AU/ACSC/16-4206/2004-05

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

# AGAINST ALL ENEMIES FOREIGN AND DOMESTIC:

# FUTURE SCENARIOS OF NATIONAL SECURITY AND THE CONSTITUTION

by

Cameron G. Holt, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Instructors: Lt Col John T. Ackerman

Maj Cynthia A. Wright

Maxwell Air Force Base, Alabama

April 2005

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **APR 2005** | | **00-00-2005 to 00-00-2005** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **AGAINST ALL ENEMIES FOREIGN AND DOMESTIC: FUTURE SCENARIOS OF NATIONAL SECURITY AND THE CONSTITUTION** | 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 Press (AUL/LP),131 W Shumacher Avenue,Maxwell AFB,AL,36112-6615** | 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

**Every American military commissioned officer serving in uniform today took a solemn oath "to support and defend the Constitution of the United States against all enemies, foreign and domestic " As America's military transforms to defeat current and future threats, could the pursuit of national security unwittingly endanger the very Constitution we are sworn to defend? What future scenarios must America's military be ready for by the year 2020, and what are the implications for the current transformation effort throughout the Department of Defense? This paper explores these critical questions using the scenarios-based future planning methodology described by Peter Schwartz in his book The Art of the Long View: Planning for the Future in an Uncertain World. The intent of this process is to encourage what Peter Schwartz calls an ongoing "strategic conversation."**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **50** | |

## Disclaimer

The views expressed in this academic research paper are those of the author(s) 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.

## *CONTENTS*

# *ILLUSTRATIONS*

# *TABLES*

# *PREFACE*

**Background: Shifting Tectonic Plates of National Security and Civil Liberty**

In retrospect, the end of the Cold War was a geopolitical earthquake of epic proportions. As the aftershocks subsided, the world cautiously and collectively emerged from the previously tense but well-understood bipolar landscape to discover a more hopeful yet unfamiliar world. Throughout the 1990s, American national security policy struggled through an uncomfortable identity crisis. Looking through the state-centric lens of the past, the world's sole remaining superpower saw current security threats as far less direct and immediate than those of the Cold War era, albeit more diverse. As Naval War College Professor Thomas Barnett observed, policy makers decided, "America was better served adopting a wait-and-see strategy…one that assumed some grand enemy would arise in the distant future. It was better than wasting precious resources trying to manage a messy world in the near term. The grand strategy…was to avoid grand strategies" (Barnett, 2004, 1). That would soon change.

As the sun set on September 11, 2001, America was forced to look at national security, and at least temporarily civil liberty, through a new lens. For the first time, asymmetric threats posed by individuals and networked non-state sponsored terrorist cells worldwide represented a clear and present danger to the US homeland. For all of its relative strength, America's national security apparatus was wholly unprepared to wage war against these individuals, not only around the world, but also within its own borders. The inevitable "re-tooling" to fight a new kind of war began just weeks later with the passage of the now controversial "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act (Barr, 2001, 10). The act removed longstanding information sharing restrictions between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). It also provided several new tools to investigate terrorism within the US, like facilitating delayed notice search warrants, relaxing wire tapping rules,

and even suspending due process as deemed appropriate for individuals declared to be enemy combatants.

The next major national security policy shift came with the "Bush Doctrine." Cast within the context of a global war on "terrorism" versus "terrorists," the Bush Doctrine played to the strength of the US military--conventional warfare between states--by equating states that harbor terrorists with the terrorists themselves. This first phase of the Global War on Terrorism (GWOT) rocketed failing states from a largely peripheral humanitarian interest to a vital national security imperative. Although US policy embraced the concepts of global humanitarian intervention and democratization prior to 9/11, the only specific reference to failing states in the December 2000 national security policy statement noted, in the context of crisis prevention, that "…helping failing states is less burdensome than rebuilding failed states…"(Clinton, 2000, 10). In contrast, the post-9/11 policy statement of September 2002 reported that "America is now threatened less by conquering states than we are by failing ones" (Bush, 2002, 1).

As of 2005, with Operations ENDURING FREEDOM and IRAQI FREEDOM ongoing, the US military continues to have an outward focus in this first state-centric phase of GWOT. Important structural changes to the national security system since 9/11, however, provide a new capability for future full spectrum operations *inside* the US if necessary with the creation of the Department of Homeland Security (DHS), a new regional combatant command (US Northern Command) and a National Intelligence Director. Will we ever need that capability to conduct full spectrum operations inside the US and, if so, what would be the Constitutional implications of the emerging military and commercial technologies that will likely be employed? The answers could be alarming.

**Acknowledgments**

There are a few people who deserve my heartfelt gratitude for helping me produce this paper without losing my mind. Top honors go to my wife, Kelly, and my two boys, Mitchell and Luke for their patience with the many hours I spent “holed up.” They don’t know I used them in one of the scenarios yet, so don’t tell them. It must be depressing enough for my four-year-old son to hear that his 36-year-old father is still in school doing homework. I would also like to thank Lt Col John Ackerman for setting the perfect environment for creativity and learning in the Future Trends Seminar. Next on the list are my “whiz-kid” seminar classmates—I enjoyed our engaging discussions about future trends. A very special thank you goes to the Assistant Course Instructor, Major Cindy Wright, who went way above and beyond to provide great feedback to me and other students despite her preparations to move on to a squadron command position. I have no doubt she is fighting back several ideas about how to improve this paragraph as she reads it for the first time. Another debt of gratitude goes to the smartest person I know, my Mother, for the great conversations we have as we solve all the world’s problems together. Last but not least, I want to thank God for taking care of my future scenario regardless of how often I try to mess it up.

## *ABSTRACT*

Every American military commissioned officer serving in uniform today took a solemn oath "to support and defend the Constitution of the United States against all enemies, foreign and domestic…" *As America's military transforms to defeat current and future threats, could the pursuit of national security unwittingly endanger the very Constitution we are sworn to defend?* What future scenarios must America's military be ready for by the year 2020, and what are the implications for the current transformation effort throughout the Department of Defense? This paper explores these critical questions using the scenarios-based future planning methodology described by Peter Schwartz in his book *The Art of the Long View: Planning for the Future in an Uncertain World.* The intent of this process is to encourage what Peter Schwartz calls an ongoing "strategic conversation."

# INTRODUCTION

## Orientation/Focal Issue

Every American military commissioned officer serving in uniform today took a solemn oath "to support and defend the Constitution of the United States against all enemies, foreign and domestic…" (AF Form 133, Oath of Office). This oath is not so remarkable for the words it contains as for the words it lacks. No reference is found of allegiance to the President or superior officers, nor is there even any specific promise to provide for national security. While the omitted references to the President and superior officers are quite intentional, support and defense of the Constitution of the United States (US) has historically been synonymous with support and defense of national security.

The attacks of September 11, 2001, however, changed the nature of national and international security in ways the world is still struggling to comprehend almost four years later. *As America's military transforms to defeat current and future threats, could the pursuit of national security unwittingly endanger the very Constitution we are sworn to defend?* What future scenarios must America's military be ready for, and what are the implications for the current transformation effort throughout the Department of Defense? This paper explores these critical questions using the scenarios-based future planning methodology described by Peter Schwartz in his book *The Art of the Long View: Planning for the Future in an Uncertain World*.

## Methodology and Scope

Although the basic scenarios-based future planning process can have variations, it is decidedly qualitative and seeks not to predict a single future but rather to illustrate extreme, and sometimes even fanciful, scenarios that may frame a range of possible futures and produce indicators relevant to the focal issue. Because a quantitative trend analysis may be forced to marginalize key driving forces that defy measurement by using simple stochastic variables, the highly unpredictable nature of future events

suggests a less deterministic approach. The scenarios method embraces the most uncertain and important driving forces from a qualitative viewpoint as the central variables that define future scenarios. In a historic continuum replete with examples of unpredictable events driving discontinuous change, this qualitative scenarios methodology can provide a logical basis for strategic leaders to see beyond current paradigms and prepare now for an uncertain future.

Figure 1 below illustrates the primary activities in the scenarios-based future planning process. The orientation process in phase one consists of research to determine what key questions might be critical to the future. The output is the focal issue. The exploration effort in phase two identifies driving forces that most affect the focal issue, prioritized by importance and categorized as either *predetermined elements* or *critical uncertainties* depending upon predictability. The synthesis process takes the two most important and most uncertain driving forces to form the basis of a graph from which four scenarios may be extrapolated. The result is fictional accounts of each scenario that provides a logical progression of events from the present to the end state defined by the scenario and a sense of what it might be like to live in such a world. Phases four and five form the conclusions by identifying *leading indicators* to watch for as the future unfolds and the key *implications and actions* necessary to prepare for the range of possible futures. The intent of the process as a whole is to encourage what Peter Schwartz calls an ongoing "strategic conversation" (Schwartz, 1991, 227).

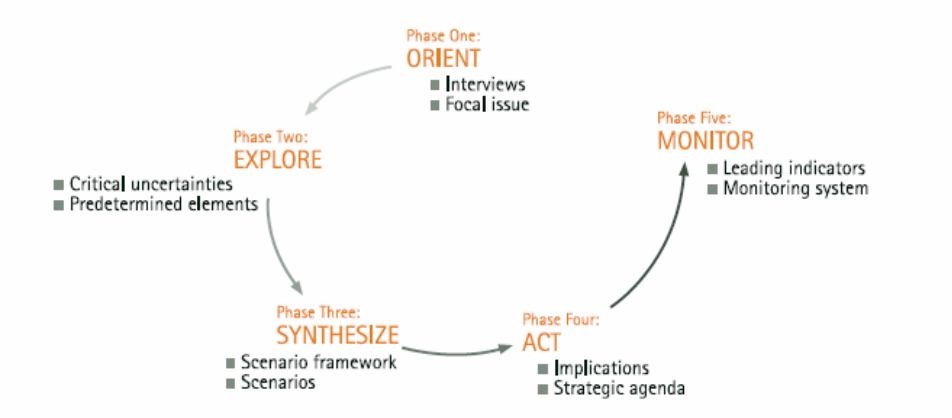

**Figure 1: The Scenarios-Based Planning Process**

**Source:** Global Business Network, "*What If? The Art of Scenario Thinking for*

Driving forces are those second- and perhaps third-order underlying variables that have the greatest influence over the direction of the focal issue. While they may not have a direct, or linear, causal relationship with the focal issue, they do form a logical foundation for the future world scenarios. They are prioritized by importance to the focal issue within two categories: *predetermined elements* and *critical uncertainties.* The predetermined elements are reasonably predictable driving forces, to include the expansion of key technologies and the established protections of the US Constitution. The critical uncertainties are those driving forces that are either inherently unpredictable or depend upon future choices that are not yet well understood. They include the nature of future threats to US national security, the public demand for protection of civil liberties and the degree of commercial technology integration with national security innovations (Schwartz, 1991, 101).

