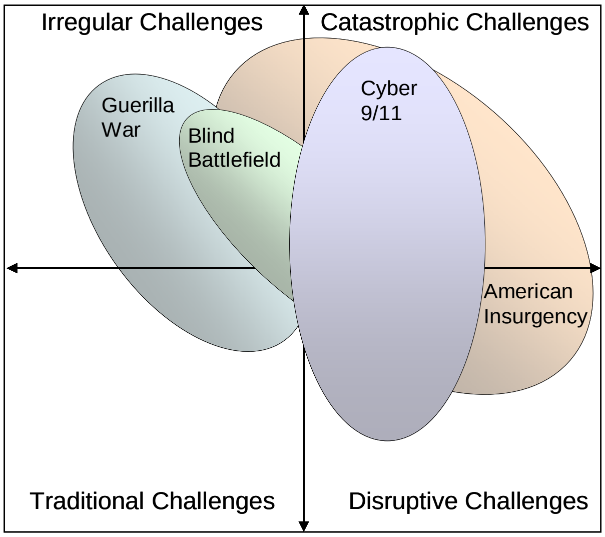

Figure C-9: Non-State Actor Scenario Comparison to QDR Priority Areas

Comparison to Force Planning Construct Objective Areas

In addition to the Priority Areas discussed above, the 2006 QDR also defined three "Force Planning Construct Objective Areas." Table C-4 below shows how the eight scenarios developed by the BH team addressed the Objective Areas of Homeland Defense, Conventional Conflicts and Irregular Conflicts. As shown by Table C-4, the scenarios provided coverage for all three Objective Areas.

Table C-4: Scenario Comparison to 2006 QDR Force Planning Construct Objective Areas

Scenario	Homeland Defense	Conventional Conflicts	Irregular Conflicts
1. Wishful Thinking		✓	
2. Information Immobilization		✓	
3. David & Goliath			✓
4. The Phantom Menace	✓		✓
5. American Insurgency	✓		✓
6. Guerrilla War			✓
7. Blind Battlefield			✓
8. Cyber 9/11	✓		✓

NOTES

[1] United States. Dept. of Defense. Secretary of Defense., *2006 Quadrennial Defense Review*, 19.

[2] Ibid., 36.

Appendix D: Implications

Introduction

The scenarios developed in the main body of the paper implied several requirements for future USAF Research and Development (R&D) efforts. The sections below provide a basic outline of these implications. By no means should the reader consider the analysis herein to be an absolute comprehensive list of future requirements; it merely provided the most obvious implications as a starting point for future discussion. Therefore, the final section included several topics the author felt were ripe for follow-on analysis.

Implications Derived from the Assumptions

Rate of Technological Change and Implications for Defense Acquisition

Improvements in technology will continue at the current rate, if not increase;[1] this will have a profound effect on the way the USAF, and DoD in general, acquires weapons systems. Specifically, it means that, if current policies and practices remain unchanged, weapons systems can become obsolete before they become operational.

For probably the first time in history, radical advances in militarily-applicable technology are occurring within one "generation" of military hardware development. For instance, the F-22 has been in development since the mid-1980s. During that time, according to Moore's law (which says that computer processing speed doubles about every 2 years), computers today are 2^{10} (1000) times as fast! Computer memory has also increased at this rate, and the cost has dropped as well.[2] Most notably, today's personal computers have a processing capability that rivals 1980's-era supercomputers, and this computing power is available across the globe. In short, the computers originally designed for the F-22 would be considered obsolete today. The long development timelines also provide US adversaries with the opportunity to counter the technology before the USAF fields the system. For instance, in 1989 the chief scientist of the Air Force stated that a "thousand-fold" increase in computer processing power could enable counter-stealth capabilities.[3] Well, according to Moore's law, we're there now, and the F-22 is just coming online. This increase in processing power is actual fact, too, not just a prediction by Moore's law. F-22 development started in the mid-1980's; since that time, microprocessor speeds have increased ~1,000 times, from 6×10^6 to 6×10^9 calculations per second, and processor performance has increased even more drastically, from 2 to 10,000 MIPS (millions of instructions carried out per second).[4] The tremendous R&D investment that went into the F-22's development could soon be rendered null and void: "With progress being made on counter-stealth technologies, the question… is whether stealth will guarantee survivability for the lifetime of the aircraft."[5] This is partly due to the faster rate of technological change, but it is also due to the longer development time cycles for military weapons systems.

To truly maintain an edge in future warfare, the US must reduce its timelines for major weapons system development. With the rate of technological change growing exponentially, one would also want to see a corresponding reduction in acquisition timelines to maintain pace and ensure the ability to employ "the latest and greatest" technologies on the battlefield. Obviously, there's a physical limit to how quickly one can acquire and field a new weapon system, but the goal should be to maintain, if not reduce, that timeframe. However, in the US acquisition system, the opposite is true: acquisition timeframes are *growing*; and to make matters even worse, the rate of growth is exponential. For example, see Figure D-1, which shows how major strike aircraft acquisition times have increased throughout the years.[6] The result will be an ever-widening gap between the state-of-the-art technologies that are commercially available, and those that the USAF employs on the battlefield. And any enemy that can react quicker will be

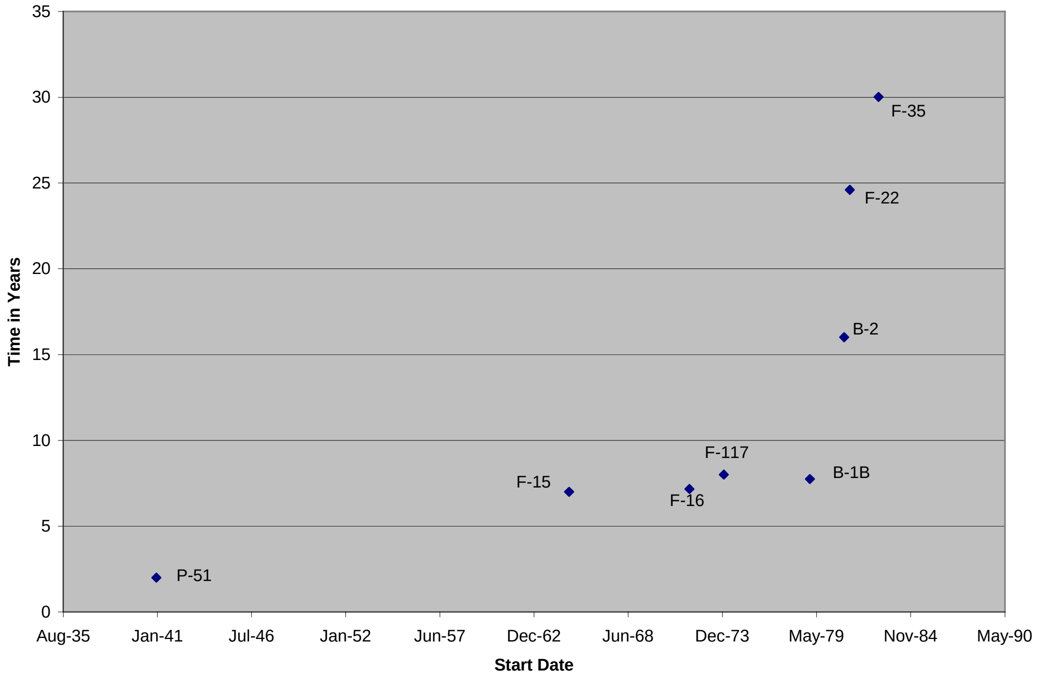

Figure D-10: Major Strike Aircraft Acquisition Times

able to field a superior system. In essence, similar to the concept of decision superiority, the enemy will be able to get inside the US's "acquisition loop." The USAF cannot control the rate of technology advancement, so it must take steps to control the one thing it can: its acquisition policies.

A key component to reduce its acquisition timelines is to get rid of the outmoded concept of a "flyoff" between two competing systems. The USAF originally adopted this technique as a way to reduce overall acquisition risk and reduce cost to the taxpayer. And it made sense in a time when the acquisition cycle was shorter than the technology development cycle. However, with technology advancing at its current pace, the USAF can no longer afford to take this extra time. The technical risk reduction is offset by the reduced timeframe in which the fielded system will be effective before an enemy is able to counter the system's capabilities.

Effective Coalition Warfare

When the USAF goes to war in 2025, it will do so as part of an ad-hoc coalition; to do so effectively will be extremely difficult. The coalition partners, with presumably less-capable systems, will find themselves relegated to "lesser" roles. For instance, gaps were already evident as early as 1999: "Allied Force showed how far apart U.S. and coalition partners had grown since the end of the cold war in capabilities and interoperability."[7] And that gap was primarily between US and NATO forces, which had the benefit of a 50-year old alliance. The disparity in capabilities existing between forces in an ad-hoc coalition will be even greater.

Future artificial intelligence (AI) systems may help alleviate some of these disparities, at least in terms of allowing coalition members to share data over a common network. Currently, systems share data over a network by sending messages that adhere to a very strict set of rules: "bit 3 of word 2 will state the number of targets," and so forth. These rigid guidelines make it difficult for developers to incorporate a new system into the network and ensure it is passing the proper data at the proper times. Advanced AI systems will make it easier to "plug" a new system into the network. For instance, when two people are communicating, "the red apple is larger than the green grape" means the same thing as "the grape, which is green, is smaller than the apple, which is red." The data structures are no where near the same, yet the two people are able to understand one another. AI systems will be able to perform this type of interpretation between networked data systems. For instance, one computer could ask another, "Hey, do you see a target at these coordinates?" The other would reply, "Yes, I think it's an airliner." And it may reply in French. Or Russian. Or German. The bottom line is that the two computers would understand one another and could share data without having to both conform to the same set of rigorous standards. The result (assuming all the players have these advanced, translating network gateways) will be a more-effective ad-hoc coalition that can all contribute to the net-centric operations.

Scenario 1. Wishful Thinking: Regular Warfare Against a Materials-Based Adversary

The *Wishful Thinking* scenario created a number of associated implications. The good news was, since this was the type of conflict the USAF generally wanted to equip itself to fight, the USAF leadership were already discussing a large number of these issues.

In the space arena, the USAF must prepare itself to operate in a conflict where the enemy is attacking, disrupting and/or destroying the US's satellite-based systems. This raises a number of issues: first, the USAF must develop an effective method to determine if a satellite is under attack; and, if so, how it's getting attacked, and by who (so the US can later retaliate in kind). According to USAF Lt. Gen. C. Robert Kehler, deputy commander of the U.S. Strategic Command,

> "The No. 1 thing we need to do is improve our space situational awareness," Kehler said. The United States must comprehend "who's on orbit, and what are they doing there," he said. If something unusual occurs, the United States must be able to determine whether it is a harmless anomaly, or whether it is "a hostile attack" on an American satellite.[8]

Improving its ability to determine who is attacking US satellites should provide some form of deterrent to make other states think twice about launching an attack. But, assuming the deterrent fails, the US must have in place satellites that can maneuver to avoid an attack and redundant systems to mitigate the effects of a downed satellite. And if these measures prove inadequate, the USAF must also be able to rapidly replace any disabled satellites while being able to operate effectively without the capabilities those satellites normally provide. In short, for the first time in its history (excluding a brief period in the late 1950's immediately after the Soviet Union launched a little satellite named *Sputnik*), the USAF may have difficulty maintaining its superiority in space.

The USAF may also find it difficult to maintain its superiority in the air. The *Wishful Thinking* adversary's counter-stealth capabilities, its DE-based IADS and its ability to employ its own stealthy micro UAVs against US troops all make the attainment of air superiority extremely challenging, if not impossible. To improve its chances of doing so, the USAF must develop its own DE systems – not only to improve its own offensive capabilities and air defenses, but to learn how to counter the enemy's DE weapons and nullify the enemy's capabilities. Finally, the USAF must also take measures to improve the airspace control and coordination of friendly UAVs, so the air defense commander can discriminate between friendly and enemy forces.

Scenario 2. Information Immobilization: Regular Warfare Against an Information-Based Adversary

The primary implication from the *Information Immobilization* scenario was that effective computer security systems will be paramount to mitigate the effects of a cyberattack. All offensive cyberattack methods described in the main paper, except for a DOS attack, required the attacker to gain some sort of access to the target computer system. This is not as difficult as it sounds, for "[s]ome entity within the cyber world has the authority, access, or ability to perform any action an attacker desires to perform. The attacker's goal is to assume the identity of that entity, in some fashion."[9] Thus, data encryption methods and username/password schemes become the key to an effective defense.

Assuming that the *Information Immobilization* enemy breaches the initial cyber defense, the USAF must take steps to mitigate the ensuing damage; the anti-virus capabilities in nature provide a good model to do so effectively. First, the USAF must develop and field AI systems that continually monitor the network traffic, search for viruses and suspicious traffic, and automatically take actions to contain the virus. Such a system would mimic the antibodies found in the human body. Second, the USAF must adjust some of its policies to improve the network's susceptibility to a virus. In particular, the push towards the "Standard Desktop Configuration" (SDC) is, in the author's opinion, a huge mistake. One of the "tools" nature uses to slow the spread of a virus is genetic diversity; when all the plants or animals are genetic copies of one another, a single malady can run rampant through the entire population without meeting any resistance. The world banana population is currently facing such a crisis; bananas are essentially genetic copies of one another, and currently a virus is spreading worldwide, threatening to make the banana, as we know it, extinct.[10] In a similar manner, forcing all the USAF's computers to have essentially the same configuration (this is the intent of the SDC) means that all the computers have the same vulnerabilities. As a result, a virus that's effective on one machine can quickly spread through the entire network with devastating effects. Thus, the CDC program, while it's meant to improve overall computer security, may in fact be opening up the network to a catastrophic collapse.

While the USAF works to improve its own computer security, it must also work with the defense industry to simultaneously improve the defense industry's computer security as well. This requirement stems from two areas of USAF-industry interaction. Most obvious is the defense industry's need to protect R&D/proprietary information from prying eyes. Less obvious is the production and distribution of USAF/DoD supplies. If an adversary can hack in and disrupt a company's record-keeping systems (orders, production schedules, financial transaction records, etc.) it could adversely impact the USAF's logistic supply chain. The result will be pandemonium on the battlefield. Thus, to negate this outcome, the USAF must also hold its defense industry partners to the same standards of cyber security.

The outcome that led to the *Information Immobilization* scenario's name provides the basis for the final major implication from this scenario. US leaders, political and military alike, will, by 2025, be used to having a constant influx of information upon which to base their decisions. These leaders must be trained to operate just as effectively in a situation where that information pipeline is cut off; they must relearn how to deal with the fog of war.

Scenario 3. David and Goliath: Irregular Warfare Against a Materials-Based Adversary

The D&G scenario is essentially a low-intensity conflict (LIC) -- at least, it's low-intensity from the US's point of view. In addition, the state actor against which the US is fighting has chosen to fight in an irregular manner; as a result, the US must adapt its capabilities (equipment, doctrine and training) to counter the irregular warfare campaign. The resulting implications are similar to those found in the *Guerrillas in the Mist* non-state actor scenario, with a few minor differences.

