Surprise, Deception, Denial and Warning: Strategic Imperatives

by Lani Kass and J. Phillip "Jack" London

Lani Kass, Ph.D., is a Corporate Strategic Advisor at CACI International. Kass previously served as a Senior Policy Advisor to the Chairman of the Joint Chiefs of Staff. She was the first woman to serve as Professor of Military Strategy at the National War College.
J. Phillip London, Ph.D., is Chairman of the Board of CACI International. A graduate of the U.S. Naval Academy, he spent 24 years on active and reserve duty. London is the recipient of numerous industry awards and serves on several boards, including the U.S. Naval Institute and CAUSE. The views presented here are the authors' alone. This article is a tribute to the National War College's distinguished graduates, among them Service Chiefs, Combatant Commanders, and literally hundreds of senior diplomats, warriors and statesmen.

Abstract: *This article frames the highly complex national security challenges of surprise, denial and deception. These ultimate asymmetric threats exploit vulnerabilities, capitalizing on hubris, complacency and self-delusion. Such actions prevent the full and accurate assessment of opponents' capabilities and intentions, and hinder appropriate actions. The long and frequent history of surprise, denial and deception suggest that these are essentially psychological phenomena. They are effective because they challenge and exploit perceptions that fill the gap between what is known and unknown. The authors present decision superiority as the fusion of information dominance and decisive action. Technology and intelligence can enhance decision superiority by ameliorating, but not eliminating, the limits of human perception. Translating knowledge into capabilities and actions requires agile, adaptive processes and open institutional collaboration within the interagency, with global allies and the private sector.*

In May 1863, on the eve of the battle of Chancellorsville, General Joseph Hooker, commander of the Union Army of the Potomac, said: "My plans are perfect… may God have mercy on General Lee, for I will have none." General Hooker's over-confidence had immediate, mid- and long-term consequences: First, he was crushed by General Lee. Second, he was fired by Abraham Lincoln. Last,

© 2012 Published for the Foreign Policy Research Institute by Elsevier Ltd.

doi: 10.1016/j.orbis.2012.10.005

his name became a synonym for certain ladies of the evening. The enduring lesson is that humility is a virtue in strategic planning. Hubris, in contrast, often spells disaster.

Strategy is hard to do, because it is both an art and a structured intellectual process. It is the constant adaptation of ends and means to shifting conditions, in an environment where chance, uncertainty, fog, friction, and ambiguity dominate. To make it even more complex, strategy is a multi-sided affair: the objectives, intentions, actions, and reactions of other participants—both allies and opponents—are often opaque and varied. National interests and policy goals play a critical role, as do diplomatic, financial, technological, and military resources. Other factors, such as history, culture, ethos, and personalities, all influence strategic behavior in subtle, but significant ways. In today's globalized world, driven by a 24/7/365 news cycle, these realities require a broader, more integrated, less linear approach.

The twenty-first century strategist's task demands that it be approached in the context of its environment, factoring in a vast array of dynamic and increasingly complex variables. Strategy is not developed in a vacuum. Any use of force is, ultimately, a political act. Military power must be considered and evaluated in tandem with other instruments of statecraft, as well as public-private interfaces. This task requires rigorous, precise thinking and the ability to reconcile or choose among a spectrum of competing options. There are no easy answers to guide the strategist along, except the knowledge that the only alternative to a holistic approach is inconsistency, wasted effort, delayed decisions, and increased risk.[1]

Strategic success is built on four mutually supporting pillars: grasp of strategic theory and historic practice; innovation; integration, and alignment.

The function of any theory is to describe, organize, and explain a body of knowledge. Strategic theory has an added function: it guides action. Thus, it is nothing but pragmatic. To quote one of America's foremost strategists, Bernard Brodie: "Strategy is a field where truth is sought in the pursuit of viable solutions."[2] Therefore, all strategies seek to optimize available means to achieve the desired ends with acceptable risk.