**Predetermined Elements**

**Expansion of Key Technologies**

The continued expansion of key commercial and military technologies is highly likely by the year 2020 and will be the most important driving force affecting the focal issue. Emerging commercial technologies such as radio frequency identification (RFID), biometrics, and database interconnectivity and mining will all be expanded and integrated. They will also likely be combined with existing commercial applications of the internet, global positioning system (GPS), nanotechnology, audio-video surveillance and wireless communications in novel ways to support new capabilities. The expansion and integration of commercial technologies alone will force the US to face serious Constitutional questions concerning civil liberties regardless of whatever else occurs between 2005 and 2020. On the military side, the two key concepts of persistent intelligence, surveillance, and reconnaissance (ISR)

and network-centric warfare (NCW) will drive the development and deployment of new technologies that may or may not affect American civil liberties depending upon whether the resulting technologies are employed within the US.

Of all the emerging commercial technologies, RFID has perhaps drawn the most attention and concern from civil liberties advocates in the US. At present, RFID technology consists of paper-thin tags, sensors that activate and read the tags, and a remote database managed by EPC Global Corporation with data about the tagged item. In this basic form, RFID has already begun to replace Universal Product Code (UPC) labels at Wal Mart and other retailers. The Department of Defense (DoD) used RFID to track shipping containers during Operation IRAQI FREEDOM and has since ordered RFID tags to track its entire supply chain (Engels, 2004, 2).

So what is the fuss about? RFID is capable of far more than just logistics management. Individual consumer profiles and other data can be stored on the tag itself. Powered RFID tags can actively emit this data, and RFID tags with embedded data and GPS locators can track something--or someone--globally. Tags can be read by invisible readers without consent or knowledge, and tags can be read from increasing distances even after purchases are made—a disturbing prospect if the tagged items are within residences or embedded in clothing.

RFID tags are already used in a rapidly expanding variety of applications, such as to facilitate automatic payment when driving through tollbooths and to track border crossings. They are also used in library books, leased vehicles, passenger bags at some airports, and livestock (Tien, 2004, 1). Later this year all US passports will have RFID tags with non-encrypted biometric data, and the IRS is considering tagging all cash as an anti-counterfeiting measure. RFID-tagged drivers' licenses may be next (Singel, 2004, 1). Although not yet combined with RFID, the US Food and Drug Administration recently approved the use of GPS-enabled VeriChip™, marketed by Applied Digital Solutions as the

first implantable chip. This chip is already being implanted into children in South America as an anti-kidnapping device and into Mexican Government officials as a facilities security measure (Scheeres, 2002, 1).

Biometrics is another key technology that is likely to expand significantly and has at least the potential to lead to the death of anonymity. Certainly biometrics such as iris scanning, finger scanning, three-dimensional holographic scanning, and DNA analysis are nothing new. It is the database collection, storage, and integration of biometric capabilities with other technologies--such as facial mapping recognition with digital cameras and DNA record collection--that will likely create future civil liberties concerns for the public.

Facial mapping is already revolutionizing border control and law enforcement capabilities. According to the Electronic Privacy Information Center (EPIC), the DHS United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program requiring finger scans and digital photographs to be collected on all foreign visitors has collected over 16.9 million biometric records and is adding approximately 33,000 daily. Although DHS credits US-VISIT with identifying and apprehending 372 people wanted by federal, state or local law enforcement officials to date, US-VISIT has yet to catch any known terrorists (EPIC, 2005, 2). When combined with the ongoing proliferation of digital surveillance cameras in government and commercial spaces, people could unknowingly be identified and matched with records indicating their tax payment status, purchasing patterns, or other information (Gallagher, 2004, 2).

DNA record collection and storage is also likely to expand. The Justice for All Act of 2004 expanded the FBI's Combined DNA Index System (CODIS) database to include anyone *indicted* for a crime in addition to the over 1.5 million existing records on convicted criminals (Simoncelli, 2004, 1). Although the original bill permitted any legal DNA collection to be added to CODIS, privacy rights

advocates successfully avoided that provision. As human genomics mapping technology advances, pre-diagnoses of diseases through DNA analysis may one day be commonplace. This would likely expand the number of DNA records captured on the public exponentially without the need for mandatory collection. Although the law currently allows stiff fines for the illegal release of DNA records, whether access to those commercial records will—or even can—be controlled remains to be seen.

Database interconnectivity and mining may become the genie that we all one day wish we could put back in the bottle. Interconnectivity and mining are likely to be the critical emerging technology since storage capacity is already vanishing as a constraint.[1] If Acxiom, ChoicePoint, LexisNexis, Seisint, and Verint are not now household names, they soon will be. These companies have close ties to credit bureaus and voraciously collect and sell personal information in their mission to "find new ways to collect, track, monitor and profile people with data, and to find new ways to make money off of it" (O'Harrow, 2005, 49). There are few limits to the kinds of data that can legally be captured and sold, and the data mining methods employed provide instant access to huge dossiers about individuals when any one piece of information, like a captured caller identification telephone number, is known.

Although Congress killed a controversial DoD anti-terrorism database linking and mining effort known as Total Information Awareness (TIA), many believe the same research continues under other programs, like the $64 million "Novel Intelligence for Massive Data" program run by the Advanced Research and Development Activity (ARDA). That software would be capable of expanding the amount of data collected at the rate of four petabytes per month and could include digital audio and video surveillance streams (Sniffen, 2004, 2). In addition, Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 authorized the creation of a massive Information Sharing

Environment (ISE) to capture and analyze information on terrorists and individuals inside or outside the US that are suspected to have ties to transnational terrorism (P.L. 108-458, 2004, 15). Although there are several legal limits to the kinds of data the Government can collect, there are few restrictions on the data that can be obtained from private data aggregators. These data aggregators maintain that individuals bear the responsibility to control what information about them is used by third parties, but there is currently no realistic way for people to know who has what information about them. The recent theft of personal dossiers and records from ChoicePoint, LexisNexis, Seisint, Bank of America and the Nevada Department of Motor Vehicles may leave some wishing they did know (Associated Press, 2005, 1).

The military technologies that result from DoD's current pursuit of persistent ISR and network-centric warfare (NCW) may or may not impact civil liberties, but there is little doubt they will enhance the military's already considerable capability to find, fix, track, target, engage and attack any target worldwide, with lethal or non-lethal effects. The pursuit of persistent ISR will likely mean layered sensors that literally saturate the battlespace with actionable target-quality ISR. This may involve everything from ground robots and backpack-portable unmanned aerial vehicles (UAVs), to an "every-system-a-sensor" approach in the oceans and in the atmosphere, to long-loiter balloons at the edge of space and a protected constellation of satellites in every orbit. The pursuit of NCW will demand changes to "organizational structures, processes, tactics and the way the choices are made" in addition to technology innovations. It will enable horizontal, as well as vertical, information sharing and will result in all-source shared situational awareness at every level (Cebrowski, 2005, i). The fusion of biometric technologies and persistent ISR/NCW with massive commercial databases, unrestricted by

[1] Storage capacities are now measured in petabytes. Just one petabyte is roughly equivalent to 40 pages of text for each of the 6.2 billion people on Earth (Sniffen, 2004, 2).

controls on law enforcement methods, is the tidal wave making technology a driving factor in future scenarios.

**Established Protections of the US Constitution**

Proliferating technology may well put the US on a collision course with the protections guaranteed by the Constitution, which every military officer has sworn to support and defend. At risk are the personal privacy protections of the Fourth Amendment, the due process protections of the Fourteenth Amendment, and the protections against self-incrimination--and perhaps also the "just compensation for takings" guarantee—found in the Fifth Amendment.

The Fourth Amendment reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…describing the place to be searched, and the persons or things to be seized. (Amendment IV, Search and Seizure, US Constitution).

Although the words "secure…against unreasonable searches and seizures" do not specifically refer to a right of privacy, subsequent Supreme Court rulings held that a technological intrusion of privacy violates the Fourth Amendment. In a 1960s wiretapping case, no warrant was obtained for electronic surveillance conducted by the police. Justice Potter Stewart explained, "The Fourth Amendment protects people not places. If people have the legitimate expectations of privacy, such as in their home, then they may invoke the protection of the Constitution to ensure that privacy" (Urofsky, 2003, 47). In *Berger v. New York* (1967) the Supreme Court struck down a New York statute permitting electronic eavesdropping because it failed to require police to establish a specific probable cause for the surveillance as required by the Fourth Amendment (Clark, 1967, 15). New pervasive surveillance capabilities may or may not compel the courts to extend the current "legitimate expectation of privacy" standard to well beyond the home.

The salient portion of the Fourteenth Amendment reads as follows:

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws. (Amendment XIV, Citizenship Rights, US Constitution).

America's characterization of the 9/11 attacks on New York and Washington D.C. as *acts of war* rather than simply *transnational organized crime* was pivotal. It authorized broad powers that enabled government to respond using national security processes rather than more restrictive law enforcement measures. Military tribunals were stood up to prosecute those declared to be enemy combatants, a military detention and interrogation facility was established outside US territory in Cuba, and the USA PATRIOT Act empowered federal law enforcement officials with broad authorities to investigate any crimes under the auspices of national security as long as simple relevance, rather than probable cause, could be established. The details of these investigations, to include surveillance and searches, are classified and therefore not available to the public or even to those under investigation. Although it is tough to generate any sympathy for individuals connected to Al Qaeda who are searched without probable cause or detained without formal charges, this has understandably raised Fourteenth Amendment due process concerns among civil liberties groups. Future investigations of US citizens under the auspices of national security may well broaden and deepen these due process concerns.