In terms of equipment required to fight an irregular battle, the largest requirement is persistent surveillance. By definition, irregular battle has no set form; as a result, timely, accurate intelligence provides the key to anticipating the adversary's actions.[11] This persistent surveillance must be effective 24/7/365, in any terrain – urban, mountainous, jungle, etc. It must be able to track the *D&G* fighters as they attack US forces, then blend back in to the general population. It must be able to back-track and see where they came from, or track them forward in time to see where they went after the attack. In short, the US needs an "unblinking eye" over the battlefield.[12] Aerial platforms may provide some of the intelligence data streams, but most would come from sensors that aircraft disperse (airdrop) throughout the operating area. These sensors will then transmit and relay their data back to the Combined Air Operations Center (CAOC).

Collecting and processing this vast amount of data will require advanced AI systems. There would be too many data streams simultaneously entering the CAOC for personnel to monitor and respond to real-time. The AI systems will scan the data streams and determine if there’s anything “interesting” to display to their human users. This is similar to the adversary’s capabilities laid out in the *Information Immobilization* scenario. However, ultimately the US would want to take the capability one step further, and use the AI systems to help predict, as opposed to simply track and report, on the adversary’s actions.

In addition to this increased intelligence requirement, battlefield medical care will become a major concern in the *D&G* scenario. Recall that the *D&G* adversary will arm its general population with small, lethal weapons in an effort to drive up the US casualty count. This implies the US forces will need improved medical care to deal with the increased destructive power (and corresponding increased amount of damage to wounded personnel) found in the *D&G* state’s weapons. In addition, Directed Energy (DE) weapons open up a whole new area of study for medical treatment. Battlefield medics must be able to quickly diagnose what type of DE weapon the *D&G* adversary used, what internal injuries it may have caused (there may be no exterior damage to the patient) and what type of treatment to administer.

In addition to improving its medical diagnostic and treatment (equipment-based) capabilities described above, the US military medical system must also maintain its skills and doctrine required to deal with a mass-casualty conflict. In particular, many of the aeromedical “success” stories currently coming out of the Iraq conflict describe the tailored response given to soldiers injured on the battlefield – how the medivac system can get that one patient flown wherever he needs to go, when he needs to get there, to deliver him to the required treatment center. By 2025, that sort of tailored medivac response may be the norm. However, tailoring the medivac response will not be possible when there are mass casualties on the battlefield. The medivac system, while still being agile enough to provide these tailored treatment options when able, must also be ready to deal with a mass-casualty conflict.

Finally, the USAF must also work to improve its training and doctrine for LICs in general. This is somewhat outside the purview of the BH program, so is just briefly touched upon here. But, recall that training and doctrine are two of the three components required to create an effective capability,[13] so one must discuss them as well to truly discuss how to improve US capabilities for the future.

In terms of doctrine, the USAF has a strong history of the "strategic bombardment" doctrine dating back to the days of Trenchard, Douhet and Mitchell.[14] Their vision of airpower application was extremely brutal: "once action has begun, both should keep in action incessantly and with the utmost violence."[15] These ideas directly led to the massive destruction that allied air power inflicted on Germany and Japan during World War II. This concept of strategic attack still pervades the USAF's doctrine.[16] Yet, how does one execute "strategic attack" against a state like the *D&G* adversary who has dispersed its forces, and whose infrastructure we may not want to destroy so we do not have to rebuild it after the combat operations are complete? These are not new lessons. History has shown that firepower applied "with the utmost violence" is not effective in LIC – while airpower *can* provide effective fire support for ground troops, the counterinsurgency fighter must limit his application of this fire support.[17] Razing an entire village does not help to win the "hearts and minds" of the villagers. Air Force planners understand this and account for issues like collateral damage to non-military targets on a daily basis, in both regular and irregular conflicts. However, the USAF still has not codified these lessons into formal doctrine for employing airpower in LIC.[18]

This lack of doctrine also translates into a lack of LIC training for USAF operators. For instance, the author was personally involved with the developmental testing of the Small Diameter Bomb (SDB). The SDB's smaller size and associated reduction in collateral damage was one of the main selling points that sped the weapon's development. Yet one of the operators involved with the test program actually said, "We don't need this thing… you know, I've never been in a planning cell where they said, 'You know what we need? A *smaller* bomb!!'" But a precise, low-collateral-damage weapon is exactly what an Air Force needs in LIC. The operator's lack of understanding of this requirement indicates the USAF's failure to train properly its personnel in LIC theory and operations. Until the USAF does so, it will not be able to prosecute effectively any sort of sustained, effective LIC campaign. Essentially, it will concede defeat to the *D&G* adversary before the conflict has even begun.

Scenario 4. The Phantom Menace: Irregular Warfare Against an Information-Based Adversary

In *The Phantom Menace* scenario, the largest question for the USAF is, "who is responsible to protect civilian and non-USAF computer systems from cyberattack?" In the case of the civilian systems, the 2003 US National Strategy to Secure Cyberspace delegates this responsibility to the private sector.[19] However, in 2005 the USAF became DoD's lead for defending cyberspace.[20] Just as the USAF is responsible for defending the airspace over private companies and citizens, is it now also charged with defending the cyberspace those entities use?

If the USAF must now defend other organizations' cyberspace, it creates a number of policy questions that the USAF must address. Does this responsibility also give the USAF the right to tap into and monitor or test civilian network security? If the USAF is given the requirement to determine the required security measures to be put in place by a non-USAF organization (civilian or otherwise), who funds the implementation of those measures, and who monitors their implementation by the private companies? And, if attacked, how will the US respond – with a cyber or physical attack?[21] These are all policy decisions the US civilian leadership must yet clarify.

Even while it is waiting for the US civilian leadership to clarify these policies, the USAF, as DoD's cyber warfare lead, must begin to develop its capabilities for cyber defense. Recall the basic capability triad: methods, equipment and skills. The USAF must work with other US agencies to develop, exercise and, if necessary, implement methods for dealing with cyberattacks. "These include anticipation and assessment, preventive or deterrent measures, defensive measures and measures for damage mitigation and reconstitution."[22] In terms of its "equipment," the USAF must also begin to fund cyberspace defense research, similar to the way it funds 6.1 basic research for airplane systems (basic propulsion, aerodynamics, etc.). Emerging concepts include quantum encryption methods and adaptive networks that self-identify and quarantine new/emerging viruses.[23] However, above all, the USAF must develop its people, particularly in the area of cyber forensics. It must create a cadre of experts who are able to quickly track a cyber attack back to its source and remove the veil of secrecy surrounding *The Phantom Menace*. Doing so will eliminate *The Phantom Menace's* ability to operate without fear of reprisal, thus reducing – if not eliminating – the risk of it attacking the US.

Areas for Future Research and Discussion

Overall, the authors felt the eight scenarios developed by the BH team adequately described the 2025 threat space. However, (as always in any research project), time constraints prevented them from delving into a number of "what if" scenarios that could strengthen the overall description of the future threat space. The sections below detail some of these areas, and the authors' suggestions for future research and discussion.

Synergistic Effects: Intersection of Multiple Scenarios

While the scenarios described in the study adequately bounded the threat space, each scenario in and of itself represented an extreme. In reality, the adversary will fall somewhere in the middle of the spectrum, and the lines between the various scenarios (and the associated adversarial capabilities) will become blurred. Synergistic effects between the various scenarios could have a profound impact on the adversary's capabilities, and thus the context in which the US forces will operate.

This idea of "combining" effects from multiple capabilities – both military and non-military alike – will be critical to success in future warfare. "He who wants to win today's wars, or those of tomorrow, to have victory firmly in his grasp, must 'combine' all of the resources of war which he has at his disposal and use them as means to prosecute the war."[24] For example, by 2025 there will be several methods adversaries could use to counter the USAF's stealth technology. The *Wishful Thinking* state had multi-spectral sensors, and the *Information Immobilization* state created essentially the same capability using networked systems and advanced processing software. In reality, the most "potent mix" would be a combination of these capabilities – "radars in multiple bands, massive computing power in small packages and innovative algorithms for sorting through huge amounts of data."[25] Thus, as mentioned in the main body of the paper, the intersection of the scenarios, where an adversary can create synergistic effects by combining capabilities, may actually represent the most dangerous region of the threat space. Examining this intersection and analyzing the resultant capabilities would prove to be beneficial, but the authors simply did not have enough time to do so during the current study.

The Effects of Invalid Assumptions

The authors made a number of assumptions to develop, and then cull down, the matrix of scenario drivers, as well as build the scenarios themselves (see Appendices A & B). An interesting exercise would be to challenge these assumptions and determine the impact on the overall threat space if the assumptions proved invalid. In particular,

- If the US was hit by a catastrophic event that essentially wiped out its ability to project military power (i.e., the conflicts against state actors were now occurring on US soil instead of foreign land), how would the scenarios change, as the US focused on homeland defense?
- If China, Russia or possibly India developed the capability to project military power for sustained combat operations, how would that affect the scenarios? Once again, as above, the US might now have to focus on homeland defense, but would do so while retaining the ability to project power if/when required. What would this mean in terms of capabilities the US or its adversary should develop?
- Most importantly, what happens if an adversary developed an effective countermeasure to the US nuclear arsenal? For instance, a force field, controlled black hole or other sort of energy sponge that could block or soak up the energy released in the explosion?[26] Many of the state-adversary scenarios relied heavily on

the assumption that the US nuclear arsenal would deter other states from inflicting catastrophic damage on the US. What happens if this assumption is no longer valid?

Again, while answering the above questions and analyzing their impact on the threat space could prove valuable, the authors left completion of this task to the myriad of futures researchers who will follow us… well, sometime in the future.

NOTES

[1] See Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*.

[2] Ibid.

[3] D. F. Bond, "Radar Networks, Computing Advances Seem as Keys to Counter Stealth Technologies. (Cover Story)," *Aviation Week & Space Technology* 131, no. 23 (1989): 41.

[4] Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*, 61, 64.

[5] Bill Sweetman, "Worth the Cost?," *Jane's Defence Weekly* 43, no. 29 (2006): 63.

[6] Many thanks to Maj James Lake, who compiled the data for Figure D-1 from various sources. James P. Lake, Maj., USAF, Email, 05 September 2006.

[7] Johnson, "Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era," 166.

[8] Ahearn, "U.S. Military, Commercial Space Assets Vulnerable to Attack: Experts," 1.

[9] Parks and Duggan, "Principles of Cyber-Warfare", 124.

[10] Dan Koeppel, "Can This Fruit Be Saved?," *Popular Science* August 2005, 60-67.

[11] Eliot Cohen et al., "Principles, Imperatives, and Paradoxes of Counterinsurgency," *Military Review* 86, no. 2 (2006): 50.

[12] Headquarters Department of the Army and Headquarters Marine Corps Combat Development Command, "Field Manual (FM) 3-24 and Marine Corps Warfighting Publication (MCWP) 3-33.5: Counterinsurgency," (Department of the Army and Department of the Navy, December 2006), E-2.

[13] See Eq. 1 in Luker, "State Actor Threats in 2025", 4.

[14] Hurley, *Billy Mitchell: Crusader for Air Power*, 25-26, 28, 43-44.; also Giulio Douhet, General, "The Command of the Air," in *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, ed. Sharon McBride (Maxwell AFB, AL: Air Command and Staff College, 2007; reprint, from *The Impact of Air Power: National Security and World Politics*, Chapter 29. D. Van Nostrand Co., Inc., 1959. Originally published as a stand-alone work, *The Command of the Air*, in 1921.), 3, 7.

[15] Douhet, "The Command of the Air," 3.

[16] United States. Dept. of the Air Force. Secretary of the Air Force., *Air Force Doctrine Document (AFDD) 1: Air Force Basic Doctrine*, 40-41.

[17] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 343-44, 94.

[18] Beebe, "The Air Force's Missing Doctrine."; and Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 4.

[19] Bush, "The National Security Strategy to Secure Cyberspace," ix.

[20] Michael W. Wynne, Secretary of the Air Force, "Cyberspace as a Domain in Which the Air Force Flies and Fights" (paper presented at the C4ISR Integration Conference, Crystal City, VA, 02 November 2006).

NOTES (Continued)

[21] Shimeall, Williams, and Dunlevy, "Countering Cyber War," 18.

[22] Ibid.

[23] Dan Tynan, "The Internet Is Sick...But We Can Make It Better," *Popular Science*, October 2006, 82.

[24] Liang and Xiangsui, "Unrestricted Warfare," 181.

[25] Fulghum, "New Radars Peel Veil from Hidden Targets," 58.

[26] While a “controlled black hole is feasible (see Rena Marie Pacella, "Man-Made Black Holes," *Popular Science* January 2006.), it would be highly unlikely in a military application – at least by 2025. The equipment required to generate even a miniscule black hole is massive – in both size and cost.

Appendix I: *Wishful Thinking* Capability Development

Step 1: Identify the Adversary's Strategic Objectives

The *Wishful Thinking* state will attempt to defeat the US by routing the US forces on the battlefield while eroding the will of the US populace to support US military actions. Table I-5 summarizes these strategic objectives, as well as the associated operational objectives for the *Wishful Thinking* adversary.

Table I-5: Wishful Thinking State's Objectives

Strategic Objectives	Operational Objectives
1. Defeat US Fielded Forces	Neutralize US Space Power
	Neutralize US Air Power
	Prevent Escalation To Nuclear War
2. Erode Will of US Populace to support US military actions	Inflict Maximum Number of US Casualties
	Achieve as many gains as possible early on, then hold while conflict drags out and casualties mount

Step 2: Identify the Centers of Gravity (COGs) to Achieve Strategic Objectives

To achieve its strategic objectives, the *Wishful Thinking* state will attempt to fight the US military in a regular conflict. For the USAF, this means the *Wishful Thinking* adversary will attack its space power, air power and its people.

Steps 3-5: COG Analysis

For each COG, the author identified operational objectives, logical lines of operation, critical capabilities, critical requirements, and critical vulnerabilities (step 3); he then identified decisive points for each critical vulnerability (step 4), as well as capabilities that could affect the decisive points (step 5). Tables I-2 to I-5 provide the details for how the *Wishful Thinking* state could attack the USAF's space power, air power and people, respectively.

Table I-6: Wishful Thinking COG Analysis (How to Attack US Space Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General (all sats)	Satellite Existence	Anti-Sat Attack	Kinetic Kill From Non Space-Based ASAT Wpn
			DE kill
			Attach nanobots to sat that "eat" it (turn it in to grey goo… eliminates "space debris" issue)
	Space-to-Ground Data Links	Prevent User from Receiving Signal	Jam satcom in AOR
			Block sat txmtr (microsats)
			Knock sat out of alignment so txmtr pointed wrong way
			Physically destroy/harm txmtr (DE/kinetics/nano)
		Spoof DL or alter signal	Duplicate H/W, feed in false data (e.g., Chechens v Russia)
			More elegant methods potentially very difficult. Directional antennae/sig processing mean would have to be done near sat location… microsats/ nanobots?
	Ground-to-Space Control Links	Prevent Sat from Receiving Control Signal	Jam control signal (difficult… originates outside AOR)
			Block sat rcvr (microsats)
			Knock sat out of alignment so rcvr pointed wrong way
			Physically destroy/harm rcvr (DE or kinetics)
		Destroy Ground Station	Not in AOR; no power projection; would be SOF or cyberattack

Table I-6: Wishful Thinking COG Analysis (How to Attack US Space Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Spoof Control Link (send bogus control info)	Again, difficult. Would need to intercept sig & re-txmt along same directional path… microsats/nanobots? If can do this, would be much easier just to block sig.
ISR & Early Warning	Able to see/sense enemy (ISR)	Blind/Destroy/Disrupt Sensor	Laser/DE to physically damage sensors
			Surround w/ microsats & get in its way
		CCD &/or Spoof Sensor	Surround w/ microsats & provide false data
			Nanobots that provide false signatures (hide or decoy)
	Positioning Data (know location of pic)	Move Satellite	Bump w/ microsat
			Nanoparticles or microsat attach to sat, build up mass, change angular rotation, handling
		Spoof Positioning Info	VERY difficult
	C2 (for EW systems)	Orient phase of OODA loop (figure out what's happening)	Overwhelm w/ decoys/ false data
Comm	Satellite Relays	Jam/Block Sat-to-Sat Comm	Microsats to surround sats/block comm txmtr/rcvrs
		Knock Sat out of position	Bump w/ microsat
			Microsat attach to sat, change rotation/handling
	Bandwidth	Fill with unwanted/bogus data	Denial of Service Attack -- duplicate H/W, "spam" sys w/ false txmsns
Weather	Able to See/Measure WX	Blind Sensors	Laser/DE to physically damage sensors
			Surround w/ microsats & get in its way
		Knock Sat out of Position	Bump w/ microsat

Table I-6: Wishful Thinking COG Analysis (How to Attack US Space Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
			Microsat attach to sat, change rotation/handling
GPS	Know where satellite is	Knock Sat out of Position	Bump w/ microsat
			Microsat attach to sat, change rotation/handling
	Timing	Disrupt Timing Sync	DE wpn to speed up/slow down crystal vibrations, disrupt timing

Table I-7: Wishful Thinking COG Analysis (How to Attack US Air Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General	Defeat IADS	Ground-Based Air Defenses (G/A attack)	Laser/DE weapons to minimize reaction time
			Handheld SAMs (minimized by high-alt PGM releases, but what happens if those are negated?)
			Mobile Launchers
		Inability to down all Acft	Small, stealthy UAVs
	Engines/Airframe Operation	Screw up Fuel/Air Mixture	Nanoparticles to alter fuel/air mixture?
			EMP to fry circuits (low prob, unless attack at staging base; need to know where is; if over adversary territory, too much risk of fratricide)
		FOD	Disperse cloud of nanoparticles to "gum up" or "eat" engines (nano flak); would require ctrl mech to prevent fratricide
UAVs	Control Links	Jamming	Difficult if relayed through satellite

Table I-7: Wishful Thinking COG Analysis (How to Attack US Air Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Spoofing	Difficult; most likely relayed through Sat, so would be like spoofing satcom (see Space page)
	Data Processors (guidance/ stability)	EMP	Adversaries systems must be hardened to minimize fratricide
Stealth	Optimized for portion of EM or audio spectrum	Multi-Spectral Sensors	Self-explanatory
	Stealth Coatings	"Stick" something to aircraft to light it up	Disperse clouds of nanoparticles that will stick to aircraft and make it visible (low prob… need to know where acft is 1st to target it…)
Airborne ISR	Sensors (Locate Target)	Blind Sensor	Similar to anti- Space ISR, w/o anti-sat capes
		Spoof Sensor	
	Determine Target Location	Interfere w/ platform's location data	Mess up GPS… see below
Precision A/G Weapons	ALL	Electronic Fuzes	Use EM field around critical defensive points to initiate fuze prematurely or disarm it
		Guidance/Control	Ditto, but to disrupt guidance sys
	GPS	Signal Reception	See Space Page for Satellite Datalink Reception
	Laser Guidance Systems	Laser Spot Location	Counter laser to pull wpn off tgt
	EO Systems	Spoof sensors	CCD -- difficult to disguise everything all the time
		Wpn relay back to acft	Jam (difficult; need to know where both acft & wpn are, wpn type, etc)

Table I-7: Wishful Thinking COG Analysis (How to Attack US Air Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Air-to-Air Capability	Find/Track Target	Sensors able to find/fix tgt	Enemies will develop stealth capabilities… (mitigated by F-22 sensor fusion)
	Engage Target (Air/Air msl or DE)	Msl Sensor	Spoof sensor (like IR sys ["force field"] we have)
		Absorb or reflect DE??	Would vary w/ DE type used in attack; hardened systems?
Air Defense	F2T2 Target	Air Defense Sensor Limitations	LO Cruise msls
			Micro/Nano UAVs
		C2 Networks/COP	See space tab on Comm systems
			Swamp w/ decoys or small UAV munitions
	Engage Target	Time for Patriots/kinetic interceptor to reach tgt	Counter-patriot TTPs
			DE wpn to shoot down Patriot
		See also Air-to-air vulnerabilities	
Global Strike/Power Projection	Tankers (THE single point of failure)	Lack of self-defense	Prevent US from gaining air superiority (reduce tanker freedom of movement, and/or attack them)
	Access to "front line" airstrips (support Non-Linear Ops)	Large/slow-moving acft (SAMs, etc)	Develop SAMs to counter current counter-SAM systems & TTPs
		Personnel on ground (aero port ops) near front lines (see "people" COG)	Bio/nano tech attack (not just bio)
	Weapons/Parts (Logistics)	More acft near front lines (more access while on ground)	Use nanobots to "eat" acft & increase strain
CSAR & Aeromed Evac	Find Downed Aircrew	Spoof systems, get CSAR to show up where aircrew aren't	

Table I-7: Wishful Thinking COG Analysis (How to Attack US Air Power)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
	Air-Mobile & battlefield Health Care	Close contact w/ patients	bioweapons to infect medics?
Centralized Control	CAOC -- General Ops & COP	Disrupt Info/ISR Reception @ CAOC	Mostly anti-sat stuff w/o getting into Info Immobilization side
			Disrupt/destroy incoming comm lines
		Destroy CAOC	EMP
			Stealth Cruise missile
			Kamikaze UAV munition

Table I-8: Wishful Thinking COG Analysis (How to Attack USAF Personnel)

USAF Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Stay Alive	Proper Biological Function	Inhale/Absorb Particulates/matter	Chem/Bio Weapons
			Nanobots/Nanoparticles (no… too indiscriminate, and too long to create effect; also may not degrade over time [??] like a bio-weapon does)
			Genetically-manipulated virus/ bioweapon
		DE Weapon Attack	Microwaves (like USAF's new riot control toy)
			DE weapon to scramble neuron firings? Kill/put to sleep/ immobilize/ heart attack, etc. etc.

Step 6: For Each Capability, Develop a Risk Assessment (Probability Versus Impact)

The first step in attempting to characterize the risk was to develop criteria against which to gauge the impact and probability of any given capability. These criteria were 100% subjective and were therefore open to debate; nevertheless, they were what the author determined to be important in judging the effectiveness of any given capability in meeting the *Wishful Thinking* state's objectives. Table I-9 lists the impact criteria, while Table I-10 does the same for the probabilities.

Table I-9: Wishful Thinking State's Impact Criteria

Impact	Justification
1	Minimal Impact to Space Capes AND USAF can attain air superiority within a few days to allow US ground forces full freedom of maneuver AND Low casualty count
2	Space Capes Denied, but only for limited amounts of time, and threat eliminated within a few days AND USAF can attain air superiority over most of the battlefield, but takes a few weeks AND Low casualty count
3	Space capes totally denied initially, then sporadically throughout entire conflict AND USAF can attain air superiority over most of the battlefield, but takes a few weeks OR Moderate Casualties
4	Space Cape Denied, but only for duration of conflict OR Can only achieve local pockets of air superiority, for very limited times OR Moderate to High Personnel Casualties
5	Total Elimination of Space-Based Capability OR Inability of USAF to establish any sort of Air Superiority OR Massive Casualties

Table I-10: Wishful Thinking State's Probability Criteria

Probability	Justification
1	Low probability due to limitations in technology, C4 structure, organization, etc. 0%<X<30%
2	Limited probability 30%<X<50%
3	Moderate probability 50%<X<60%
4	Fair probability 60%<X<70%
5	High probability >70%

Once the author determined the above criteria, he subjectively judged each capability relative to the criteria to determine the risk associated with that capability. Table I-11 summarizes the capabilities the *Wishful Thinking* state would attempt to develop. The "Rationale" column provides a brief description of the thought process that went into the numbers assigned to the impact and probability for each capability. The number for risk was simply the product of the impact and probability.

In the scenario analysis, the author considered two factors to be important: overall risk and probability of occurrence. Table I-11 uses color coding to highlight these factors. In the probability column, the most-probable capabilities have a brown background. In the risk column, green equated to low risk, yellow was medium risk, and red meant the risk was high.

Table I-11: Wishful Thinking State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
1	Use microsats to surround satellite, feed false data in to sensors	space	Easier than spoofing, but if can station-keep like this, just block signal	3	1	3
2	DE weapon to disrupt GPS timing	space; air	VERY low probability… figment of author's imagination.	3	1	3
3	Nano coatings to absorb or reflect energy (DE, radars, IR, etc.)	air; space	Impact could be high… could be improved active stealth as well… but coatings must be "perfect" so probability is low	4	1	4
4	Use microsats to surround satellite, intercept signals, alter them, and retransmit false data	space	Very difficult to do; signal diff't for each type of sat; and if can station-keep like this, much easier to just block signal	4	1	4
5	Disperse Clouds of Nanoparticles to interfere w/ coalition acft	air	Must know head of time where coalition will be; also must have method to control to prevent fratricide	2	2	4
6	Jam UAV control link	air	Directional antennae help mitigate this	2	2	4
7	Nanobots to "eat" coalition equipment or harm personnel	air; space; people	Low prob -- would need control mech	5	1	5
8	Nanobots to "eat" satellite	space	Nanobot tech still not even lab-ready (just theory); fielding sys by 2025 would be difficult	5	1	5
9	Attach microsats to target sat to mess up its attitude/position control	space	Slightly less impact than blocking satellite, since target sat may be able to maintain attitude for awhile until out of maneuvering capability. Less probability, too -- autonomous docking tech not quite there yet	3	2	6
10	Personal Laser/DE Weapons (Rifles)	air; people	Low prob[1]	4	2	8
11	Use nanotech to enable advanced CCD	air; space	May be feasible, but by 2025??; also, other low-tech approaches could be equally as effective	4	2	8

Table I-11: Wishful Thinking State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
12	Duplicating hardware to spoof signal or "SPAM" system with bogus transmissions to use up bandwidth	air; space	Fairly easy to do… if can get an original model. Similar to Chechens spoofing Russians to create fratricide[2]… but would be sporadic events, not constant detriment	3	3	9
13	Mobile Air Defense Platforms	air	Have them now	2	5	10
14	Multi-spectral sensors	air	Have them now, but need to improve resolution/response times to enable acft tracking	4	3	12
15	Block Satellite txmtr/receiver/sensor w/ microsats	space	Relatively high impact, but fairly low probability. Would be easier to just detonate explosive and damage satellite; but does have advantage of not creating space debris, and is reversible after conflict	4	3	12
16	Stealth UAVs and Acft	air	Other nations will have them;[3] but US claims it has counter-stealth capes already,[4] so impact not as high as it could be	3	4	12
17	DE "force field" to affect weapon guidance/control/fuzing	air	USAF already testing similar concepts for acft & counter-IEDs	3	4	12
18	Ground-Based Laser/DE Weapons for IADS	air	Probability only 3 because, while capes have been demonstrated, will take time to field operational sys; also must overcome stealth capes first to enable F2T2	5	3	15
19	Space-Based Laser/DE Weapons	air	Huge impact, but push to keep space from being weaponized, and ability to generate more power on ground, will delay fielding	5	3	15
20	Jam Satcom Links in AOR	space	Impact would vary depending on system jammed; would be difficult to jam them all; but adversary will try to jam some for sure (GPS)	3	5	15
21	EMP weapons	air	Available, but must make them directional for use over own soil; also, difficult to predict actual results, so impact only a 4[5]	4	4	16
22	Micro UAVs	air	Cheap, and under development	4	4	16

Table I-11: Wishful Thinking State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
23	LO cruise missiles	air	Combination of impact/probability of stealth & normal UAVs… plus, "stealthy cruise and ballistic missiles may be on the world market within a few years."[6] However, not as likely as UAVs since they are more expensive for essentially the same capes	4	4	16
24	Ground-Based Laser/DE ASAT Weapons	space	Demonstrated by China, but will take some time to make fully operational[7]	5	4	20
25	Kinetic, Space-Based ASAT Weapons	space	China has "mystery satellites" in orbits near US satellites; US is not sure what they are for… think some sort of ASAT weapons… so high probability[8]	5	4	20
26	Genetically modified bio weapons	people	Getting easier to create, can make them easier to employ, and possibly more "controllable" than "regular" bioweapons to minimize effects on own troops	5	4	20
27	"Normal" sized-UAVs	air	Building them now; cheap	4	5	20
28	Vehicle-Mounted DE anti-personnel weapons	people	US already has these; largest barrier to employment is policies, not tech	4	5	20
29	Hi-yield explosives to improve Pk for man-portable weapons	people	Evolutionary Cape Improvement	4	5	20
30	Kinetic, Ground-Based ASAT Weapons	space	Already demonstrated	5	5	25

Finally, the author mapped the capability analysis onto a risk matrix chart to graphically depict where each capability fell in the "risk space." Figure I-11 contains this mapping.

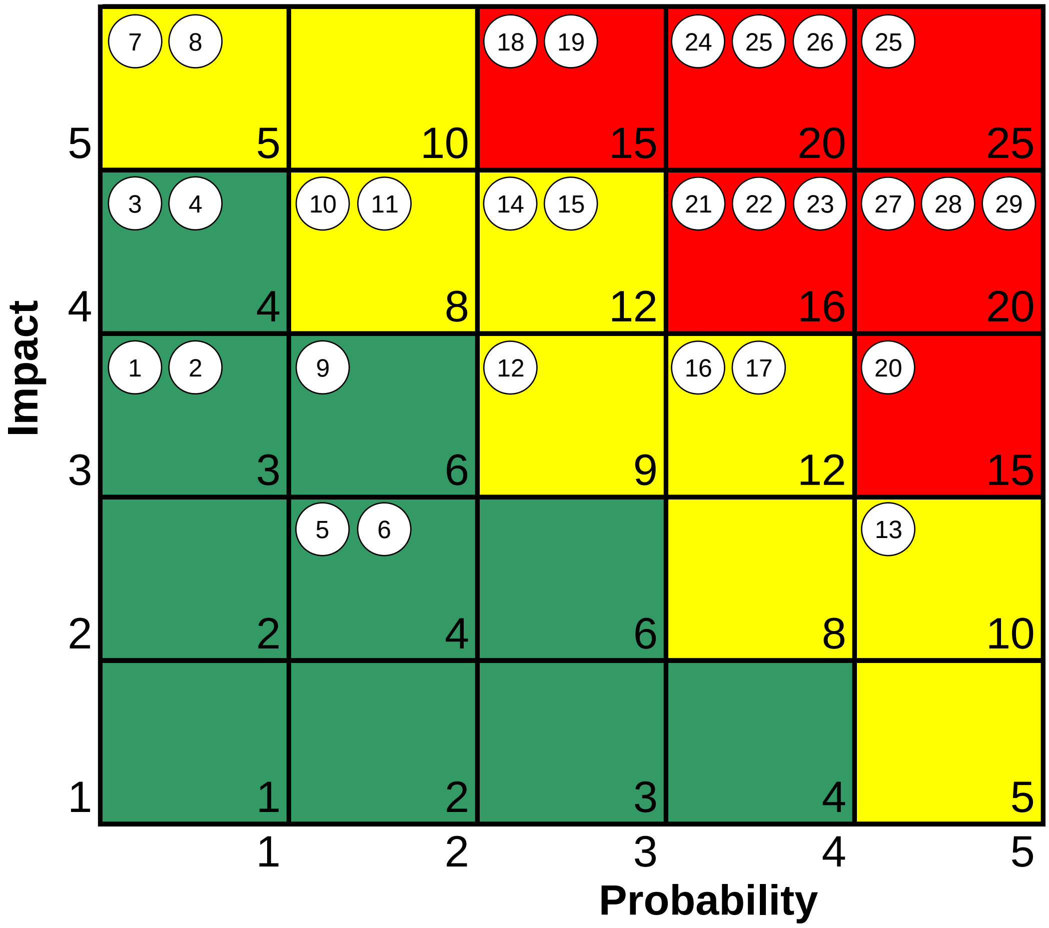

Figure I-11: Wishful Thinking Risk Matrix

NOTES

[1] See Geis II, "Directed Energy Weapons on the Battlefield: A New Vision for 2025".