The Fifth Amendment reads as follows:

> No person...shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation. (Amendment V, Trial and Punishment, Compensation and Takings, US Constitution).

The ubiquitous surveillance and personal data exploitation that appears to be an inevitable part of future society may well raise substantial concerns over Fifth Amendment protections against self-incrimination. The US Supreme Court has repeatedly held that the Fourth and Fifth Amendments are

closely related and together provide a comprehensive liberty against unreasonable intrusion by the Government. Pervasive and indiscriminate surveillance and data collection, either collected by the Government directly or obtained from private third-party sources, could effectively negate any reasonable opportunity for citizens to avoid self-incrimination. Chief Justice Earl Warren commented in *Lopez v. United States* (1963) even as he upheld a lower court's admittance of electronic surveillance as evidence,

> …the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual…Indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments…(in Clark, 1967, 15).

Although somewhat less likely, another future debate may revolve around the Fifth Amendment's guarantee of just compensation for the seizure of private property for public use. As any seasoned paparazzi can doubtless explain, the current "legitimate expectation of privacy" standard provides little protection of privacy, or ownership of pictures taken, outside the home. Likewise, as ChoicePoint and Acxiom might argue, current law suggests that individuals generally forfeit their privacy and ownership interests in any personal information provided to others voluntarily for some product, service or convenience. This is true even if the individual is unaware of the potential for their information to be exploited for commercial or Governmental purposes (O'Harrow, 2005, 6). This kind of "transactional forfeiture" of privacy and ownership of personal information could become so invasive and coercive as to erode the basic civil right to pursue life, liberty and property. Such a future may well precipitate a change in law, or to the Constitution itself, that allows individuals to retain some form of ownership of their personal information unless justly compensated under the Fifth Amendment.

**Critical Uncertainties**

**Nature of Future Threats to US National Security**

Whether the nature of future threats to US national security will support the military's current outward, state-centric focus is the most critical uncertainty affecting the focal issue. The threat of transnational terrorism from Al Qaeda and other violent non-state actors is still considerable four years after 9/11. Even so, the main thrust of military operations since 9/11 in response to that surprisingly concentrated threat has been largely state-centric and outside the US—most notably in Afghanistan and Iraq. Other near-term threats posed by Iran, Syria and North Korea, while worrisome, do not disrupt the military's current outward focus. Will threats to US national security continue to be mostly concentrated and external in 2020 or could events demand an inward focus from America's military? Two prominent prognosticators of post-Cold War era international order and conflict, Samuel P. Huntington and Thomas P.M. Barnett, may provide some valuable insights into the sources of future threats.

Samuel P. Huntington, author of *Clash of Civilizations and the Remaking of World Order*, envisioned future threats emerging along a plurality of global "fault lines" between civilizations with distinct cultural differences. He defines nine major civilizations to include Western, Latin American, African, Islamic, Sinic, Hindu, Orthodox, Buddhist and Japanese. Huntington suggests that "alignments defined by ideology and superpower relations are giving way to alignments defined by culture and civilization" (Huntington, 1996, 125). He foresees protracted, almost communal, conflicts between groups from different civilizations along these cultural "fault lines." According to Huntington, these violent "on again, off again" struggles will be difficult to resolve through negotiations or compromise because they revolve around cultural identity rather than political ideology (Huntington, 1996, 253).

Thomas P.M. Barnett, author of the more recent *The Pentagon's New Map: War and Peace in the Twenty-First Century*, foresees future conflicts concentrating along a "rule set" boundary between the "Functioning Core" of globalized nations and the "Non-Integrating Gap" of disconnected nations and societies. According to Barnett, this Non-Integrating Gap includes most of Central America and the Caribbean, northern and western portions of South America, most of Africa, the Balkans, all of the Middle East, central and southeast Asia and Indonesia. The comprehensive and interdependent rule set governing the western-style "Functioning Core" drives less violence and common interests within that system. The Non-Integrating Gap, however, includes an assortment of motivations and agendas. There are states pursuing greater economic connectivity with the world that must willingly accept a broad range of western political and security rule sets. There are also regimes that attempt to defy these rule sets out of fear they may lose control over their people that are consequently labeled "rogue regimes." Perhaps the most dangerous element within the "Non-Integrating Gap," however, is what Barnett calls the rise of the "lesser includeds." Like Al Qaeda, these violent individuals actively fight globalization because they see the western rule sets as a direct threat to their society and power (Barnett, 2004, 83).

At first glance, the global lines governing the locations and sources of future conflict drawn by either Huntington or Barnett seem to indicate a continuation of the military's current outward focus. Certainly as President Bush begins his second term with a diplomatic "full-court-press" to spread democracy as a means to end tyranny and achieve greater global stability, elements of both Huntington's and Barnett's hypotheses are evident in the world's reaction. If large-scale civil wars or broader theater wars result from the mounting global pressure on Iran or other non-democratic states to conform to a western agenda, the predominant threats to US national security may well remain concentrated and external for many years to come. If Huntington and Barnett are only partially correct,

however, the future could be far muddier for the US military and far more threatening for the Constitution and the American way of life. It is possible that the threats outlined by Huntington's cultural "fault lines" or by Barnett's rise of the "lesser includeds" may be taking shape now from within the "Western Civilization" or the "Functioning Core" themselves. If one day it becomes clear that the lines of conflict can no longer be drawn on any world map, America's national security focus could turn inward quickly. If that day ever comes, *posse comitatus* will likely be the first casualty of war. Soon thereafter, the cascading effects of public-private technology integration and other driving factors could work together to make the pursuit of national security and the defense of the Constitution divergent goals.

**Public Demand for Protection of Civil Liberties**

No doubt, there will always be special interest groups in America proclaiming the Constitution is in mortal danger, but the question of whether public opinion will coalesce around the protection of civil liberties is a critical uncertainty. Without question, the amount of personal data that is accessible by the Government and third parties alike is at an all-time high. Data aggregators are voraciously building and selling consumer dossiers, identity theft is on the rise, and the Government is racing to gain as much information about travelers and suspicious groups as possible in the interest of national security (Singel, 2004, 1). Nonetheless, even as Congress prepares to consider renewing the temporary provisions of the USA PATRIOT Act, there does not seem to be a national consensus forming to demand greater protection of civil liberties.

It is said that a frog dropped into a pot of boiling water will immediately jump out while a frog in cold water may be gradually heated to a fatal boil without protest. Either consciously or unconsciously, Americans are increasingly conducting transactions that trade individual privacy rights and perhaps

other civil liberties for some benefit. International travelers may soon avoid lines and inconvenient delays if they are willing to relinquish biometric and personal data to the Government so that their identity and movements can be monitored electronically (Singel, 2004, 1). Shoppers receive discounts in exchange for allowing the grocer or bookstore to record and sell data about the food they eat, the medicines they take, and the books they read. Will the water in the pot ever get too hot for the public to bear?

National consensus in America is as rare as it is difficult to measure. Figure 2 below provides a conceptual basis for using public fora as a proxy to observe the progression of a single viewpoint as it moves toward becoming a national consensus. National consensus becomes more likely as the number of reasonable perspectives on an issue narrows while simultaneously increasing national attention moves the issue to fora that resonate with a larger share of the public.

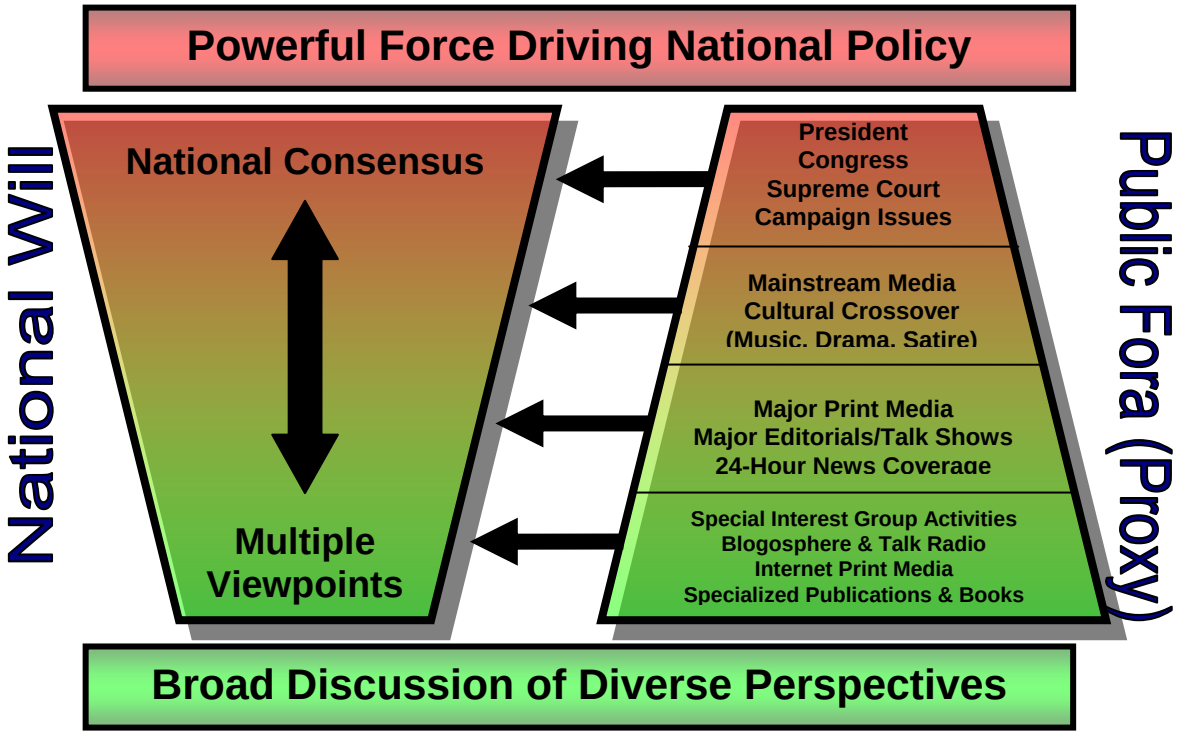


**Figure 2: Observing the Formation of National Consensus**

This phenomenon can occur virtually overnight, as in the cases of Pearl Harbor and 9/11. It could just as easily take months or years, as in the case of colonists' support for the American Revolutionary War or opposition to the Vietnam War. Based upon these examples, if history is any judge, the incredible power of national consensus in America does not depend upon how fast or slow the proverbial frog jumps.