[2] Takacs, "The Russian Air Force in Chechnya: Have Lessons Been Learnt and What Are the Future Perspectives?," 463.; and de Haas, "The Use of Russian Air Power in the Second Chechen War," 482.

[3] Fulghum, "New Radars Peel Veil from Hidden Targets," 59.

[4] Ibid.: 58.

[5] Jamie G. G. Varni, Lt Col, USAF et al., "Space Operations: Through the Looking Glass," in *Air Force 2025* (Maxwell AFB, AL: Air University, April 1996), 27-30.

[6] Fulghum, "New Radars Peel Veil from Hidden Targets," 58.

[7] Muradian, "Pentagon Turns Attention to Chinese Space Threat," 18.

[8] Vago Muradian, "China's Mystery Satellites," *C4ISR Journal* 6, no. 2 (2007).

Appendix J: *Information Immobilization* Capability Development

Step 1: Identify the Adversary's Strategic Objectives

Like the *Wishful Thinking* state (see Appendix I), the *Information Immobilization* state will attempt to defeat the US by routing the US forces on the battlefield while eroding the will of the US populace to support US military actions. However, while the *Information Immobilization* state has the same strategic objectives as the *Wishful Thinking* state, its operational objectives differ slightly due to its information-based capabilities. Table I-5 summarizes the strategic and operational objectives for the *Information Immobilization* adversary.

Table J-12: Information Immobilization State's Objectives

Strategic Objectives	Operational Objectives
1. Defeat US Fielded Forces	Neutralize US net-centric ops advantage (air & space)
	Conduct Offensive Cyber Ops to disrupt & distract US forces from concentrating on mil ops (disrupt DoD finance, health care, travel, etc)
2. Erode Will of US Populace to support US military actions	Inflict Maximum Number of US Casualties (This is most difficult to achieve w/ info-centered ops… must create physical effects to achieve this!!)
	Conduct offensive info ops to shape ideas/perceptions of US populace

Step 2: Identify The Centers Of Gravity (COGs) To Achieve Strategic Objectives

To achieve its strategic objectives, the *Information Immobilization* state will attempt to fight the US military in a regular conflict. For the USAF, this means the *Information Immobilization* adversary, like the *Wishful Thinking* sate, will focus its attack on the USAF's space power, air power and USAF personnel.

Steps 3-5: COG Analysis

For each COG, the author identified operational objectives, logical lines of operation, critical capabilities, critical requirements, and critical vulnerabilities (step 3); he then identified decisive points for each critical vulnerability (step 4), as well as capabilities that could affect the decisive points (step 5). Tables J-2 to J-5 provide the details for how the *Information Immobilization* state could attack the USAF's space power, air power and people respectively.

Table J-13: Information Immobilization COG Analysis (How to Attack US Space Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General (all sats)	Satellite processing/functioning	Computer Virus (CV)	Would need to "upload" computer virus through control link or data feed
	Data Security	Data Encryption Method	AI processors to decrypt
	Space-to-Ground Data Links (DLs)	Prevent User from Receiving Signal	CV in receiver? Difficult (many receivers, each on diff't system, some not networked)
		Spoof DL or alter signal	Upload CV to sat to disrupt signal being txmtd (requires access to upload sig)
		Monitoring	Hack in and just "watch" feeds to see what US knows, & when they know it
	Ground-to-Space Control Links	Prevent Sat from Receiving Control Signal	CV to disrupt signal txmsn (press "Ok" and nothing happens… or tells you command sent but nothing happens)
		Disrupt Ground Station Ops	DOS attack so grnd stn loses connections to outside (i.e., can't tell what others want them to track/do)… would slow, but not eliminate, control
			CV to slow networks/ctrl systems themselves

Table J-13: Information Immobilization COG Analysis (How to Attack US Space Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Spoof Control Link (send bogus control info)	Networked attack into Ctrl stn ground ctr to upload bogus instructions (positioning, etc)
		Monitor System	Hack in and monitor sys to predict US COAs, etc
ISR & Early Warning	C2 (for EW systems)	Orient phase of OODA loop (figure out what's happening)	Flood systems with False data; reduce trust in systm
Comm	Bandwidth	Fill with unwanted/bogus data	Denial of Service Attack

Table J-14: Information Immobilization COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General	Air Superiority	CV	Inject through DL; attack onboard computer systems or jam internal bandwidth
		Spoofing DL	Create/txmt bogus target info over datalink (can do this now during testing)
		AD-Hoc, "Self-Healing" IADS	Advanced AI will re-route IADS data/control through ad-hoc nets; no more just taking out command bunker, etc
	Logistics/Support Operations	Logistics (parts/fuel/supplies) Distribution System	Cyberattack to delay/disrupt "JIT" logistics
		TPFDD/Deployment Schedules	Take down entire system
			Monitor Schedules
			Alter records
		Medical/Dental Records	Delete or mess up medical records (switch blood types, etc)

Table J-14: Information Immobilization COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Personnel Records	Don't just do blanket "delete all" because of backups; mix and match some records, but not all, slowly over time.
		Finance	Hack into and hose up DFAS
		Travel	Take down DTS & travel office systems
			Mess up travel pay
			Change/delete existing travel reservations
		Comm	DOS attack or CV to shut down email & other supporting computer systems
UAVs	Control Links	Spoofing	If relayed through sat, would be like spoofing satcom (see Space page); LOS difficult -- must have txmtr near UAV or hack into grnd control sys (laptop?)
	Data Processors (guidance/ stability)	Computer Virus	Would have to get in to sys via ctrl or data links (see above)
Stealth	Optimized for portion of EM or audio spectrum	Sensor Data Fusion	Two types: "onboard" and networked. Onboard like F-22; all sensors are subcomponents of one main system, connected through bus. Networked are distributed w/ data transferred over the net
	Reflect Energy Away from Txmtr	Networked Sensors	Bistatic Radars: one sensor txmts data, rcvr at multiple other location(s) receive and correlate
Airborne ISR	Pass Info to Users (DL)	Hack into DL	Alter data (red to blue; decoy targets, wrong coordinates, etc)

Table J-14: Information Immobilization COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
	Determine Target Location	Interfere w/ platform's location data	Mess up GPS… see Space page
Precision A/G Weapons	GPS	Signal accuracy	See Space Page for Satellite Datalink Reception
Air Defense (US's)	F2T2 Target	C2 Networks/COP	Hack in, create false tracks or hide true ones
			DOS attack to slow data txmsn
Global Strike/Power Projection	Tankers	Scheduling system	Hack in, alter sched
CSAR & Aeromed Evac	Find Downed Aircrew	ISR systems	See ISR section above
			Hack in, change location or create false need for rescue; then ambush
	Air-Mobile & battlefield Health Care	Scheduling system	Hack in, mess up sched
		Medical Records	Alter medical records to increase chance of fatal mix-up (blood type, allergies, etc)
Centralized Control	CAOC -- General Ops & COP	Disrupt Info/ISR Reception @ CAOC	Hack in and alter
	Maintain decision superiority (fastest OODA loop)	Adversary can get inside your OODA loop	Enemy will develop AI systems to aid in data processing/speed their decision loop

Table J-15: Information Immobilization COG Analysis (How to Attack USAF Personnel)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Military Personnel: Conduct of Operations	Current SA (observe & orient)	Information Systems	Hack in and alter or reduce confidence in received data
	Decision Superiority	Speed	Adversary will develop AI systems that speed data processing, allow them to Decide faster
		Accuracy (was it "good" decision)	Develop AI systems to process more variables & options in same amt of time
	Attention to Detail/Focus	PsyOps	
		Attack supporting infrastructure (mil pay, records, etc)	See "air power" table
	Stay Alive	Fratricide	Hack into IFF systems, change red to blue, vice versa, create fratricide
		Armed UAVs	Hack in, take control of UAV, use it against owner's own troops
CONUS Mil & Civ Support to Operations	Accurate SA/knowledge	Info Ops	Massive disinformation IO campaign; reduce trust in media, military & political leadership
			Hack into & disrupt satellite TV feeds (turn off info flow)

Step 6: For Each Capability, Develop a Risk Assessment (Probability Versus Impact)

The first step in attempting to characterize the risk was to develop criteria against which to gauge the impact and probability of any given capability. These criteria were 100% subjective and were therefore open to debate; nevertheless, they were what the author determined to be important in judging the effectiveness of any given capability in meeting the *Information*

Immobilization state's objectives. Table I-9 lists the impact criteria, while Table I-10 does the same for the probabilities.

Table J-16: Information Immobilization State's Impact Criteria

Impact	Justification
1	No Outage In Systems, But Performance Slows Down AND No Loss of Trust In Info Systems AND Low US Casualties
2	Outages In US Information Systems Last < 1 Hr AND No Loss Of Trust In Systems AND Low to Moderate US Casualties
3	[Sporadic Outages In US Information Systems, But Back Online Within 1-3 Hrs AND Troops still trust systems when back online] OR Moderate US Casualties
4	Outages In US Information Systems Last 3 Hrs + OR US Troops Only Use Networked Information Systems after Lengthy Process to Re-Verify Data are Accurate Or Moderate to High US Casualties OR Moderate Adverse Impact on US Will to Support Effort
5	US Troops Stop Using Networked Information Systems (lack of functionality and/or trust in data) OR High US Casualties OR High Adverse Impact on Will of US Population to Support Effort

Table J-17: Information Immobilization State's Probability Criteria

Probability	Justification
1	Low probability due to limitations in technology, C4 structure, organization, etc. 0%<X<30%
2	Limited probability 30%<X<50%
3	Moderate probability 50%<X<60%
4	Fair probability 60%<X<70%
5	High probability >70%

Once the author determined the above criteria, he subjectively judged each capability relative to the criteria to determine the risk associated with that capability. Table I-11 summarizes the capabilities the *Information Immobilization* state would attempt to develop. The "Rationale" column provides a brief description of the thought process that went into the numbers assigned to the impact and probability for each capability. The number for risk was simply the product of the impact and probability.

In the scenario analysis, the author considered two factors to be important: overall risk and probability of occurrence. Table I-11 uses color coding to highlight these factors. In the probability column, the most-probable capabilities have a brown background. In the risk column, green equated to low risk, yellow was medium risk, and red meant the risk was high.

Table J-18: Information Immobilization State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
1	Advanced AI Software Equivalent to Human Rationalization/Thought	air; space	2030-2040 might be better timeframe for "human-level" software, but will be getting close by 2025;[1] this is why humans will still be kept in loop for final decision-making; impact low because this is just enabler for other capes listed below	1	3	3
2	Advanced Processors Equivalent to Human Processing Power	air; space	Already see Moore's law slowing a bit as we reach some physical limitations in processors; will require "leap" to next portion of S-curve (3D processing, etc) to continue current pace… but supercomputers projected to be there by early 2010s and PCs by 2025;[2] but impact low because this is just enabler for other capes listed below	1	4	4
3	Hacking into & Monitor Secure Networks	air; space	Can do this now… big question is whether or not US comes up with better security measures; impact is low, though, since this is enabler for other actions	1	4	4
4	Hacking into & Monitor Regular Networks	air; space	Can do this now… big question is whether or not US comes up with better security measures; impact is low, though, since this is enabler for other actions	1	5	5
5	"Decision Superiority" AI	air	Dependent on AI software + advanced processors + personnel trust in computers to aid decisions	5	2	10

Table J-18: Information Immobilization State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
6	Spoof/Flood w/ False Data	air; space; people (fratricide)	Requires hacking in; hardest to do after that since you need to first understand how system works	4	3	12
7	Hack into Link-16/Data Links	air	Would require equipment (possible to get) and daily codes (harder), or a cape to decrypt codes	4	3	12
8	Self-Healing IADS	air	Slightly less prob than AI software + processors + counter-stealth, since those provide the foundation	4	3	12
9	DOS Attack	air; space	Can fully expect this, since it's relatively easy; impact lower, though, since effects are not targeted	3	5	15
10	Advanced CG to "make up" news – disinformation campaign	people (will)	Hollywood has this now… and starting to export special effects work overseas, so highly probable; impact would vary w/ quality and story broadcast	3	5	15
11	Take Control of Computer Networks	air; space; people (fratricide)	Requires hacking in; slightly harder than just uploading virus	4	4	16
12	Networked, counter-stealth sensors (bistatic radars)	air	US already developing;[3] but still many kinks to work out to improve resolution/ tracking capes	4	4	16
13	Disrupt (Computer Virus)	air; space; people (distract)	Fully expect this to occur	4	5	20
14	Sensor Fusion	air	US has this now in F-22	4	5	20

Finally, the author mapped the capability analysis onto a risk matrix chart to graphically depict where each capability fell in the "risk space." Figure I-11 contains this mapping.

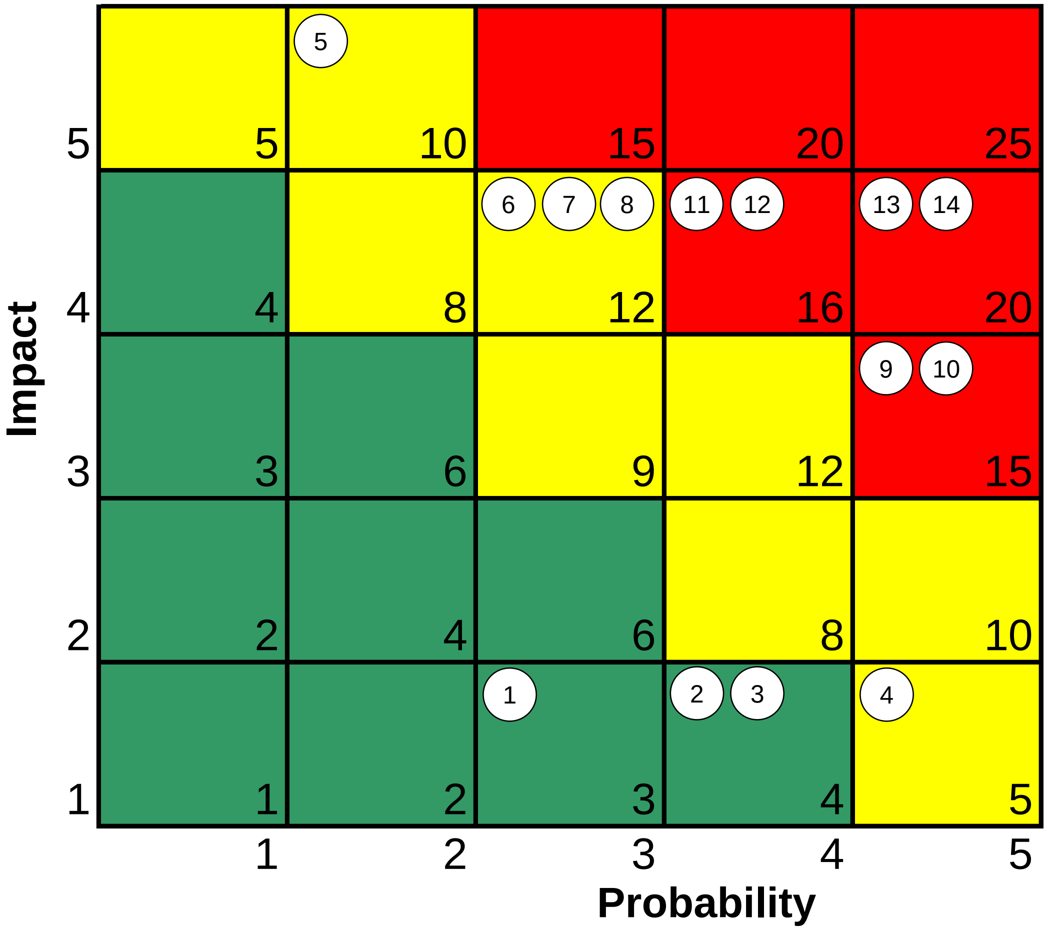

Figure J-12: Information Immobilization Risk Matrix

NOTES

[1] Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*, 200.

[2] Ibid., 124-26.

[3] David A. Fulghum, "Eliminating Noise Key to Anti-Stealth Radar," *Aviation Week & Space Technology* 150, no. 3 (1999): 60.

Appendix K: *David and Goliath* Capability Development

Step 1: Identify the Adversary's Strategic Objectives

Like the *Wishful Thinking* state (see Appendix I), the *David and Goliath (D&G)* state will attempt to defeat the US by routing the US forces on the battlefield while eroding the will of the US populace to support US military actions. However, while it has the same strategic objectives, its operational objectives differ slightly due to its decision to fight the US in an irregular manner. Table I-5 summarizes the strategic and operational objectives for the *D&G* adversary.

Table K-19: David and Goliath State's Objectives

Strategic Objectives	Operational Objectives
1. Erode US will to support military actions	Inflict maximum number of US casualties
	Draw out conflict as long as possible while maintaining "statehood"
	Use other IOPs to increase pressure on US population (economics -- drive up oil price, etc)
2. Erode International Support for US-led action	Fracture US alliance/coalition
	Worldwide IO campaign to discredit US action; maybe even give US false pretense for going to war (like Iraq did)

Step 2: Identify the Centers Of Gravity (COGs) to Achieve Strategic Objectives

To achieve its strategic objectives, the *D&G* state will attempt to fight the US military in an irregular conflict. However, the USAF COGs it must defeat are still the USAF's space power, air power and USAF personnel.

Steps 3-5: COG Analysis

For each COG, the author identified operational objectives, logical lines of operation, critical capabilities, critical requirements, and critical vulnerabilities (step 3); he then identified decisive points for each critical vulnerability (step 4), as well as capabilities that could affect the decisive points (step 5). Tables K-2 to K-5 provide the details for how the *D&G* state could attack the USAF's space power, air power and people respectively.

Table K-20: David and Goliath COG Analysis (How to Attack US Space Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General (all sats)	Satellite Existence	Anti-Sat Attack	DE kill
	Space-to-Ground Data Links	Prevent User from Receiving Signal	Jam satcom in AOR
			Physically destroy/harm txmtr (DE/kinetics)
		Spoof	Duplicate H/W, feed in false data (e.g., Chechens v Russia)
	Ground-to-Space Control Links	Prevent Sat from Receiving Control Signal	Physically destroy/harm rcvr (DE or kinetics)
ISR & Early Warning	Able to see/sense enemy (ISR)	Blind/Destroy/Disrupt Sensor	Laser/DE to physically damage sensors
		CCD &/or Spoof Sensor	Nanobots that provide false signatures (hide or decoy)
	C2 (for EW systems)	Orient phase of OODA loop (figure out what's happening)	Overwhelm w/ decoys/ false data
Comm	Bandwidth	Fill with unwanted/bogus data	Denial of Service Attack -- duplicate H/W, "spam" sys w/ false txmsns
Weather	Able to See/Measure WX	Blind Sensors	Laser/DE to physically damage sensors
GPS	Timing	Disrupt Timing Sync	DE wpn to speed up/slow down crystal vibrations

Table K-21: David and Goliath COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
General	Air Superiority/Defeat IADS	Ground-Based Air Defenses (G/A attack)	Laser/DE weapons to minimize reaction time
			Handheld SAMs
			Mobile IADS
		Inability to down all Acft	Small, stealthy UAVs
	Engines/Airframe Operation	Screw up Fuel/Air Mixture	EMP to fry circuits (low prob, unless attack at staging base; need to know where is; if over adversary territory, too much risk of fratricide)
		FOD	Disperse cloud of nanoparticles to "gum up" or "eat" engines (nano flak); would require ctrl mech to prevent fratricide
UAVs	Control Links	Jamming	Difficult if relayed through satellite
		Spoofing	Difficult; most likely relayed through Sat, so would be like spoofing satcom (see Space page)
	Data Processors (guidance/ stability)	EMP	Adversaries systems must be hardened to minimize fratricide
Stealth	Optimized for portion of EM or audio spectrum	Multi-Spectral Sensors	Self-explanatory
	Stealth Coatings	"Stick" something to aircraft to light it up	Disperse clouds of nanoparticles that will stick to aircraft and make it visible (low prob… need to know where acft is 1st to target it…)
Airborne ISR	Sensors (Locate Target)	Blind Sensor	Similar to anti- Space ISR, w/o anti-sat capes
		Spoof Sensor	
	Determine Target Location	Interfere w/ platform's location data	Mess up GPS… see below

Table K-21: David and Goliath COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Precision A/G Weapons	ALL	Electronic Fuzes	Use EM field around critical defensive points to initiate fuze prematurely or disarm it
		Guidance/Control	Ditto, but to disrupt guidance sys
	GPS	Signal Reception	See Space Page for Satellite Datalink Reception
	Laser Guidance Systems	Laser Spot Location	Counter laser to pull wpn off tgt
	EO Systems	Spoof sensors	CCD -- but difficult to disguise everything all the time
		Wpn relay back to acft	Jam (difficult; need to know where both acft & wpn are, wpn type, etc)
Air-to-Air Capability	Find/Track Target	Sensors able to find/fix tgt	Enemies will develop stealth capabilities… (mitigated by F-22 sensor fusion)
	Engage Target (Air/Air msl or DE)	Msl Sensor	Spoof sensor (like IR sys we have)
		Absorb or reflect DE??	Would vary w/ DE type used in attack; hardened systems?
Air Defense	F2T2 Target	Air Defense Sensor Limitations	LO Cruise msls
			Micro/Nano UAVs
		C2 Networks/COP	See space tab on Comm systems
			Swamp w/ decoys or small UAV munitions
	Engage Target	Time for Patriots/kinetic interceptor to reach tgt	Counter-patriot TTPs
			DE wpn to shoot down Patriot

Table K-21: David and Goliath COG Analysis (How to Attack US Air Power)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		See also Air-to-air vulnerabilities	
Global Strike/Power Projection	Tankers (THE single point of failure)	Lack of self-defense	Prevent US from gaining air superiority (reduce tanker freedom of movement, and/or attack them)
	Access to "front line" airstrips (support Non-Linear Ops)	Large/slow-moving acft (SAMs, etc)	Develop SAMs to counter current counter-SAM systems & TTPs
		Personnel on ground (aero port ops) near front lines (see "people" COG)	Bio/nano tech attack (not just bio)
	Weapons/Parts (Logistics)	More acft near front lines (more access while on ground)	Use nanobots to "eat" acft & increase strain
CSAR & Aeromed Evac	Find Downed Aircrew	Spoof systems, get CSAR to show up where aircrew aren't	See Spoofing Comm
	Air-Mobile & battlefield Health Care	Close contact w/ patients	bioweapons to infect medics?
Centralized Control	CAOC -- General Ops & COP	Disrupt Info/ISR Reception @ CAOC	Mostly anti-sat stuff w/o getting into Info Immobilization side
			Disrupt/destroy incoming comm lines
		Destroy CAOC	EMP
			Stealth Cruise missile
			Kamikaze UAV munition

Table K-22: David and Goliath COG Analysis (How to Attack USAF Personnel)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Stay Alive	Proper Biological Function	Inhale/Absorb Particulates/matter	Chem/Bio Weapons
			Nanobots/Nanoparticles (no… too indiscriminate, and too long to create effect; also may not degrade over time [??] like a bio-weapon does)
			Genetically-manipulated virus/bioweapon
		DE Weapon Attack	Microwaves (like USAF's new riot control toy)
			"EMP" type weapon to scramble neuron firings? Kill/put to sleep/ immobilize/ heart attack, etc. etc.
			Laser rifles
	Medical Care (as required)		See Air Power Medivac

Step 6: For Each Capability, Develop a Risk Assessment (Probability Versus Impact)

The first step in attempting to characterize the risk was to develop criteria against which to gauge the impact and probability of any given capability. These criteria were 100% subjective and were therefore open to debate; nevertheless, they were what the author determined to be important in judging the effectiveness of any given capability in meeting the *D&G* state’s objectives. Table I-9 lists the impact criteria, while Table I-10 does the same for the probabilities.

Table K-23: David and Goliath State's Impact Criteria

Impact	Justification
1	Minimal Impact to Space Capes AND USAF can attain air superiority within a few days to allow US ground forces full freedom of maneuver AND Low casualty count
2	Space Capes Denied, but only for limited amounts of time, and threat eliminated within a few days AND USAF can attain air superiority over most of the battlefield, but takes a few weeks AND Low casualty count
3	Space capes totally denied initially, then sporadically throughout entire conflict AND USAF can attain air superiority over most of the battlefield, but takes a few weeks OR Moderate Casualties
4	Space Cape Denied, but only for duration of conflict OR Can only achieve local pockets of air superiority, for very limited times OR Moderate to High Personnel Casualties
5	Total Elimination of Space-Based Capability OR Inability of USAF to establish any sort of Air Superiority OR Massive Casualties

Table K-24: David and Goliath State's Probability Criteria

Probability	Justification
1	Low probability due to limitations in technology, C4 structure, organization, etc. 0%<X<30%
2	Limited probability 30%<X<50%
3	Moderate probability 50%<X<60%
4	Fair probability 60%<X<70%
5	High probability >70%

One the author determined the above criteria, he subjectively judged each capability relative to the criteria to determine the risk associated with that capability. Table K-25 summarizes the capabilities the *D&G* state would attempt to develop. The "Rationale" column provides a brief description of the thought process that went into the numbers assigned to the impact and probability for each capability. The number for risk was simply the product of the impact and probability.

In the scenario analysis, the author considered two factors to be important: overall risk and probability of occurrence. Table K-25 uses color coding to highlight these factors. In the probability column, the most-probable capabilities have a brown background. In the risk column, green equated to low risk, yellow was for medium risk, and red meant the risk was high.

Table K-25: David and Goliath State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
1	DE weapon to disrupt GPS timing	space; air	VERY low probability… figment of author's imagination.	3	1	3
2	Nano coatings to absorb or reflect energy (DE, radars, IR, etc.)	air; space	Impact could be high… could be improved active stealth as well… but coatings must be "perfect" so probability is low	4	1	4
3	Disperse Clouds of Nanoparticles to interfere w/ coalition acft	air	Must know head of time where coalition will be; also must have method to control to prevent fratricide	2	2	4
4	Jam UAV control link	air	Directional antennae help mitigate this	2	2	4
5	Personal Laser/DE Weapons (Rifles)	air; people	Low prob[1]	4	2	8
6	Use nanotech to enable advanced CCD	air; space	May be feasible, but not by 2025; also, other low-tech approaches could be equally as effective	4	2	8
7	Duplicating hardware to spoof signal or "SPAM" system with bogus transmissions to use up bandwidth	air; space	Fairly easy to do… if can get an original model. Similar to Chechens spoofing Russians to create fratricide[2]… but would be sporadic events, not constant detriment	3	3	9
8	Nanobots to "eat" coalition equipment or harm personnel	air; space; people	Low prob -- would need control mech	5	2	10
9	Mobile Air Defense Platforms	air	Have them now	2	5	10
10	Multi-spectral sensors	air	Have them now, but need to improve resolution/response times to enable acft tracking	4	3	12
11	EMP weapons	air	Available, but must make them directional for use over own soil; also, difficult to predict actual results, so impact only a 4[3]	4	3	12
12	Stealth UAVs and Acft	air	Other nations will have them;[4] but US claims it has counter-stealth capes already,[5] so impact not as high as it could be	3	4	12
13	DE "force field" to affect weapon guidance/control/fuzing	air	USAF already testing similar concepts for acft & counter-IEDs	3	4	12
14	Ground-Based Laser/DE Weapons for IADS	air	Probability only 3 because, while capes have been demonstrated, will take time to field operational sys; also must overcome stealth capes first to enable F2T2	5	3	15

Table K-25: David and Goliath State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
15	Ground-Based Laser/DE ASAT Weapons	space	Reduced prob from Wishful Thinking scenario… D&G state is smaller, would probably focus on anti-air before anti-space. But still plausible.	5	3	15
16	Kinetic, Ground-Based ASAT Weapons	space	Reduced prob from Wishful Thinking side… D&G state is smaller, would focus on anti-air before anti-space… but more likely than DE weapon to shoot down satellites	5	3	15
17	Jam Satcom Links in AOR	space	Impact would vary depending on system jammed; would be difficult to jam them all; but adversary will jam some for sure (GPS)	3	5	15
18	LO cruise missiles	air	Combination of impact/probability of stealth & normal UAVs… plus, "stealthy cruise and ballistic missiles may be on the world market within a few years."[6] However, not as likely as UAVs since they are more expensive for essentially the same capes	4	4	16
19	Micro UAVs	air	Cheap, and under development	4	4	16
20	Genetically modified bio weapons	people	Getting easier to create, can make them easier to employ, and possibly more "controllable" than "regular" bioweapons to minimize effects on own troops	5	4	20
21	"Normal" sized-UAVs	air	Building them now; cheap	4	5	20
22	Vehicle-Mounted DE anti-personnel weapons	people	US already has these (Active Denial); largest barrier to employment is policies, not tech	4	5	20

Finally, the author mapped the capability analysis onto a risk matrix chart to graphically depict where each capability fell in the "risk space." Figure I-11 contains this mapping.