**Degree of Commercial Technology Integration for National Security Purposes**

As a general rule, the engines powering technological innovation in the commercial and defense sectors are as different as chocolate and peanut butter. Despite the apparent altruism of some corporate mission statements, technology development in a free market economy must be guided by actual or predicted return on investment. Where the money leads, technology will follow. Defense technology development, however, is driven by actual or perceived capability gaps that must be closed to overcome current and future threats to national security. The nexus between the two, the "Reese's™ peanut butter cup" of capital investment, is where the chocolate time- and results-driven thoroughbreds of American industry meet the peanut butter "failure-is-not-an-option" cost and schedule tolerance of national security imperatives. The raw technological outcomes of that union can be staggering. The internet, for example, was arguably one such pre-9/11 outcome.

Public-private cooperation in the days immediately following 9/11 provides some insight into the longer term possibilities for ubiquitous private sector technologies, developed for purely commercial purposes, to quickly morph into homeland defense applications.

> Swept away by a patriotic fervor, information technology specialists flung open giant computer systems across the country to help law enforcement and intelligence agencies search for clues about the nineteen hijackers and their accomplices. Financial institutions gave access to credit card activity. Banks pored through customer accounts. Internet service providers helped trace email and account details. Data giants like Acxiom Corp., ChoicePoint, and Seisint searched through billions of demographic and marketing records on behalf of investigators…to pull together hefty dossiers about [suspects'] time in the United States. Northwest, JetBlue, American,

> and other airlines handed over manifests about passengers from across the country. Never mind the carefully crafted privacy promises, issued over the years to soothe customers. (O'Harrow, 2005, 6)

To what extent the chocolate and peanut butter will come together for the long-term future remains to be seen. Will it one day be deemed necessary to have full information on all citizens in order to track down a few hostile actors and thereby avoid unpleasant physical barriers at the border and layered perimeter defenses around population centers? Could the military be asked to take on a major security role within the US? It is at least conceivable that future events could precipitate an inward defense focus driving full integration of the commercial applications of RFID, database linking and mining, biometrics, and nanotechnology with transformational defense technologies enabling persistent ISR and NCW. If that is the future of national security, failure will indeed not be an option, and the outcomes could unwittingly reach Orwellian proportions. The Technology Integration Example at Appendix B provides a notional illustration of this kind of capability applied to one possible future scenario.

### Mapping the Range of Possible Futures

In scenario building, the most important and most uncertain driving forces affecting the focal issue form the axis of a graph upon which the future world scenarios take shape. The focal issue can be summarized in one key question: *as America's military transforms to defeat current and future threats, could the pursuit of national security unwittingly endanger the very Constitution we are sworn to defend?* The two most important and most uncertain driving forces behind that question are the public's demand for protection of civil liberties and the nature of future threats to US national security.

## SYNTHESIS: FUTURE SCENARIOS OF THE YEAR 2020

### Overview of Scenarios

The next step in the future scenarios-based planning process is to synthesize the driving forces into fictional accounts of the future. Figure 3 below illustrates the possible future scenarios balancing US national security against Constitutional protections between now and 2020. These future worlds are not intended to be predictive, but they do mark the outer boundaries of possibility using the most important and most uncertain driving forces as a common context. Each future world scenario contains a "history" of events from 2005 to 2020 and, through some creative license with current factual trends, provides a brief sense of what that world might be like to live in. The Future World Characteristics Matrix at Appendix A provides a detailed basis for contrasting and comparing the alternative futures.

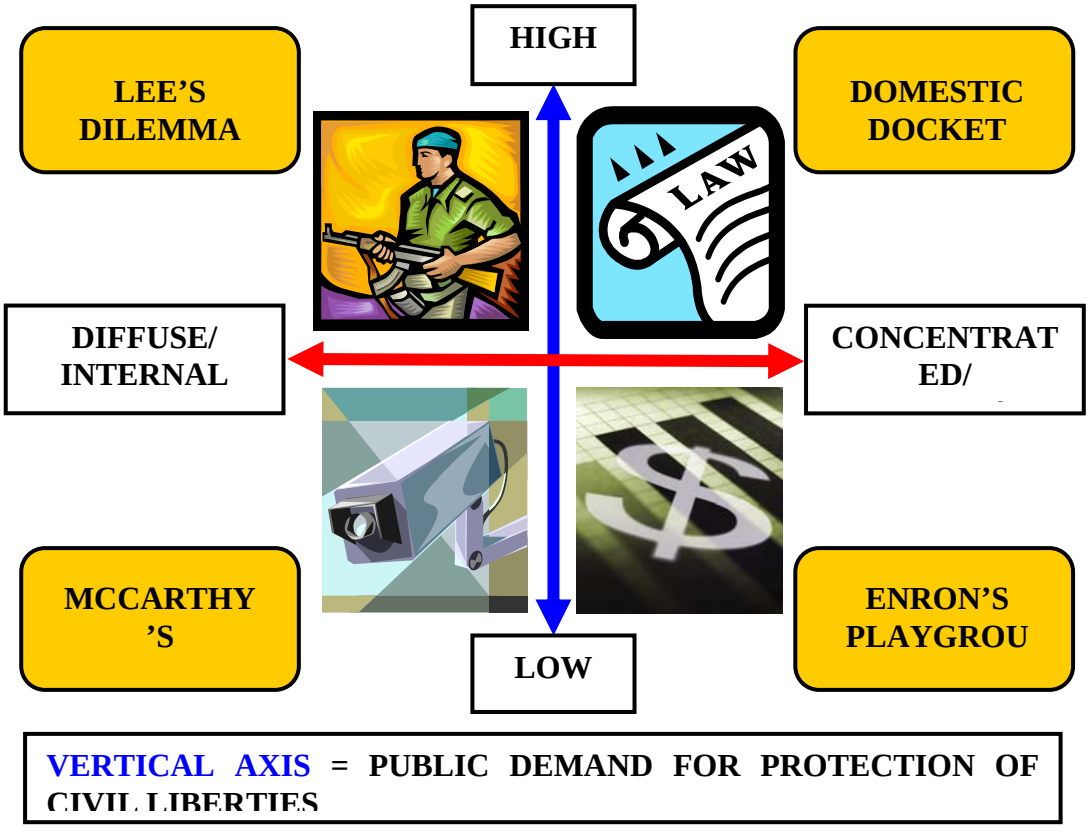

**Figure 3: Scenarios of National Security and the Constitution by 2020**

If the current trend towards "transactional forfeiture" of civil liberties continues unabated by an opposing national consensus, Americans may look forward to the technologies that will cause anonymity to die the slow death of the boiling frog. From a certain perspective, this future may not be all bad. As long as America's national security focus remains outward, Adam Smith's "invisible hand" will undoubtedly guide innovations to provide low-cost, individualized conveniences to consumers on a scale heretofore unimaginable. That is the world of *Enron's Playground*. If, however, future threats drive an *inward* national security focus, the Government and the private sector may jointly apply technologies that leave would-be terrorists and their sympathizers with no tree to hide behind. In this future, evocatively named *McCarthy's Witchhunt*, the country is swept by outward demonstrations of fervent patriotism, and those fortunate enough to be cleared of all suspicion view the Government as a benevolent protector. Vigilante groups are plentiful and are tacitly encouraged by law enforcement and military officials.

If a future national consensus does demand that the protection of civil liberties keeps pace with invasive new technologies, the future could be as tame as a spate of legal reforms or as turbulent as divisive incidents of domestic resistance. If national security threats continue to be external, the aftershocks from 9/11 will fade, and the high demand for civil liberty protections will generate new laws and regulations to curb private industry's insatiable appetite for consumer data exploitation. These legal protections could be as sweeping as a landmark Supreme Court ruling or perhaps even a Constitutional Amendment that gives individuals some degree of ownership or control over their own data that cannot be severed easily through commercial transactions. They could also take the shape of evolutionary adjustments to law and industry oversight regulations as each new technology application

offends the public's privacy sensibilities. Simson Garfinkel, the author of *Database Nation: The Death of Privacy in the 21st Century*, proposed several adjustments that might typify the future called *Domestic Docket.* These adjustments include a new non-partisan privacy oversight agency, expansion of the US Fair Credit Reporting Act of 1970 into a new "Data Protection Act," and a new law prohibiting the blanket personal data consent agreements required from consumers for even basic access to goods and services (Garfinkel, 2001, 260). In this future, investigative news segments about the latest infringements of privacy by the government and corporations alike always seem to fetch the highest ratings, and the front-runners for President never miss an opportunity to make public calls for legal reform while they express righteous indignation at the emerging surveillance society.

On the other hand, the future may not be so docile. In April of 1861, US Army General Robert E. Lee faced a gut-wrenching dilemma as the US Civil War seemed inevitable and President Lincoln offered him command over Union forces. If diffuse and internal national security threats abound in combination with a high demand for the protection of civil liberties, some may wish to organize local militias to protect their communities and cease to rely on, or cooperate with, federal authorities. Such a scenario is conceivable if future events cause the public to lose confidence in the Government's ability to protect them. To regain public trust, the Government might take extraordinary steps to include the repeal of *posse comitatus* and the temporary suspension of various civil liberties to ensure national security through a nationwide dragnet. Such a reaction could cause many to further mistrust the Government and invoke their constitutional right to simply be left alone, or worse, to replace their government. This is the world of *Lee's Dilemma*, and it promises to be the worst of all worlds for the military professional--trained to provide national security but sworn to support and defend the Constitution.

**Future Scenario 1: Enron's Playground**

*All that is necessary for the triumph of evil is that good men do nothing.*

—Edmund Burke

***Setting**:* Strategy Conference, Acxiom-Markle International (AMI), welcome letter from John Gallagher, Chief Executive Officer, to attending conferees, 13 April 2020.

Welcome to the 2020 AMI Strategy Conference! We have come a long way in the last twenty years, and your presence here will help determine where we go from here. As you have heard me say before, AMI brings the world to the doorstep of every consumer. Together with our sister data management firms and credit agencies, we have also collectively increased the efficiency of every market we serve. The comprehensive consumer information we provide to our customers allows unprecedented efficiency of capital investment, and highly predictable supply, demand, and return on investment.

Before we involve ourselves in the business of mapping out the road ahead, allow me to briefly recap some of the successes and challenges over the last two decades that have made us who we are today. In the days after the 9/11 attacks on New York and Washington D.C., we were first in line to assist government investigators seeking information about the highjackers and their accomplices. In retrospect, our partnering efforts with DoD and DHS during that period opened new commercial opportunities even as the threat of terrorism faded with the capture and conviction of Osama Bin Laden in 2008.

We've all discovered since then that peace is good for business! We have built our business through a partnership with the American consumer. Consumers across the country have benefited from conveniences and discounted prices for cutting-edge products and services specifically tailored to their preferences in return for nothing more than allowing AMI to gather, analyze and distribute useful marketing data on them. To facilitate this mutually beneficial relationship, we have built a complex network of web monitoring, automated passive and active RFID, biometric identification nano-cameras, on-board automobile location and telemetry data, travel and entertainment spending patterns, data-linked smart appliances and many others.

Our vast database interconnectivity within the "Information Sharing Environment" funded by the Government in 2004, combined with the remarkable "Novel Intelligence from Massive Data" mining capabilities, provides our customers with instant access to almost any information about the needs, desires and behavior of every individual consumer. This has in turn allowed them to manufacture complex products specifically to suit each customer's preferences and actual usage habits.

The future holds an even greater promise for consumers and clients alike if Congress passes the current legislation to complete the transition to a cashless society. This development would revolutionize the quality of our products and most likely reduce crime to even lower levels. Thanks to several visionary members of Congress who are not deterred by wild doomsday theories promoted by special interest groups, we expect the bill to pass. Thank you for your dedicated service. I look forward to seeing what new directions will result from your participation in this Strategy Conference.

**Future Scenario 2: McCarthy's Witchhunt**

*All erroneous ideas, all poisonous weeds, all ghosts and monsters, must be subjected to criticism; in no circumstances should they be allowed to spread unchecked.*

—Chairman Mao-Tse Tung
*Chinese Communist Party's National Conference on Propaganda, 12 March 1957*

***Setting**:* Suicide note found near the body of TSgt Jack Jones, USAF, suspected enemy agent, apprehended 23 July 2020 in Phoenix, AZ Defense Zone via DHS unmanned intercept.

Dear Kelly, we both knew this moment might come ever since my brother John was found to have transported a weapon shipment used in the third attack of this year—the one in Atlanta. Apparently, I was already on the watch list and then one of the web vigilante groups found that paper I wrote for my college course that was critical of the surveillance methods we are using against US citizens these days. They must

have turned me in and tipped my threat index score over into the red. I sure hope they are happy with their reward money! People are getting turned in everywhere you look.

It seems like killing Bin Laden in 2012 has only made things worse. Now he is seen as some sort of martyred hero. It is hard to believe that so many sleeper cells were right under our noses in the US and Canada. At first, I thought it was great how everyone in the US rallied around our Government—the gadgets we got as Security Forces to help the DHS were mind boggling. The unmanned combat air vehicle that got me was one of those that the Air Force transferred over to DHS with all the commercial data upgrades—some sort of legal reason for giving all those weapon systems to the DHS. What a joke, it sure didn't protect mine or John's rights.

I can't tell you how angry I am that it has to be this way. I really wanted to see the boys grow up, but you know as well as I do that I'm damaged goods and will only cause problems for you and the boys even if I do ever get out of the offshore interrogation facility they set up. I hope the insurance money is enough for you to find a new life…just follow the plan we talked about. Tell Mitchell and Luke I love them. Love, Jack.

**Future Scenario 3: Domestic Docket**

*The public good is in nothing more essentially interested, than in the protection of every individual's rights.*

—Sir William Blackstone, English Jurist, 1723 – 1780

***Setting**:* Prepared testimony of F. Leon Davis, Chairman of the Electronic Frontier Foundation (EFF), before the Senate Committee on the Judiciary, 17 April 2020.

Chairman Brownback, Senator Davies, men and women of the Judiciary Committee, thank you for allowing me to testify today on the need for a Constitutional Amendment to protect the civil liberties of all Americans in this modern age. Mr. Chairman, I applaud your outstanding record of service on the Subcommittee on Civil Rights and Property

Rights, which is so central to the question now facing the Congress, President Hernandez, and every state in our union. Allow me to begin by reading a brief prepared statement recounting some of the developments over the last fifteen years that I believe have brought us to this point, and then I will be happy to respond to any questions the Committee may have.

In 2005 the future of Iraq and Afghanistan was still very much in doubt, and the country was understandably concerned Al Qaeda and like-minded insurgents faced overseas would regain a foothold within our borders. That fear fueled an almost Machiavellian disregard for the long-term consequences of personal information dossiers, biometric travel surveillance, and temporary suspension of civil liberties in the name of national security. Clearly the 109th Congress showed some wisdom in rolling back some of the scarier provisions of the USA PATRIOT Act, but the more disturbing developments in private sector data aggregation, biometrics, and RFID proceeded virtually unopposed. The warning signs of widespread data theft from data aggregators and banks in 2005, and the associated financial attack of 2007 that used the stolen data to flood our financial networks with millions of simultaneous fraudulent transactions and automated credit requests, went largely unheeded. The data aggregators went back to business as usual after a few cosmetic security patches while correctly citing their legal right to any consumer's information "voluntarily" provided to a third party.

While many expected the DNA mapping and preventative medicine breakthroughs of 2010 to be cost prohibitive for most Americans, the insurance industry saw a long-term benefit to subsidizing the elective procedure, as long as individuals were willing to sign releases misleadingly described as "privacy policies." Millions of Americans

understandably took advantage of this low cost miracle of science and thereby added their DNA profiles to their already considerable dossiers sold on the open market—all perfectly legal. Due to loopholes in the genetic discrimination prohibitions passed in 2004, hundreds of thousands were dropped by their health insurance companies without explanation.

Although the passage of the long overdue Data Protection Act of 2011 and the creation of the Privacy Protection Agency (PPA) finally allowed Americans to at least see their dossiers along with a list of who purchased them and why. The subsequent public outrage at the unequivocal confirmation of what EFF has been saying for years was too little and too late. It did not change the legal determination that their Constitutional rights had not been infringed upon. The genie was out of the bottle, and they had no legal recourse. Though legally speaking, they were not forced to participate or provide any of the information found in the dossiers; the reality was that they had been offered unacceptable alternatives. For example, if you don't want a biometric picture of yourself on file, don't use an automatic teller machine, don't get a driver's license, don't get a passport…and so on.

Since that time we have seen one horror story after the next. In 2012, the RFID-tagged currency started being associated electronically with the consumer who uses it through surveillance-linking despite the initial controls put in the currency chips. Now every kind of monetary purchase can be tracked and thieves can case victims by passive detection of how much money they have. In 2014, the Social Security Administration had to reissue new encrypted numbers—that caused more pain than it was worth and was quickly rendered irrelevant by massive data interlinking. In 2016, Federal Transportation Safety Standard 301.62 required every new vehicle to have a GPS-enabled "black box" that

automatically enforces traffic laws, pays tolls, tracks individual movements, thwarts thieves, notifies authorities of accidents, and transmits maintenance and wear data to the manufacturer. Another win for the lawyers and insurance companies, who now have all kinds of data to incriminate drivers filing what used to be legitimate insurance claims or tort suits. Today, marketing subsidies and necessity have made the "voluntary" nature of the many releases we authorize daily nothing more than a cruel joke that renders privacy extinct. Will a struggling family of four really buy a $10,000 stand alone refrigerator or sign the release and buy a $2,500 data-linked model that, among other functions, transmits product usage and re-supply orders to grocers and nutrition information to health insurance companies?

Ladies and gentlemen, this Constitutional Amendment is essential in order to clearly define what data is so inherent to the pursuit of life and liberty as to be protected as the non-severable property of every citizen—subject to the full protections of the Fourth, Fifth and Fourteenth Amendments. Thank you, I will now respond to whatever questions you may have.

**Future Scenario 4: Lee's Dilemma**

> *With all my devotion to the Union and the feeling of loyalty and duty of an American citizen, I have not been able to make up my mind to raise my hand against my relatives, my children, my home. I have therefore resigned my commission in the Army, and save in defense of my native State, with the sincere hope that my poor services may never be needed, I hope I may never be called on to draw my sword...*
>
> —General Robert E. Lee
> *Letter to his Sister, April 20, 1861*

***Setting:*** Letter of resignation from Charles P. Graves, General, USA, Chairman of the Joint Chiefs of Staff, to President David Hernandez, 17 April 2020.

Mr. President, with a heavy heart I must inform you that I can no longer serve at your pleasure and must therefore resign my commission in the United States Army. I have sent a similar notification to the Secretary of Defense and will assist in any manner to nominate a suitable replacement. I consider myself blessed to have served this country over the last thirty-five years, and I am deeply grateful to you for the opportunity to have served as the Chairman of the Joint Chiefs. Since I hold you and my own good office in the highest regard, I will not presume to take this action without a suitable explanation. You have my personal assurance that I will not share this information with the public so long as I may live.