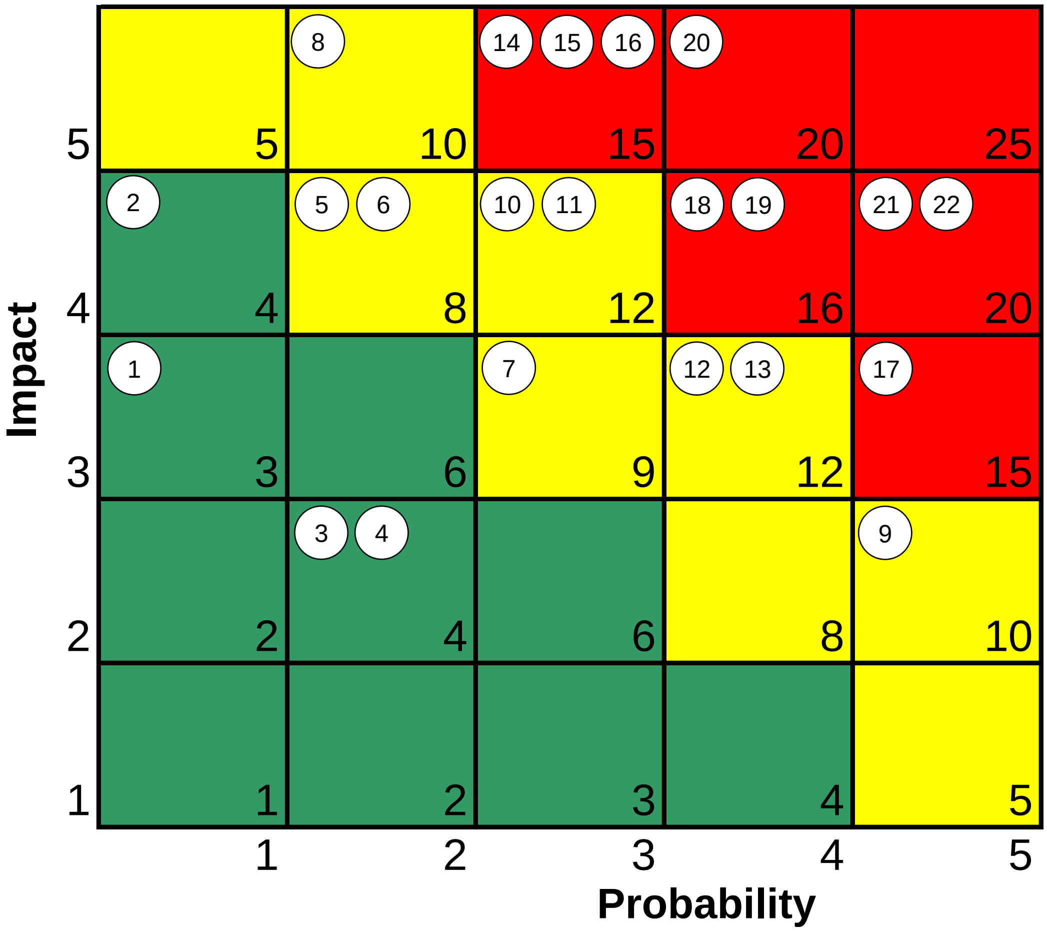

Figure K-13: David and Goliath Risk Matrix

NOTES

[1] See Geis II, "Directed Energy Weapons on the Battlefield: A New Vision for 2025".

[2] Takacs, "The Russian Air Force in Chechnya: Have Lessons Been Learnt and What Are the Future Perspectives?," 463.; and de Haas, "The Use of Russian Air Power in the Second Chechen War," 482.

[3] Varni et al., "Space Operations: Through the Looking Glass," 27-30.

[4] Fulghum, "New Radars Peel Veil from Hidden Targets," 59.

[5] Ibid.: 58.

[6] Ibid.

Appendix L: *The Phantom Menace* Capability Development

Step 1: Identify the Adversary's Strategic Objectives

Unlike the other state actors, *The Phantom Menace (TPM)* state will attempt to defeat the US by attacking targets within the US. It cannot project traditional military power to do so; as a result, it will instead use cyberattacks and Influence Operations (IFO). Table I-5 summarizes *The Phantom Menace's* Strategic and Operational Objectives.

Table L-26: The Phantom Menace State's Objectives

Strategic Objectives	Operational Objectives
1. Remain Hidden/Disguise Attacker's Identity	Minimize/eliminate "traceability;" use Cyberspace to inflict damage (SOF troops would also be a potential threat, but if caught could pinpoint attacker, so assume not used)
2. Minimize US presence in my region so I can start to exert my own influence	Conduct Offensive Ops to disrupt & distract US from concentrating on my region (force US to take care of problems at home first)
3. Erode Will of US Populace to support any US military actions	IF US begins to figure out who hit them, conduct Info Op campaign to try to place blame on someone else or muddy the waters so they cannot demonstrate clearly who attacked them

Step 2: Identify the Centers Of Gravity (COGs) to Achieve Strategic Objectives

To achieve its strategic objectives, the *TPM* state will circumvent the US military and attack the US's will to fight using non-military means. Specifically, *The Phantom Menace* will attack US infrastructure and institutions using cyberattacks, financial attacks and other non-military means. While doing so, its main goal is to remain hidden to prevent the US from retaliating with massive force (i.e., nukes). If the US does start to figure out who might be attacking it, the *TPM* state will launch an IFO campaign designed to confuse the facts at hand.

Steps 3-5: COG Analysis

For each COG, the author identified operational objectives, logical lines of operation, critical capabilities, critical requirements, and critical vulnerabilities (step 3); he then identified decisive points for each critical vulnerability (step 4), as well as capabilities that could affect the decisive points (step 5).

In the case of *The Phantom Menace*, the capability analysis was slightly different than the other scenarios. The capabilities possessed by the state could be summed up in two broad areas: computer hacking and IFO. Thus, the "capability analysis" turned out to be more of an exercise in determining what types of targets *The Phantom Menace* would attack. Tables L-2 and L-3 provide the details for how *The Phantom Menace* might attack the US's infrastructure and institutions, respectively. In this case, one cannot consider this list anywhere near complete, since the choice of potential targets was huge. But, hopefully it at least provided a starting point for further analysis, as well as discussion of the resources that the US must protect from an unconventional attack.

Table L-27: The Phantom Menace COG Analysis (How to Attack US Infrastructure)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Energy	Fuel Source	Shipment from original source to power plant	Disrupt production
			Disrupt Transportation to Power Plant (see Transpo LOO)
	Power Generation Plants	Computer Control Systems	Computer Virus to disrupt plant operations/control software
	Distribution System	Power routing substations	Disrupt key nodes to create rolling blackouts or power surges

Table L-27: The Phantom Menace COG Analysis (How to Attack US Infrastructure)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Transformers & Power Lines	Disrupt system to create spikes that can damage hardware?
	Waste Disposal	Transportation to Storage	Disrupt Transportation to Storage (see Transpo LOO)
		Storage/Disposal Location	Not much you can do here w/ IO capes and no real access to site (no mil power projection, and want to remain hidden, so no SOF)
Chemical Manufacturing Plants/ Refineries	Proper Operation	Computerized Control Systems	CV to disrupt plant ops; release toxic chems to kill people or create environmental disaster
Transportation	Fuel Source	Overseas suppliers	Disrupt shipments
	Clear/Accessible Routes	Traffic Control Systems (Including Air Traffic Control)	Use CV to disrupt central controls (highways, rail, air, etc)
	Shipping Company Logistics Control Systems	Centralized Computer Systems	Alter/disrupt schedules
			Alter requests/orders
			Alter financial records (who's paid for what??)
Water/Food	Production	Computerized Control Systems	Disrupt w/ CV to adversely impact recipies, quality control, etc.
	Distribution	Transportation	See Transportation LOOs
Comm	Computer Control Systems (Telephone & TV/Cable, etc)	Ability to Transmit	As move towards digital transmissions, may be possible to embed malicious code in datastream
		Content	Intercept & alter content (IFO)

Table L-27: The Phantom Menace COG Analysis (How to Attack US Infrastructure)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
	Satellite Relays	Ground Control Links	See Information Immobilization LOOs… but now targeting civilian as well as military comm systems
		Bandwidth	Ditto
	Internet Routers	Worldwide accessible	DOS attack
			Intercept & alter content
Sewage/Waste	Pick-Up/Removal	Customer Databases	Alter companies' records of who is supposed to have trash picked up
		Command & Control Systems (schedules, etc)	Alter schedules
	Disposal/Storage		See LOOs for disposal/ storage of energy waste; similar
	Treatment	Computer Control Centers	Disrupt systems to spew waste into rivers, etc & create ecological disaster
Crisis Management/Response (FEMA, Fire, Police, Medical)	C2	Communications	See Comm LOOs; take down or DOS for 911 system
	Supplies	Storage Sites	Alter/disrupt inventories, etc.
		Transportation to Emergency Site	See Transportation LOOs

Table L-28: The Phantom Menace COG Analysis (How to Attack US Institutions)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
Government	Public Trust	Ability to Protect Citizens	Media/IFO campaign to reduce trust in gov't
	Protection of Individual Rights	Ability to maintain law & order with minimum amount of impingement on rights	Coordinate attacks to create chaos, cause martial law to be required to control situation
		Gov't need to surveil its own population to root out crazies while trying to protect the majority	IFO campaign; make populace distrust one another, call for more gov't surveillance, etc
	Ability to effect change when required	Inability to achieve clear majority in House/Senate	IFO campaign to further split/divide Senate, House, Prez & populace
	Accurate Public Records	Computerized Databases	Alter/destroy/disrupt computerized property records, etc.
Religious			IFO campaign to stir up fanatics against one another
Law Enforcement	Public Trust	Media footage of "bad actors"	IFO campaign
	Accurate Records	Computerized Systems	Alter arrest & court histories, DNA & fingerprint record databases, etc.
Educational & Professional Licensing	College Attendance Records, Class Schedules, etc	Computerized Records	Alter transcripts/ graduation records
	SAT, ACT scores	Computerized Records	Alter histories (affects ability to get into college)
	Professional Licensing Societies (AMA, ABA, etc)	Computerized Records	Alter/disrupt/destroy records
Economic/E-commerce	Personal Info Security	Computer Systems/Internet Transmissions	Monitor Transmissions & steal personal info

Table L-28: The Phantom Menace COG Analysis (How to Attack US Institutions)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
	Logistics/Distribution Systems	Computerized Databases/Records	Disrupt/Destroy/Alter
Financial	100% accuracy	Stock Market records	CV to alter/disrupt/ destroy trading records
			Flood system with false buy or sell requests
		Banking Records	CV to alter/disrupt/ destroy bank records
		Stock Market Values	Financial Attack -- devalue currency, speculating, etc
	Faith that Currency Is Valid	Counterfeit Money	Flood market with counterfeit dollars
Medical	Know Who to Treat	Command and Control	Disrupt C2 for crisis management; see infrastructure page
	Accurate Medical Records	Medicare System Records/Files	Alter/disrupt medicare/ HMO/insurance company records (erase/make it look like no one has coverage)
		Computerized Files	Alter computerized files to change blood types, medical histories, etc
	Proper Drug Doses/Contents	Drug production facilities	Disrupt computer-controlled systems to change drug mixtures/ doses/ ingredients
		Pharmacy Records	Disrupt doctor-to-pharmacy electronic records (hand out wrong pil types, doses, etc)
Media	Public Trust	Public Perception	Create false stories, get media to run them as true, then debunk them; media loses credibility (see CBS scandal)

Table L-28: The Phantom Menace COG Analysis (How to Attack US Institutions)

US Capabilities	Requirements	Vulnerabilities	Adversary Capabilities
		Signal Content	Intercept and modify signal content to broadcast own info
			Alter newswire service (AP, etc) transmissions
	Production	Computer-control systems	Disrupt TV, newspaper, internet news production systems
	Distribution		See "Comm" section on Infrastructure COG

Step 6: For Each Capability, Develop a Risk Assessment (Probability Versus Impact)

The first step in attempting to characterize the risk was to develop criteria against which to gauge the impact and probability of any given capability. These criteria were 100% subjective and were therefore open to debate; nevertheless, they were what the author determined to be important in judging the effectiveness of any given capability in meeting *The Phantom Menace's* objectives. Table I-9 lists the impact criteria, while Table I-10 does the same for the probabilities.

Table L-29: The Phantom Menace State's Impact Criteria

Impact	Justification
1	No noticeable economic impact AND No Disruption to Emergency/Essential Services AND No Disruption to US Military Power Projection Capability AND Low US Civilian Casualties (<100)
2	Negative Economic Impact, but Recoverable within 1 year AND Minor Disruptions to Emergency/Essential Services; no associated loss of trust in gov'ts ability to protect populace AND No Disruption to US Military Power Projection Capability AND Low US Civilian Casualties (<100)
3	Negative Economic Impact, But Recoverable Within 2-3 years (like 9/11) AND Some Impacts to Emergency/Essential Services, but Restored w/in a few weeks; no other real loss of gov't trust/control (ala Hurricane Katrina) AND No Disruption to US Military Power Projection Capability AND Moderate US Civilian Casualties (<1000)
4	Negative Economic Impact, But Recoverable Within a Decade OR Spawns Sporadic Riots throughout major cities due to US gov'ts inability to provide basic services OR Inability of US to Support Military Power Projection For At Least a Decade OR Moderate to High US Civilian Casualties (1000 - 10,000)
5	Total US Economic Collapse OR Collapse of US Gov't OR Inability of US to Support Military Power Projection For Unforseen Amt of Time OR Massive US Civilian Casualties (like nuclear reactor overload)

Table L-30: The Phantom Menace State's Probability Criteria

Probability	Justification
1	Low probability due to limitations in technology, C4 structure, organization, etc. 0%<X<30%
2	Limited probability 30%<X<50%
3	Moderate probability 50%<X<60%
4	Fair probability 60%<X<70%
5	High probability >70%

One the author determined the above criteria, he subjectively judged each capability relative to the criteria to determine the risk associated with that capability. Table I-11 summarizes the capabilities *The Phantom Menace* would attempt to develop. The "Rationale" column provides a brief description of the thought process that went into the numbers assigned to the impact and probability for each capability. The number for risk was simply the product of the impact and probability.

In the scenario analysis, the author considered two factors to be important: overall risk and probability of occurrence. Table I-11 uses color coding to highlight these factors. In the probability column, the most-probable capabilities have a brown background. In the risk column, green equated to low risk, yellow was medium risk, and red meant the risk was high.