I, like all Americans, was devastated upon hearing the news in 2015 that Los Angeles was destroyed by a nuclear device, and horrified to learn that the "LA Day" attack was carried out by groups inside the US and Canada that had gone undetected for years in their accumulation of materials from Los Alamos NM. As you know, I initially supported your declaration of a state of emergency along with the repeal of *posse comitatus* and the temporary suspension of *habeas corpus* while we restore security within the US and root out enemy combatants wherever they may be. I took a solemn oath to support and defend the Constitution against all enemies foreign and domestic, and I did not hesitate to lead our forces to live up to the full weight of that duty—even within our own borders.

As Operation VIGILANT EAGLE began, the US Northern Command (USNORTHCOM) led an outstanding effort, with the assistance of DHS, US Strategic Command, and the Joint Warfare Analysis Center, to integrate the full range of commercial and military capabilities to immediately gain situational awareness over the entire battlespace in the US and Canada. The massive targeting database that was created with

extensive information on every man, woman, and child known to be residing in the US and Canada allowed us to prioritize surveillance, seizure, and strike missions by assigning individual threat index scores based upon the best enemy profiling and social network intelligence available. This was a truly remarkable effort that resulted in many early successes and allowed for revolutionary control over the top priority I gave to USNORTHCOM—minimal collateral damage.

What I failed to anticipate was the public's widespread loss of confidence in our Government's ability to protect them and the resultant armed "Constitutional Militias" that began to actively oppose our efforts across the country. As our tactics became more aggressive and our reliance on the continued suspension of *habeas corpus* became more pronounced, I began to have serious doubts about the constitutionality of this fight. I am now convinced that the kind of collateral damage I should have been concerned about avoiding in modern domestic military operations is that which impacts the Constitution itself. I have failed to live up to my oath and can no longer serve as Chairman of the Joint Chiefs of Staff.

## CONCLUSION

*They who would give up an essential liberty for temporary security, deserve neither liberty or security.*

—Benjamin Franklin, 1787

The final phases of scenarios-based future planning describe conclusions derived from the synthesis process that produced the future worlds. These conclusions include leading indicators to watch for as the future unfolds, and implications and actions for consideration. The intent of

this process is to prepare now for an uncertain future and to initiate an ongoing "strategic conversation" (Schwartz, 1991, 227).

**Leading Indicators**

Although leading indicators could be identified and tracked for all driving forces, gauging the nature of threats to US national security and the public demand for civil liberties provides the best method to monitor which future scenarios are becoming more or less likely over time. It is also beneficial to provide context by prioritizing the future scenarios from the most desirable to the least desirable with respect to the focal issue. A central assumption in this analysis is that the *predetermined element* of expanding key technologies will tend to erode civil liberties.

| Rank | Future Scenario | Threats to US Security | Demand for Civil Liberties | Reaction to Eroding Civil Liberties |
|---|---|---|---|---|
| **1** | *Domestic Docket* | External | High | Significant legal reforms |
| **2** | *Enron's Playground* | External | Low | None—traded for benefits |
| **3** | *McCarthy's Witchhunt* | Internal | Low | None—traded for security |
| **4** | *Lee's Dilemma* | Internal | High | Conflict—some violent |

**Table 1: Future Scenarios Ranked by Desirability to the Focal Issue (Most to Least)**

As illustrated by Table 1 above, leading indicators of future threats becoming internal are the most critical to the focal issue of whether national security and defense of the Constitution could ever become divergent goals. Obviously, the first such indicator to watch for is actual events that could lead to an inward defense focus. However, one critical problem with this indicator is that a single "LA Day" attack could shift the defense focus inward immediately. Therefore, leading indicators signaling the likely *invasiveness* of methods and *resistance* to operations if an inward defense focus emerges are also important to monitor. Table 2 below depicts how these indicators might be used.

| Indicator | Possible Measure(s) | Positive Indication | Negative Indication |
|---|---|---|---|
| **Events driving inward focus** | "Sleeper Cells" in US | No suspected cells | Cells suspected/found |
| | Attacks on US soil | None from within US | Executed from within |
| **Invasiveness of an inward focus** | Emerging approach to homeland security | Focused investigations of specific suspects | Broad data dragnets to isolate suspect patterns |
| **Resistance to an inward focus** | Govt. transparency | High accountability | Low accountability |
| | Public confidence | Perceived safety | Fear/vulnerability |

**Table 2: Leading Indicators Regarding an Inward Defense Focus**

Although less critical to the focal issue, leading indicators of the demand for protection of civil liberties could be used to measure the degree to which expanding technologies will likely erode Constitutional rights. Barring the formation of a national consensus, each new technology employed and each new bill considered with the potential to affect privacy rights will determine the net civil liberties outcomes resulting from the public's demand for protections. The critical limitation, however, is the difficulty of assigning a value judgment to those outcomes. Outcomes that consistently strengthen civil liberties could also result in dangerous security vulnerabilities. This delicate balance makes general leading indicators problematic. Therefore, developments in the protection of civil liberties must be evaluated on the merits, individually and collectively.

**Implications and Actions**

To be ready for the full range of future possibilities, the US military must be prepared to operate effectively within the two least desirable scenarios: *McCarthy's Witchhunt* and *Lee's Dilemma.* To do this, leaders should consider the need to revise or develop new concepts of operation to employ joint forces within the US with or without *posse comitatus* and with or without broad public support. This analysis should take place at the strategic, operational, and tactical levels of war to identify what adjustments might be necessary or advisable to joint

doctrine, command and control, weapon system characteristics and capabilities, and training at all levels. The results of this analysis should be reflected in deliberate and crisis action planning.

Strategic leaders should also consider adopting a broader definition for "collateral damage" in domestic operations to account for unintended Constitutional effects as well as unintended physical effects. Security and stability operations executed within the US, to the maximum extent possible, should not rely upon the curtailment or outright suspension of individual civil liberties guaranteed by the Constitution. In addition, since Constitutional collateral damage can result from a much broader range of kinetic and non-kinetic operations than traditional collateral damage, new methods of target analysis may be required.

Mission statements, military end-state descriptions, and commander's intent documents that do not consider the protection or restoration of Constitutional rights a top priority are insufficient and fail to recognize the sworn duty of every officer. In some cases, this requirement can and should even outweigh short-term military necessity. If strategic leaders fail to recognize the importance of this point, the enemies of freedom could achieve their desired end-state without "winning" a single operational engagement.

## Appendix A

# Future World Characteristics Matrix

| ***YEAR: 2020*** | **Enron's Playground** | **McCarthy's Witchhunt** | **Domestic Docket** | **Lee's Dilemma** |
|---|---|---|---|---|
| **World Motto** | We know what you want…with 98.3% confidence! | A terrorist behind every tree! | *Heinous Corpus!* | Freedom Fighters Unite! |
| **Biggest News Story in a Decade** | Bin Laden captured and convicted by US-led Int'l Criminal Court proceeding; Dow hits 15,000! | Bin Laden killed, millions hail him as martyred hero—sleeper cells emerge throughout western world--vow revenge | Mega-thrust quake strikes Japan | Los Angeles nuked—culprits operated in US and Canada for years undetected--materials origin: Los Alamos NM |
| **Military/ Commercial Technology Integration for Homeland Defense** | Military far outpaced by private sector tech—most high tech companies have no interest in defense market | Dossiers to be developed on every person in US. Mandatory imbedded chips being implemented. | Military role in US strictly "consequence management" and support to civil authorities | Dossiers to be developed on every person in US. Mandatory imbedded chips debated. |
| **Public Trust in Government** | Public mostly clueless about who has what info on them | Most consider the invasive measures a security imperative | Strained. Privacy laws not keeping up with technology | Widespread mistrust. Some violently oppose. |
| **Technology** | Prolific growth– Commercial advances staggering | ID cameras linked to dossiers—unknowns considered subjects of interest | Biotech and data mining stunted by legal restrictions | Race to integrate military and commercial tech |
| **Law Enforcement** | Largely automated. Imbedded chips in all new autos, cash, and children—ubiquitous urban surveillance--organized crime & drugs rampant—all | Small-scale attacks becoming common. Overwhelmed law enforcement turns to military for ISR-many systems are | Modest advances in automated traffic law enforcement. Limited use RFID in cash thwarts | *Posse comitatus* repealed, *habeas corpus* suspended. Curfews in effect for most urban areas. Operation VIGILANT |

| | | | | |
|---|---|---|---|---|
| | others in significant decline. ID theft crashes social security system | transferred to DHS including armed unmanned vehicles and patrol robots. Vigilantism tolerated | counterfeiting. Private surveillance/data used in criminal cases causes public backlash | EAGLE in US and Canada—USNORTHCOM is supported Commander |
| **Energy** | Becoming selectable options when buying a car (biofuel or fuel cell) or home (gas, electric, solar, biofuel) | Ending reliance on foreign oil becomes a patriotic duty—local papers print names of energy abusers | Still largely petroleum-based, but biofuel popular in EU, Japan and some parts of US | Personal energy production popular in rural areas (biofuel, solar) |
| **Actors** | Int'l trade blocs replacing states as the primary int'l actors | Transnational culture groups, Int'l trade blocs | Power held by mix of states and int'l trade blocs | Transnational culture groups, states, trade blocs |

| ***YEAR: 2020*** | **Enron's Playground** | **McCarthy's Witchhunt** | **Domestic Docket** | **Lee's Dilemma** |
|---|---|---|---|---|
| **International Governance** | UN starting second reform since 2005—new security council to have trade bloc members vice states | UN proposes broad new charter to respond to mounting terrorism—asks for direct command over portion of all members' forces | NATO disbanded due to conflicting EU security protocols. UN restoring its lost credibility | UN dysfunctional and powerless to confront terrorists or suspected state sponsors |
| **2020 Presidential Campaign Issues** | ID theft insurance. UN internet control of IP addresses, tele-communications and commerce standards to facilitate trade and standardize data sharing. Tax reform | Support for strengthening UN, genetic profiling, monetary rewards for turning in "persons of interest" for questioning, national energy tax | Constitutional amendment to protect personal data. Funding for hydrogen energy infrastructure. Tighter genetic discrimination laws | Highly divisive as incumbent is blamed for "LA-Day." Massive reforms proposed to regain security but all candidates urge calm/peace |
| **Health Care** | Drugs fit specific | Socialized health | Partially | Black market for |