Table L-31: The Phantom Menace State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
1	Alter/destroy educational records (College Transcripts, SAT scores, etc)	Institutions	Very low impact, so probability also low	1	1	1
2	Hack into and destroy/disrupt banking records	Institutions	Fairly recoverable; banks have back-up databases; impact also reduced because each bank has its own record system, and would have to hack into all/most of them simultaneously	1	3	3
3	Alter/destroy/disrupt computerized public records (land records, etc.)	Institutions	Impact Low; would generally just disrupt life for a few months while records sorted out. Associated probability low simply due to low impact (not worth effort)	2	2	4
4	Financial Attack to Disrupt Global Markets, Devalue dollar	Institutions	Easy way to affect US economy; but difficult to control… thus, mitigated by blowback against TPM state; also, may leave paper trail that US can follow to source and retaliate	3	2	6
5	CV to disrupt control systems at food processing plants	Infrastructure	Potentially high impact in economics as well as US casualties; low blowback on TPM. Big question is how to hit large number at once, since all companies' systems are different… so lowered probability somewhat	3	2	6

Table L-31: The Phantom Menace State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
6	Hack in, alter newswire transmissions to create false stories, reduce trust in media	Institutions	Would reduce trust in media, but not much other impact by itself; coupled with other actions, could have higher impact. Probability lowered because of low impact, as well as TPM's requirement to hide…TPM would only use this option as part of IFO if US started to figure out puzzle pieces, or if TPM was doing well enough where it wanted to start trying to disrupt US gov't control over its populace.	2	3	6
7	Disrupt TV, radio, internet news site production and dissemination systems	Institutions	Would reduce trust in media, but not much other impact by itself; coupled with other actions, could have higher impact. Probability lowered because of low impact, as well as TPM's requirement to hide…TPM would only use this option as part of IFO if US started to figure out puzzle pieces, or if TPM was doing well enough where it wanted to start trying to disrupt US gov't control over its populace.	2	3	6
8	Flood US market with false buy/sell requests (electronically emulate E*Trade and other online brokers)	Institutions	Major market disruption, but short-lived (like 9/11) while records straightened out; probability mitigated by blowback	3	3	9
9	Disrupt logistical systems for energy plant supplies	Infrastructure	Even if energy plant computer systems are secure or not networked, provides method to disrupt production (hit the side target); but impact only lasts as long as logistics disrupted	3	3	9
10	DOS attack to slow internet comm	Infrastructure	Easy to implement; widespread effects, but difficult to control/predict, and how long will they last?	2	5	10

Table L-31: The Phantom Menace State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
11	Financial Attack -- Flood World Market with near-perfect counterfeit money & devalue dollar	Institutions	People lose trust in US currency, and it may no longer be world's central form of currency (it's accepted almost anywhere); probability reduced somewhat due to: 1. economic blowback; 2. Huge amounts of counterfeit money that TPM would need to introduce to have impact; and 3. US's efforts to make money more difficult to counterfeit	4	3	12
12	Cyberattack to take down Wall Street	Institutions	Impact mitigated by back-up systems; but would still cause fairly major jolt to economy. Probability slightly mitigated by adverse impact to world markets and blowback on TPM state	3	4	12
13	Advanced CG to "make up" news – disinformation campaign	Institutions; People (will)	Hollywood has this now… and starting to export special effects work overseas, so highly probable; impact would vary w/ quality and story broadcast; probability reduced slightly compared to Information Immobilization scenario because TPM trying to hide; would only use IFO campaign if the truth started to come out, or was so far along in its plans it felt US was no longer a threat it had to hide from	3	4	12
14	Destroy/disrupt records for logistical companies like UPS, FedEx, etc.	Institutions	Slows e-commerce, and reduces people's trust in online merchants' ability to deliver goods… but other more lucrative targets and worldwide blowback drops probability	3	4	12

Table L-31: The Phantom Menace State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
15	CV to disrupt chemical processing plant/ oil refinery/sewage treatment etc. control systems	Infrastructure	Impacts depend on plant hit; effects fairly local for chem plant; more widespread for refineries. Probability increased because of fairly low economic blowback on TPM	3	4	12
16	Disrupt ground traffic control systems (rail, metros, etc)	Infrastructure	Potential US casualties; disrupts economy; reduces US's ability to respond to disaster areas	3	4	12
17	CV to disrupt power plant control systems	Infrastructure	Widespread impact, but length depends on damage to plant; worst case, nuclear plant explosion… or, for normal plant, taken offline until repaired	4	4	16
18	Disrupt civilian satellite control systems	Infrastructure	High impact in terms of gov't ability to manage chaos, distribute instructions & information; fairly major target for TPM	4	4	16
19	Destroy/disrupt civilian medical records (including medicare, insurance, etc)	Institutions	Increases number of US casualties; actual medical histories not centralized, which makes this harder to accomplish there, but Medicare and insurance records may be prime target	4	4	16
20	Disrupt Pharmaceutical Production (recipies/quality control)	Institutions	Increase US death toll	4	4	16
21	Coordinate all of these attacks at once	All	Obviously, extremely high impact; but probability mitigated by US's nuclear triad and potential to respond if it can figure out who is attacking it, as well as its importance in world economy and blowback that would occur if another state did launch catastrophic attack	5	4	20

Table L-31: The Phantom Menace State Risk Analysis

ID	Capability	Target DP	Rationale	Impact	Probability	Risk
22	Steal personal info out of economic transactions (make people lose trust in e-commerce security so they don't buy stuff online anymore… slows economy)	Institutions	E-commerce huge part of US economy already, and growing; so will have major economic impact by 2025; and people already doing this, so high probability	4	5	20
23	Disrupt computerized communications control systems (TV, radio, internet)	Infrastructure	High impact in terms of gov't ability to manage chaos, distribute instructions & information; major target for TPM	4	5	20
24	Disrupt 9/11 systems -- CV or DOS attack	Infrastructure	Easy way to disrupt system: with voice-over-IP phone systems now, could easily SPAM 9/11 to use up its bandwidth, disrupt emergency services	4	5	20
25	Disrupt Air Traffic Control (ATC)	Infrastructure	Major impact to US economy, as well as potential US civilian casualties	4	5	20

Finally, the author mapped the capability analysis onto a risk matrix chart to graphically depict where each capability fell in the “risk space.” Figure I-11 contains this mapping.

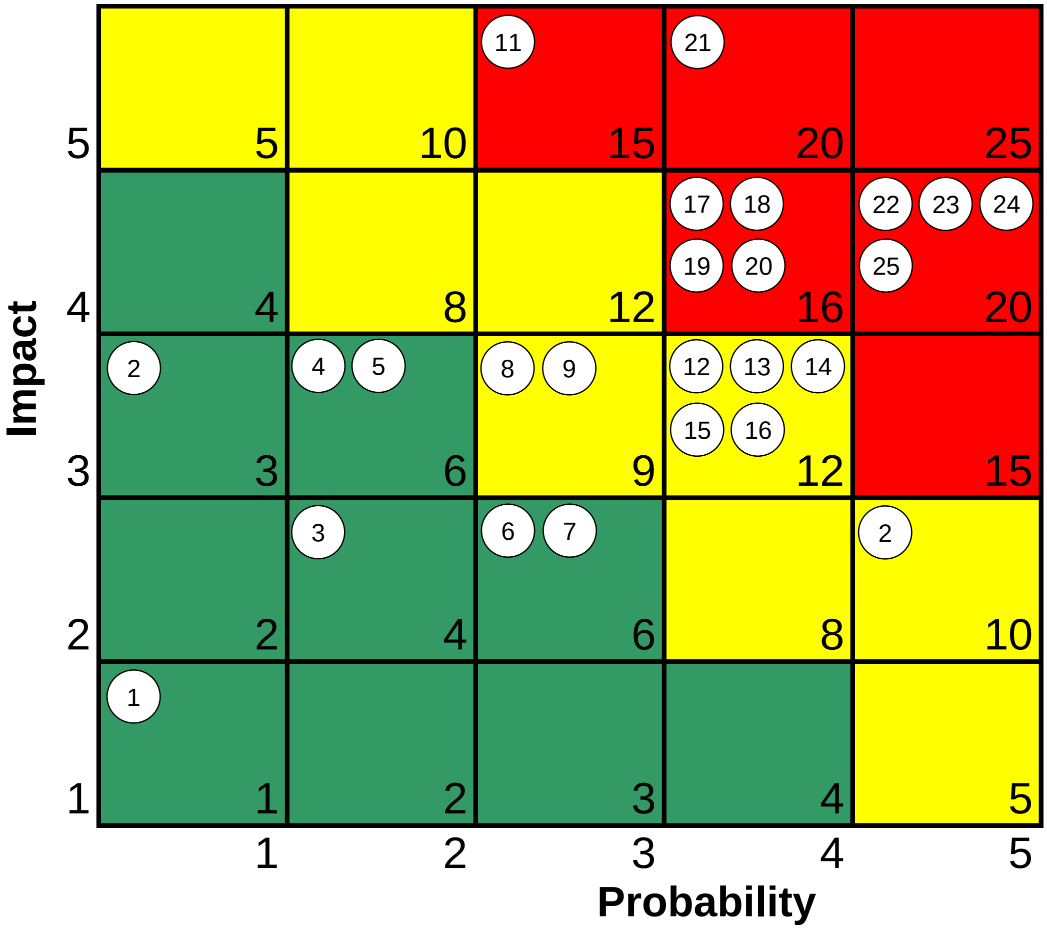

Figure L-14: The Phantom Menace Risk Matrix

Bibliography

Abbot, Spencer. "Air Power Strategy and the Problem of Coercion." In *Immaculate Warfare,* edited by Stephen D. Wrage. Westport, CT: Praeger, 2003.

Ahearn, Dave. "U.S. Military, Commercial Space Assets Vulnerable to Attack: Experts." *Defense Daily* 230, no. 58 (22 June 2006).

Air Force Research Laboratory. *Active Denial System*, United States Air Force Fact Sheet. Kirtland AFB, NM: United States Air Force, August 2006.

Air University. *Spacecast 2020*. Vol. 1. Maxwell AFB, AL, Jun 1992.

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare : Developing and Leveraging Information Superiority*, Ccrp Publication Series. Washington, DC: National Defense University Press, 1999.

Alibek, Ken, and Stephen Handelman. *Biohazard : The Chilling True Story of the Largest Covert Biological Weapons Program in the World, Told from the inside by the Man Who Ran It*. 1st ed. New York: Random House, 1999.

Arquilla, John, David Ronfeldt, and Michelle Zanini. "Information-Age Terrorism." *Current History* (2000): 7.

Arts, Bas, Math Noortmann, and Bob Reinalda. *Non-State Actors in International Relations*, Non-State Actors in International Law, Politics, and Governance Series. Aldershot, Hants, England ; Burlington, VT: Ashgate, 2001.

Badari Narayana, K., and V. Venkata Reddy. "Thermal Design and Performance of Hamsat." *Acta Astronautica* 60, no. 1 (2007): 7-16.

Barley, S.R. "What Can We Learn from the History of Technology?" *Journal of Engineering and Technology Management* 15, no. 4 (1998): 19.

Beebe, Kenneth, Maj, USAF. "The Air Force's Missing Doctrine." *Air & Space Power Journal* (Spring 2006).

Berman, Ilan. "How to Eliminate Iran's Nuclear Weapons: A Symposium." The Claremont Institute, http://www.claremont.org/writings/crb/spring2006/symposium.html.

Boeing. "News Release: Boeing Avionics Help Guide F-22 Missile to Its Target." http://www.boeing.com/news/releases/2001/q3/nr_010924n.htm.

Bond, D. F. "Radar Networks, Computing Advances Seem as Keys to Counter Stealth Technologies. (Cover Story)." *Aviation Week & Space Technology* 131, no. 23 (1989): 41.

Bush, George H. W. "The National Security Strategy to Secure Cyberspace." Washington, DC, February, 2003.

———. "National Strategy for Combating Terrorism." 2003.

Campbell, Edwina, and Lewis Griffith. "An Introduction to the Instruments of Power." In *Inter/National Security and War, AY07 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 19 Apr 2004.

Canada. Treasury Board. *Integrated Risk Management Framework = Cadre De Gestion Intégrée Du Risque*. [Ottawa]: Treasury Board of Canada Secretariat, 2001.

Carey, Col Michael J. "Integrating Space Capabilities in Support of the USCENTCOM Theater of War a Challenge for the DIRSPACEFOR." In *Joint Air and Space Operations, AY2007*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2006. Reprint, from *High Frontier*, vol. 1, no. 4, Space Warfighting. Headquarters US Air Force Space Command.

Cebrowski, Arthur K.; Garstka, John J. "Network-Centric Warfare: It's Origin and Future." *Proceedings*, no. January 1998 (1998).

"CENTCOM, Pentagon Confirm Destruction of GPS Jamming Equipment." *Defense Daily* Vol.217, Iss. 57 (26 March 2003).

Chernoff, Scott. "George Lucas Interview - the Story Comes First." Star Wars.com, http://www.starwars.com/episode-ii/bts/profile/f20020115/indexp4.html.

Church, George J. "Disarmament: How to Hide an A-Bomb." *Time* 08 July 1991.

Clancy, Tom, and Gen (Ret.) Chuck Horner. *Every Man a Tiger*. New York, NY: Berkley Books, 1999.

Cohen, Eliot A. "A Revolution in Warfare." *Foreign Affairs* (1996).

Cohen, Eliot, Conrad Crane, Jan Horvath, and John Nagl. "Principles, Imperatives, and Paradoxes of Counterinsurgency." *Military Review* 86, no. 2 (2006): 49-53.

Cooper, Scott. "Air Power and the Coercive Use of Force." In *Immaculate Warfare*, edited by Stephen D. Wrage. Westport, CT: Praeger, 2003.

Cortes, Lorenzo. "JASSM Costs Could Go up 100 Percent If Congressional Cuts Hold, Air Force Says." *Defense Daily*, 10 September 2003, 1.

Corum, James S., and Wray R. Johnson. *Airpower in Small Wars: Fighting Insurgents and Terrorists*. Lawrence, KS: University Press of Kansas, 2003.

de Haas, Dr. Marcel. "'Russia's Military Strategy: Preparing for the Wrong War?" Power and Interest News Report (PINR), http://www.pinr.com/report.php?ac=view_report&report_id=478&language_id=1.

de Haas, Maj Marcel. "The Use of Russian Air Power in the Second Chechen War." In *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2007. Reprint, from Royal Air Force, *Air Power Review*, vol. 6, no. 1. Director of Defence Studies, Spring 2003.

Dombrowski, Dr. Peter. "Alternative Futures in War and Conflict: Implications for U.S. National Security in the Next Century." In *An Occasional Paper of the Center for Naval Warfare Studies*. Newport, RI: Naval War College, Strategic Research Department Center for Naval Warfare Studies, April 2000.

Douhet, Giulio, General. "The Command of the Air." In *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2007. Reprint, from *The Impact of Air Power: National Security and World Politics*, Chapter 29. D. Van Nostrand Co., Inc., 1959. Originally published as a stand-alone work, *The Command of the Air*, in 1921.

Dunnigan, James. "F-22 Secrets Too Precious to Sell." http://www.strategypage.com/dls/articles/2007227221547.asp.

Eisendrath, Craig. "Why Is the U.S. Weaponizing Outer Space?" *USA Today Magazine* 135, no. 2740 (2007): 52-55.

Engelbrecht Jr., Col Joseph A., Lt Col Robert L. Bivins, Maj Patrick M. Condray, Maj Merrily D. Fecteau, Maj John P. Geis II, and Maj Kevin C. Smith. "Alternate Futures for 2025: Security Planning to Avoid Surprise." In *Air Force 2025*. Maxwell AFB, AL: Air University, April 1996.

Ennett, Jimmy. "The Impact of Emerging Technologies on Future Air Capabilities." edited by Defence Science and Technology Organisation Science Policy Division: Australian Department of Defence, 1999.

"Fear and Breathing." *Economist* 360, no. 8241 (2001): 37-37.

Federation of American Scientists. "Introduction to Biological Weapons: Biological Weapons Production." FAS.org, http://www.fas.org/biosecurity/resource/bioweapons.htm.

Fiszer, Michal. "Polish Troops in Iraq Getting Counter-IED Devices." *Journal of Electronic Defense* 29, no. 3 (2006): 18-19.

"Five-Year Plan (FY04 – FY08) for the Manufacturing Technology (ManTech) Program." Department of Defense, July 2003.

Fulghum, David A. "Eliminating Noise Key to Anti-Stealth Radar." *Aviation Week & Space Technology* 150, no. 3 (1999).

———. "New Radars Peel Veil from Hidden Targets." *Aviation Week & Space Technology* 150, no. 3 (1999).