| | | | | |
|---|---|---|---|---|
| | DNA profiles. China clones human--raises biometrics concerns | care system. Useful to gain more info on people | socialized to include primary care and drugs | anonymous health care emerging |
| **Primary Threats/World Politics** | GWOT fades to be on par with the "War on Drugs"- Reformers in a nuclear Iran take a leadership role in Mid-East Trade Bloc. China and a nuclear armed Japan are worrisome, but war is unlikely due to strong economic links | Unity of EU starting to decline as the cultural identity of Europe becomes increasingly eastern. France and the Islamic Republic of Spain propose new EU constitution. Russia collapses creating great concern over nuclear proliferation | Bin Laden presumed to have died a natural death—Pakistan and India form alliance with Japan to balance perceived ambitions in China. N. Korea implodes peacefully with death of Kim Jong Il. Mid-East still unstable—dominated by nuclear armed Iran | The Government claimed victory in GWOT just a month before "LA Day." All nations put on notice that any links to "LA Day" or interference in US internal affairs to be immediately met with "the most extreme US response possible" |
| **US Economy** | Booming as new industries emerge and productivity soars. Final plans made to go to cashless society—imbedded chips w/ biometrics and acct data seen as only viable long term solution for ID and purchasing | Recession. Investors wary of more intense attacks in US. New data becoming available on consumer spending and travel from embedded chips may have positive effect in near-term future | Recession--GDP of China and India surpass US. Interest rates up again to control inflation. However, consumer confidence still relatively high—many expect an upturn soon. | Devastated by "LA-Day" attack. US Dollar replaced by Euro as world's reserve currency due to emerging US instability. Stock market crashes. Widespread unemployment |
| **Military Budget** | Lean. US going to give the "peace dividend" concept another try | Robust, but DHS budget growing exponentially | Lean by US standards, but oversees presence still essential | Historic highs imperative to conduct homeland ops and deter opportunists |

# Appendix B

# Technology Integration Example

## Find, Fix, Track, Target, Engage and Attack…in Arizona?

***Setting**:* Operational Effectiveness Evaluation Web Meeting Hosted by Boeing Corporation and attended by representatives of the US Air Force and the DHS,15 August 2020.

Thank you for attending today's web meeting to discuss the operational effectiveness of the modified unmanned combat air vehicles (UCAVs) transferred to the DHS a little over two years ago. We believe we have achieved a new milestone with recent success story involving UCAV 193F. As you know, UCAV 193F is part of the first fully operational DHS squadron to have the integrated surveillance, biometric identification, and commercial data package installed.

Less than a month ago while on a routine surveillance mission, UCAV 193F used its new functionality to identify, evaluate, and apprehend an enemy combatant. The enemy combatant had infiltrated the US Air Force Security Forces at Luke AFB AZ and was captured outside Phoenix behaving suspiciously near a desert highway. I'll now direct your attention to the UCAV video taken of the successful engagement (see below).

The target's biometric profile and RFID cross-reference delivered a positive match from the master database with a 97.3% probability factor. The UCAV operator then used the upgraded commercial data tools to evaluate the target's characteristics. The family analysis cause immediate concern since his brother was recently apprehended and relocated for interrogation in connection with one of this year's attacks in Atlanta. The social network map, recent movements, and recent purchases indicated a 75% probability of direct ties to the same known terrorists associated with his brother. The target's genetic profile revealed a fourth generation connection of Iranian origin. The political views evaluation uncovered interest in several publications classified by the system as unpatriotic, and it revealed a disturbing treatise he wrote criticizing the methods of friendly forces. Following the rules of

engagement under the current "SEVERE" DHS security advisory threat level, his threat index score required that the target be apprehended. A warrant was electronically requested and received, and the UCAV operator transmitted a detain order to ground-based patrol robots who apprehended the target.

I think we can all be very proud of this success story. It proves that we have the capability to take this fight to the enemy no matter where they might try to hide—within our borders—or even within our military ranks. Thank you for your attention, I will now be happy to entertain any technical questions.

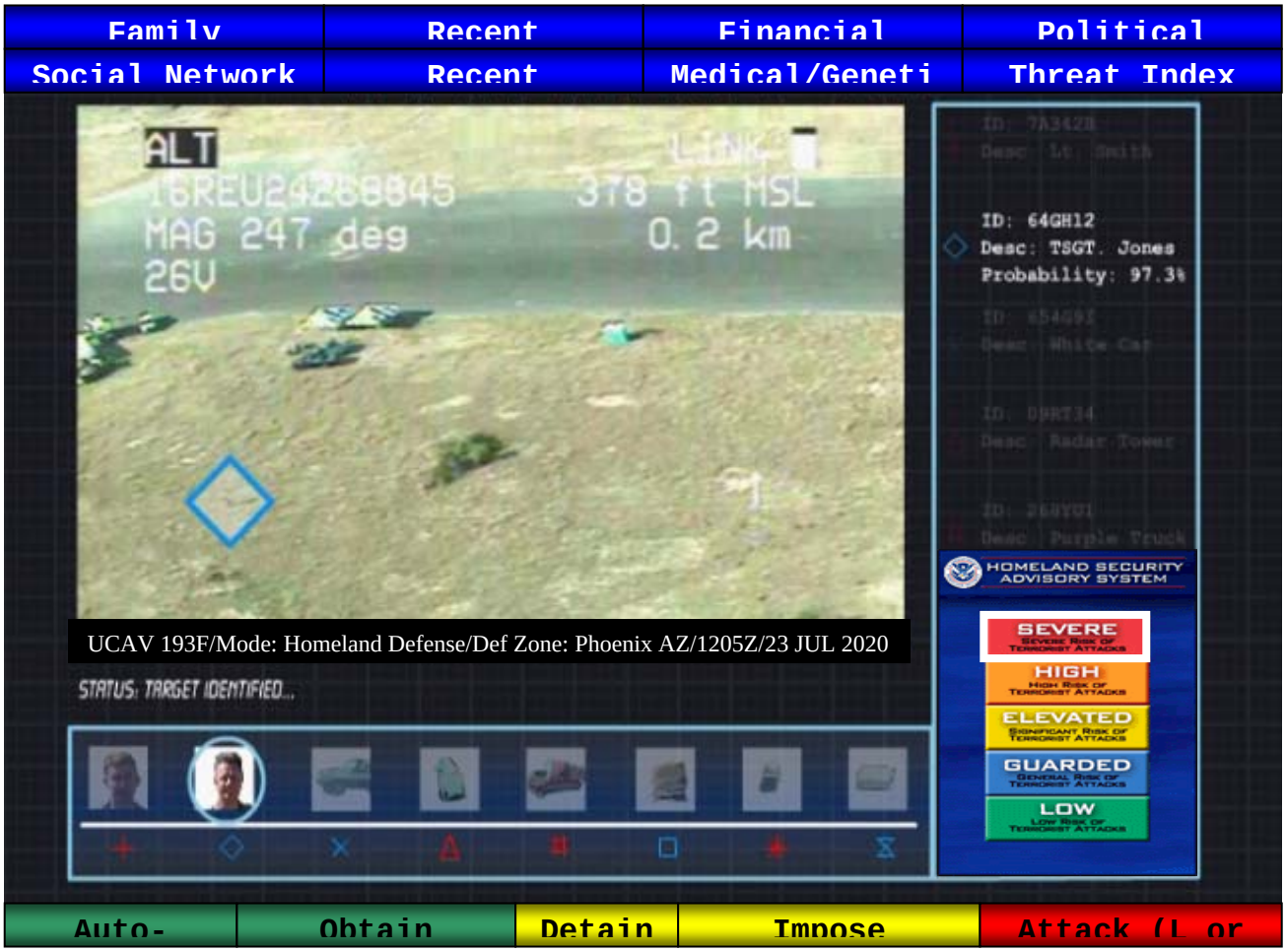


**Figure 4: Notional Future Homeland Security Technology Integration Example**

**Source:** Adapted from DIVOT Automated Target Identification System Status Briefing, Unmanned Aerial Vehicles, 2004 Air Combat Command Weapons and Tactics Conference, 16 January 2004.

**authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action.**

**All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.**

****WARNING**WARNING**WARNING****

## *BIBLIOGRAPHY*


"A Need for Flexibility." *The Economist*, 27 November 2004: 75-76.

Agnew, John. *Geopolitics: Re-Visioning World Politics, Second Edition.* New York: Routledge, 2003.

Annan, Kofi. "Courage to Fulfill Our Responsibilities." *The Economist*, 4 December 2004: 23-25.

Anton, Philip S., Richard Silberglitt and James Schneider. "The Global Technology Revolution: Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015." RAND National Defense Research Institute, 2001.

Associated Press. "FBI Tosses Carnivore to the Dogs." Available from World Wide Web: (http://www.wired/news/privacy), 18 January 2005.

Associated Press. "Hackers Nab U.S. Citizens' Data." Available from World Wide Web: (http://www.wired/news/privacy), 9 March 2005.

Associated Press. "Passport Privacy Protection? Nope." Available from World Wide Web: (http://www.wired/news/privacy), 27 November 2004.

Baard, Mark. "RFID Driver's Licenses Debated." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 6 October 2004.

Baard, Mark. "Watchdogs Push for RFID Laws." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 5 April 2004.

Barnett, Thomas P.M. *The Pentagon's New Map: War and Peace in the 21st Century*. New York: J.P. Putnam's Sons, 2004.

Barr, Bob. "Fighting Terrorism, Preserving Civil Liberties." Address. CATO Institute Policy Forum, CATO Institute, Washington, D.C., 2 October 2001.

Belsie, Laurant. "The Eyes Have It—For Now: As Surveillance Cameras Proliferate, a Band of Skeptics is Questioning the Social Impact of All This Watching." *Christian Science Monitor*, 7 November 2002: 15-16.

Bradbury, Michael. "Dumbing Down a Smart Watch." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/ privacy), 29 November 2004.

Booth, Ken, and Tim Dunne. *Worlds in Collision: Terror and the Future of Global Order*. New York: Palgrave Macmillan, 2002.

de Borchgrave, Arnaud. "Coming Geopolitical Quakes." *The Washington Times*, Available from World Wide Web: (http://www.washingtontimes.com/commentary/), 14 December 2004.

Bullinga, Marcel. "Intelligent Government: Invisible, Automatic, and Everywhere." *The Futurist*, July-August 2004: 32-36.

Bush, George W. *The National Security Strategy of the United States of America*. Washington, D.C.: The White House, 2002.

Cebrowski, A.K. *The Implementation of Network-Centric Warfare*. Washington D.C.: The Office of Force Transformation, Department of Defense, 2005.

"China's Growth Spreads Inland." *The Economist*, 20 November 2004: 13.

Clark, Tom C. *Berger v. New York, Certiorari to the Court of Appeals of New York.* Washington D.C.: United States Supreme Court, 1967.

Clinton, William J. *A National Security Strategy for a Global Age*. Washington D.C.: The White House, 2000.

EPIC. "United States Visitor and Immigrant Status Indicator Technology (US-VISIT)." Electronic Privacy Information Center, Available from World Wide Web: (http://www.epic.org/privacy/us-visit), 2005.

Engels, Daniel W. Ph.D. "RFID: The Technical Reality." Auto-ID Labs, Massachusetts Institute of Technology testimony submitted to the Federal Trade Commission RFID Workshop, Washington, D.C., 21 June 2004.

Etzioni, Amitai. "Forming a Global Authority: A World-Government Response to Terrorism." *The Futurist*, November-December 2004: 12-13.

Fallows, James. "Will Iran be Next?" *The Atlantic Monthly*, December 2004: 99-110.

Fulton, Katherine and Diana Scearce. "What If? The Art of Scenario Thinking for Non-Profits." Global Business Network, Available from World Wide Web: (http://www.gbn.com), July 2004.

Gallagher, Sean. "The New Face of Surveillance." Baseline Magazine, Available from World Wide Web: (http://www.baselinemag.com), 1 November 2004.

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA.: O'Reilly Media, 2001.

Gartner, John. "Automakers Give Biodeisel a Boost." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/autotech), 23 September 2004.

Gartner, John. "Fuel Cell Vehicles Close the Gap." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/autotech), 22 December 2004.

Givens, Beth. "Implementing RFID Responsibly: Calling for a Technology Assessment." Testimony submitted to the Federal Trade Commission RFID Workshop, Washington, D.C., 21 June 2004.

Glenn, Jerome C. and Theodore J. Gordon. *2004 State of the Future*. Washington, D.C.: American Council for The United Nations University, 2004.

Gossett, Sherrie. "Post-9/11 Security Fears Usher in Subdermal Chips: VeriChip Recipients Can Be ID'd, Monitored Anywhere in the World." *WorldNetDaily*, Available from World Wide Web: (http://www.wnd.com/news/), 4 February 2002.

Grossman, Wendy M. "British ID Cards Gain Ground." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/ privacy), 4 January 2005.

Hall, Mimi. "Homeland's Privacy Czar Balances Needs of Nation, Citizens." *USA Today*, 13 June 2004.

Harper, Jim. "Privacy Threats from a Banana Republic." *Tech Knowledge*, no. 93, (11 November 2004)

Hastert, Dennis J. "Delayed Notice Search Warrants: A Vital and Time-Honored Tool for Fighting Crime." U.S. House of Representatives, Washington D.C., September 2004.

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. New York, NY: Simon and Schuster, 1996.

Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 458. 108th Cong., 2d sess., 2004: Available online (http://frwebgate. access.gpo.gov), Government Printing Office, Washington D.C., 2004.

Justice for All Act of 2004. Public Law 405. 108th Cong., 2d sess., 2004: Available online: (http://frwebgate.access.gpo.gov), Government Printing Office, Washington D.C., 2004.

Lewis, Bernard. *The Crisis of Islam: Holy War and Unholy Terror*. New York, NY: The Random House Publishing Group, 2003.

McCullagh, Declan. "House Backs Major Shift to Electronic IDs." *CNet News*, Available from World Wide Web: (http://www.news.com.com), 10 February 2005

Millett, Stephen M. "Personalized Energy: The Next Paradigm." *The Futurist*, July-August 2004: 44-48.

National Intelligence Council. "Mapping the Global Future: A Report of the National Intelligence Council's 2020 Project." Available from World Wide Web: (http://www.globalsecurity.org), 2005.

O'Harrow, Robert Jr. *No Place to Hide.* New York, NY: Free Press, 2005.

"ORBCOMM Announces Application Development Agreement with VeriChip Corporation: Companies Will Jointly Develop Military, Security and Healthcare Applications for VeriChip™, the World's First Implantable Microchip." *Yahoo Financial News.* Available from World Wide Web: (http://www.biz.yahoo.com), 15 December 2004.

Ratner, Daniel and Mark A. *Nanotechnology and Homeland Security: New Weapons for New Wars.* Upper Saddle River, NJ: Prentice Hall, 2004.

Reuters. "Scammers Snag Money on Net Phones." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 20 March 2005.

Sandhana, Lakshmi. "There's No Place to Hide." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 26 August 2002.

Schwartz, Peter. *The Art of the Long View: Planning for the Future in an Uncertain World.* New York, NY: Currency Doubleday, 1991.

Scheeres, Julia. "Kidnapped? GPS to the Rescue." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/), 25 January 2002.

Scheeres, Julia. "Tracking Junior With a Microchip." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/), 10 October 2003.

Simoncelli, Tania. "Retreating Justice: Proposed Expansion of Federal DNA Database Threatens Civil Liberties." *GeneWatch*, March-April 2004: 3-10.

Singel, Ryan. "Airlines Ordered to Expose Data." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 12 November 2004.

Singel, Ryan. "American Passports to Get Chipped." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/ privacy), 21 October 2004.

Singel, Ryan. "Bush Forms Civil Liberties Board." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 31 August 2004.

Singel, Ryan. "New Screening Technology is Nigh." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/ privacy, 19 October 2004.

Singel, Ryan. "Reform Bill Weak on Privacy." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 7 December 2004.

Singel, Ryan. "Senate Wants Database Dragnet." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 6 October 2004.

Singel, Ryan. "The Business of Fighting Terror." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 5 January 2005.

Singel, Ryan. "Web Won't Let Government Hide." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 29 November 2004.

Smith, Dan. *The Penguin Atlas of War and Peace.* New York, NY: Penguin Books, 2003.

Sniffen, Michael J. "Controversial Terror Research Lives On." *The Washington Times*, 23 February 2004.

Snyder, David Pearce. "Five Meta-Trends Changing the World." *The Futurist*, July-August 2004: 22-27.

"Southern Comfort, Eastern Promise: How Biotechnology from Poor Countries Can Tackle Local Problems." *The Economist*, 11 December 2004: 78-79.

Sterling, Bruce. "Science's Next Big Score." *Wired Magazine*, November 2004: 154.

"The Challenger: Vladimir Putin Takes On Democracy, the West and All-Comers." *The Economist*, 11 December 2004: 9-10.

"The Passing of the Buck?" *The Economist*, 4 December 2004: 71-73.

Tien, Lee. "RFID: Government Use + Privacy Issues," Electronic Frontier Foundation testimony submitted to the Federal Trade Commission RFID Workshop, Washington, D.C., 21 June 2004.

"Too Soft a Touch: Lifting its Arms Ban on China Will Do the EU No Credit." *The Economist*, 11 December 2004: 11-12.

United Nations. *A More Secure World: Our Shared Responsibility.* New York, NY: United Nations, 2004.

United Press International. "Ridge Backs National Driver's ID Standards." Available from World Wide Web: (http://www.knology.net/news), 30 January 2005.

United States Air Force. "United States Air Force Strategic Planning Directive for Fiscal Years 2006-2023." Deputy Chief of Staff for Plans and Programs, Headquarters United States Air Force, Washington D.C. 2004.

United States Department of Justice. "Report from the Field: The USA PATRIOT Act at Work." Department of Justice, Washington D.C., July 2005.

United States Department of Justice. "USA PATRIOT Act Overview." Department of Justice, Washington D.C., 2001.

United States Air Force. "United States Air Force Transformation Flight Plan." Headquarters United States Air Force, Washington D.C. 2004.

Urofsky, Melvin. *Rights of the People: Individual Freedom and the Bill of Rights*. Washington D.C.: United States Department of State, 2003.

US House. *A bill to require federal ID standards, the Real ID Act of 2005*. Available from World Wide Web: (http://www.thomas.loc.gov/).109th Cong., 1st sess., 2005. H. R. 418.

Van Der Heijden, Kees. *Scenarios: The Art of Strategic Conversation.* West Sussex, England: John Wiley & Sons, Ltd., 1996.

Warwick, David R. "Toward a Cashless Society." *The Futurist*, July-August 2004: 38-42.

Zakaria, Fareed. *The Future of Freedom: Illiberal Democracy at Home and Abroad.* New York, NY: W.W. Norton & Company, 2003.

Zetter, Kim. "Brave New Era for Privacy Fight." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 13 January 2005.

Zetter, Kim. "School RFID Plan Gets an F." *Wired News*, Available from World Wide Web: (http://www.wired.com/news/privacy), 10 February 2005.

Zoller, Martha. "Pro-Con—Is America's New Security Law Squeezing Out Privacy Rights?" *World & I*, United Press International, October 2004: n.p.

Zolli, Andrew *Tech TV's Catalog of Tomorrow: Trends Shaping Your Future.* Indianapolis, IN: Que Publishing, 2003.