———. "Sensor Mix Means No Place to Hide." *Aviation Week & Space Technology* 150, no. 3 (1999).

Garamone, Jim. "Review Changes Status of Nuclear Deterrent." *Pentagon Brief* (January 2002).

Garreau, Joel. *Radical Evolution*. New York: Doubleday, 2004.

Geis II, John P., Lieutenant Colonel, USAF. "Directed Energy Weapons on the Battlefield: A New Vision for 2025." Air University, April 2003.

Glenn, Jerome C., and The Futures Group International. "Scenarios." In *Futures Research Methodology--Version 2.0*. Washington, DC: American Council for the United Nations University, 2003.

Glenn, Jerome Clayton, Theodore J. Gordon, UN Millennium Project., and American Council for the United Nations University. *Environmental Scanning*. Version 2.0. ed, Futures Research Methodology. Washington, DC: American Council for the United Nations University the Millennium Project, 2003.

———. *Scenarios*. Version 2.0. ed, Futures Research Methodology. Washington, DC: American Council for the United Nations University the Millennium Project, 2003.

Global Security.org. "Small Diameter Bomb / Small Smart Bomb." Global Security.org, http://www.globalsecurity.org/military/systems/munitions/sdb.htm.

"Googlescholar.Com." http://www.scholar.google.com.

Gordon, Michael R., and Gen (Ret.) Bernard E. Trainor. *Cobra II: The inside Story of the Invasion and Occupation of Iraq*. New York, NY: Pantheon Books, 2006.

Goss, Thomas J., and Naval Postgraduate School (U.S.). "Building a Contingency Menu : Using Capabilities-Based Planning for Homeland Defense and Homeland Security." Naval Postgraduate School, 2005.

Gray, Colin S. "Another Bloody Century -- Future Warfare." In *Inter/National Security and War, AY07 Coursebook,* edited by Sharon McBride, 230-46. Maxwell AFB, AL: Air Command and Staff College, August 2006. Reprint, from *Another Bloody Century*. London: Weidenfield & Nicholson, 2005.

———. "Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?" In *Inter/National Security and War, AY07 Coursebook*, edited by Sharon McBride.

Maxwell AFB, AL: Air Command and Staff College, August 2006. Reprint, from *Strategic Studies Institute (SSI) Monograph*. US Army War College, March 2006.

Griffith, Dr. Lewis. "Defining Globalization." Maxwell AFB, AL, 2006.

Headquarters Department of the Army, and Headquarters Marine Corps Combat Development Command. "Field Manual (FM) 3-24 and Marine Corps Warfighting Publication (MCWP) 3-33.5: Counterinsurgency." Department of the Army and Department of the Navy, December 2006.

Hebert, Adam J. "Compressing the Kill Chain." *Air Force Magazine* 86, no. 3 (2003).

Helmenstine, Anne Marie, Ph.D. "Chemical Weapons and Warfare Agents." About.com, http://chemistry.about.com/cs/chemicalweapons/a/aa040303a.htm.

Hitchens, Theresa, Michael Katz-Hyman, and Jeffrey Lewis. "U.S. Space Weapons." *Nonproliferation Review* 13, no. 1 (2006).

Hurley, Alfred F. *Billy Mitchell: Crusader for Air Power*. Bloomington, IN: Indiana University Press, 1975.

Hutchinson, Robert. *Weapons of Mass Destruction : The No-Nonsense Guide to Nuclear, Chemical and Biological Weapons Today*. Cassell military paperbacks ed, Cassell Military Paperbacks. London: Cassell, 2004.

International Crisis Group. "Iran: Is There a Way out of the Nuclear Impasse?" International Crisis Group, Middle East Report No. 51, 23 February 2006.

Israel Aerospace Industries LTD. "Dragon Eye Miniature UAV." http://www.defense-update.com/products/d/dragoneyes.htm.

———. "Rpg-7/Rpg-7v/Rpg-7vr Rocket Propelled Grenade Launcher (Multi Purpose Weapon)." http://www.defense-update.com/products/r/rpg.htm.

Johnson, David E. "Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era." In *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2007. Reprint, from *Learning Large Lessons: The Evolving Roles of Grond Power and Air Power in the Post-Cold War Era*, Chapters 3 and 4. RAND, 2006.

Johnson, Ronald M., and U.S. Army Command and General Staff College. "Application of Aspects of Unconventional Warfare : Tools for Engaging the Current and Future Threat Trends of the Post-Cold War Environment." U.S. Army Command and General Staff College, 1999.

Joseph, Earl C. "Forecasting Change and Developing Futures." Walden University, 2002.

Kem, Jack D. *Campaign Planning : Tools of the Trade*. 2ND ED ed: US ARMY COMM & STAFF COLL, 2006.

Koeppel, Dan. "Can This Fruit Be Saved?" *Popular Science* August 2005.

Kornblum, John. "Help Wanted in Iraq." *The Washington Post*, 27 June 2006.

Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. New York, NY: Penguin Group, Sept. 2005.

Lake, James P., Maj., USAF. Email, 05 September 2006.

Larsen, Jeffrey; Wirtz, James J.; Croddy, Eric A. *Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology, and History*. Edited by James J. Wirts: Abc-Clio Inc, 2004.

Levin, Senator Carl. "Statement of Senator Carl Levin on Armor Piercing Ammunition." In *FDCH Press Releases*.

Liang, Qiao, and Wang Xiangsui. "Unrestricted Warfare." Beijing: PLA Literature and Arts Publishing House, February 1999.

"Lockheed Martin Successfully Tests Low-Cost Autonomous Attack System." *Defense Daily* 228, no. 21 (04 November 2005).

Lorber, Azriel. *Misguided Weapons: Technological Failure and Surprise on the Battlefield*. Dulles, Virginia: Brassey's, Inc., 2002.

Luker, Joel J., Maj., USAF. "State Actor Threats in 2025." United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007.

Mansbach, Richard W., Yale H. Ferguson, and Donald E. Lampert. *The Web of World Politics : Nonstate Actors in the Global System*. Englewood Cliffs, N.J.: Prentice-Hall, 1976.

"Military." *GPS World* 16, no. 12 (2005): 48.

"Missile Monitor." *Journal of Electronic Defense* 25, no. 12 (2002): 43.

Mitchell, William. *Winged Defense*. Mineola, New York: Dover Publications, Inc., 1925; reissued in 2006.

Muradian, Vago. "China's Mystery Satellites." *C4ISR Journal* 6, no. 2 (2007): 42-43.

———. "China Attempted to Blind U.S. Satellites with Laser " DefenseNews.com, http://www.defensenews.com/story.php?F=2121111&C=america.

———. "Pentagon Turns Attention to Chinese Space Threat." *Air Force Times* 67, no. 30 (2007): 18.

Myers, James "Buster", Maj., USAF. "Non-State Actor Threats in 2025." United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007.

National Aeronautics and Space Administration (NASA). "Deep Impact Kicks Off Fourth of July with Deep Space Fireworks." http://www.nasa.gov/mission_pages/deepimpact/media/deepimpact-070405-1.html.

Newmyer, Jacqueline A. "China's Air-Power Puzzle." *Policy Review* (June & July, 2003): 71-85.

O'Sullivan, Patrick. "A Geographical Analysis of Guerilla Warfare." *Political Geography Quarterly* 2, no. 2 (1983): 11.

Pacella, Rena Marie. "Man-Made Black Holes." *Popular Science* January 2006.

Parks, Raymond C., and David P. Duggan. "Principles of Cyber-Warfare." Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY 5-6 June, 2001.

Peacock, Brent, Maj., USAF. "Connecting the Edge: Mobile Ad-Hoc Networks (Manets) for Network-Centric Warfare." United States Air Force (USAF) Air Command and Staff College (ACSC), April 2007.

Phaal, R.; Farrukh, Clare, Probert, David R. "Technology Roadmapping--a Planning Framework for Evolution and Revolution." *Technological Forecasting and Social Change* (2003).

Pirnie, Bruce R., Alan Vick, Adam Grissom, Karl P. Mueller, and David T. Orletsky. "Kosovo (Operation Allied Force)." In *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2007. Reprint, from *Beyond Close Air Support: Forging a New Ground-Air Partnership*, Chapter 3. RAND, 2005.

"Production Fuzion." *Aviation Week & Space Technology* 165, no. 12 (2006): 53.

"Restructuring Plan for Anti-Satellite Program." *Aviation Week & Space Technology* 126, no. 11 (1987): 19.

Rich, Ben R., and Leo Janos. *Skunk Works*. New York: Little, Brown and Company, 1994.

Richardson, Doug. *Stealth Warplanes*. Osceola, WI: MBI Publishing, 2001.

Rivers, Brendan P. "US Army Seeks New System to Counter IEDs." *Journal of Electronic Defense* 28, no. 4 (2005): 22-23.

Romano, Allison. "CBS Scandal, Local Fallout." *Broadcasting & Cable* 135, no. 3 (2005): 26-26.

Rossi, Carole, Benoît Larangot, Pham Phuong-Quyên, Danick Briand, Nicolass F. de Rooij, Manel Puig-Vidal, and Josep Samitier. "Solid Propellant Microthrusters on Silicon:

Design, Modeling, Fabrication, and Testing." *Journal of Microelectromechanical Systems* 15, no. 6 (2006): 1805-15.

Scearce, Diana, Katherine Fulton, and The Global Business Network Community. "Scenario Thinking in Practice." In *Leadership, Command and Professional Development; Leadership and the Staff Environment II LB Course*, edited by Sharon McBride, 33-51. Maxwell AFB, AL: Air Command and Staff College, 2004. Reprint, from *What If? The Art of Scenario Thinking for Nonprofits*, Chapter 2. Global Business Network, 2002.

Schnaars, Steven, and Paschalina Ziamou. "The Essentials of Scenario Writing." *Business Horizons* 44, no. 4 (2001).

Sellers, Jerry Jon. *Understanding Space: An Introduction*. Edited by Douglas H. Kirkpatrick. Revised 2nd ed. Boston, MA: McGraw-Hill, 2004.

Sherman, Gabriel, Eric Adams, Sarah Goforth, and William Jacobs. "Maximum Velocity." *Popular Science*, February 2005, 46.

Shimeall, Timothy, Phil Williams, and Casey Dunlevy. "Countering Cyber War." *NATO Review* (Winter 2001/2002): 16-18.

Sloggett, Dave. "Decision Superiority in Operations Other Than War." *Jane's Defence Weekly* 42, no. 48 (2005): 17-17.

"Space Weapons Policy." *Congressional Digest* 63, no. 3 (1984): 67.

Squassoni, Sharon. "Iran's Nuclear Program: Recent Developments." Library of Congress Congressional Research Service, 23 November 2005.

Stephenson, Michael. *Battlegrounds : Geography and the History of Warfare*. Washington, D.C.: National Geographic, 2003.

Stewart, Cameron. "US Rules out Deal on F-22." *The Australian*, 14 February 2007.

Strange, Susan. *The Retreat of the State : The Diffusion of Power in the World Economy*, Cambridge Studies in International Relations ;. New York: Cambridge University Press, 1996.

Sweetman, Bill. *Lockheed Stealth*. St. Paul, MN: MBI Publishing, 2001.

———. "Worth the Cost?" *Jane's Defence Weekly* 43, no. 29 (2006): 59-63.

Takacs, Maj. J. "The Russian Air Force in Chechnya: Have Lessons Been Learnt and What Are the Future Perspectives?" In *Expeditionary Air and Space Warfare, Academic Year 2007 Coursebook*, edited by Sharon McBride. Maxwell AFB, AL: Air Command and Staff College, 2007. Reprint, from Royal Air Force, *Air Power Review*, vol. 4, no. 4. Director of Defense Studies, Winter 2001.

Tynan, Dan. "The Internet Is Sick...But We Can Make It Better." *Popular Science*, October 2006, 82.

U.S. Army Training and Doctrine Command (TRADOC). "A Military Guide to Terrorism in the Twenty-First Century: TRADOC DCSINT Handbook No.1." Ft. Leavenworth, KS: United States Army, 2005.

United States. Dept. of Defense. Office of Force Transformation. *Elements of Defense Transformation*. Washington, DC, Oct 2004.

United States. Dept. of Defense. Office of the Secretary of Defense. "Annual Report to Congress: Military Power of the People's Republic of China (2006)." 2006.

United States. Dept. of Defense. Secretary of Defense. *2006 Quadrennial Defense Review*. Washington, DC, 2006.

United States. Dept. of the Air Force. Chief of Staff. *The Edge: 2005 Air Force Transformation*. Washington, DC, 2005.

———. *The U.S. Air Force Transformation Flight Plan 2004*. Washington, DC, 2004.

United States. Dept. of the Air Force. HQ USAF/A8X. *Air Force Roadmap 2006 > 2025*. Washington, DC, 2006.

United States. Dept. of the Air Force. Secretary of the Air Force. *Air Force Doctrine Document (AFDD) 1: Air Force Basic Doctrine*. Washington, DC: Dept. of the Air Force, 17 November 2003.

———. *Air Force Doctrine Document (AFDD) 2-1.3: Counterland Operations*. Washington, DC: Dept. of the Air Force, 12 September 2006.

———. *Air Force Doctrine Document (AFDD) 2-5: Information Operations*. Washington, DC: Dept. of the Air Force, 11 January 2005.

United States. Joint Chiefs of Staff. "Joint Publication (JP) 3-13: Information Operations." Department of Defense, 2006.

Van Riper, Paul K. "Information Superiority." *Marine Corps Gazette* 81, no. 6 (1997): 54.

Varni, Jamie G. G., Lt Col, USAF, Gregory M. Powers, Dan S. Crawford, Maj, USAF, Craig E. Jordan, Maj, USAF, and Douglas L. Kendall, Maj, USAF. "Space Operations: Through the Looking Glass." In *Air Force 2025*. Maxwell AFB, AL: Air University, April 1996.

Vizard, Frank. "Attempts to Jam U.S. GPS-Based Weapons and Navigation Systems in Iraq Were a Reminder of Just How Vulnerable the Technology Is " Scientific American.com, http://www.sciam.com/article.cfm?articleID=00079DD3-DAA0-1E96-8EA5809EC5880000.

von Clausewitz, Carl. *On War*. Translated by Michael Howard and Peter Paret. Edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Warrick, Joby. "Custom-Built Pathogens Raise Bioterror Fears." *The Washington Post*, 31 July 2006.

Waxman, Matthew C., and Project Air Force (U.S.). *International Law and the Politics of Urban Air Operations*. Santa Monica, CA: Rand, 2000.

"Weapons Testing." *Air Force Times* 58, no. 6 (1997): 24.

Wikipedia.com. "List of States with Nuclear Weapons." http://en.wikipedia.org/wiki/List_of_states_with_nuclear_weapons.

———. "OODA Loop." http://en.wikipedia.org/wiki/OODA_Loop.

———. "Rocket-Propelled Grenade." http://en.wikipedia.org/wiki/Rocket_propelled_grenade.

Williams, Mark. "Technology and the Future of Warfare." *Technology Review (MIT)*, 23 Mar 06.

Wrage, Stephen D. "Conclusion." In *Immaculate Warfare*, edited by Stephen D. Wrage. Westport, CT: Praeger, 2003.

Wynne, Michael W., Secretary of the Air Force. "Cyberspace as a Domain in Which the Air Force Flies and Fights." Paper presented at the C4ISR Integration Conference, Crystal City, VA 02 November 2006.