Innovation is the ability to think anew and capitalize on changed circumstances—the fusion of creativity and logic. Some innovations involve science and technology, while others are in the realm of concepts and organizational design. In all cases, the ability to innovate rests on foresight—the aptitude to read both current and emerging trends, as well as to anticipate their impact. Innovation also requires courage, perseverance, entrepreneurship, and readiness to "break glass," especially in large bureaucracies and across sector boundaries.

[1] For a most elegant analysis of the subject see Mackubin Thomas Owens, "Strategy and the Strategic Way of Thinking," *Naval War College Review*, Autumn 2007.
[2] Bernard Brodie, *War and Politics* (New York: Macmillan, 1974), pp. 452-3.

Throughout history, some leaders have chosen to stick with comfortable assumptions and time-tested constructs, failing to realize that the strategic environment within which they function has been fundamentally transformed. Other leaders have managed to exploit the potential for innovation, fusing new concepts, technologies, approaches, and organizational structures into overwhelming combinations of effects. Their gift was integration and holistic thinking.

Integration is the ability to "connect the dots" and relate seemingly disparate activities to one another. Absent integration, second and third order effects are difficult, if not impossible, to anticipate. Holistic thinking is an approach that captures both the whole and its parts, allowing one to grasp multi-dimensional, dynamic relationships as they are today and as they might evolve tomorrow. It prepares the practitioner to foresee a wide array of potential consequences, yet neither assumes nor expects perfect congruence or linearity. Without integration and holistic thinking, one would be a permanent victim of surprise, reacting haphazardly to unanticipated, seemingly random events.

All strategic designs must be integrated horizontally and vertically. The best plan, even if flawlessly executed, will fail if its implementation does not support the over-arching objectives. Likewise, a lofty strategy unsupported (or unsupportable) by operational or fiscal realities is, at best, an academic exercise or, more often, a prescription for disaster.[3]

Alignment and coordination within and among military Services and government agencies, and with the private sector, produce synergies, save lives, and enhance strategic effectiveness. They are predicated upon and reflect trust and confidence in each other's capabilities, as well as an in-depth understanding of and ability to compensate for their inherent limitations.

In sum, strategy is the product of imagination, creativity and sound logic. Effectiveness comes from an integrated, synchronized effort, sustained over the long-term, and guided by a clear vision of the desired end-state.

Against this backdrop, surprise is a strategic discontinuity; a startling seismic shock. It upends best laid plans, unbalances a comfortable posture, and gives a whole new meaning to the adage that "the opponent gets a vote." Surprise causes psychological dislocation and at least temporary paralysis: one is no longer driving events and is forced, instead, to respond in and to an environment shaped by another's actions.

[3] Mackubin Thomas Owens, "Strategy and the Strategic Way of Thinking," *Naval War College Review*, Autumn 2007. For a lengthier discourse see: Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999); Michael Howard, *The Causes of War* (Cambridge: Harvard University Press, 1983); Colin S. Gray, "How Has War Changed Since the End of the Cold War?," *Parameters,* Spring 2005, pp. 14-26; and Colin S. Gray, *Explorations in Strategy* (Westport: Praeger, 1998).

Learning the Lessons of History

Surprise, denial and deception are as old as war itself. Surprise attacks, ruses, and guiles were practiced by biblical warriors and kings. A millennium later and a continent apart, their virtues were recognized and extolled as "the strategist's key to victory" by the Chinese warrior-philosopher Sun Tzu in his seminal *Art of War*. From ancient empires, through two World Wars, to the twenty-first century, nations and non-state actors have practiced surprise and deception and fallen victim to them—often with devastating consequences.[4]

Surprise and deception are not only fundamental, enduring elements of diplomacy and warfare; they are a basic and recurring part of everyday life. We constantly fail to anticipate events. Frequently, we spring traps; more often, we fall into them. And always we promise to learn from experience and do better next time.

In his 1962 introduction to Roberta Wohlstetter's ground-breaking book *Pearl Harbor: Warning and Decision*, Thomas C. Schelling wrote words that are as true and resonant today as they were 50 years ago:

> Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility, but also responsibility so poorly defined or so ambiguously delegated that action gets lost. It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it. It includes the alarm that fails to work, but also the alarm that has gone off so often it has been disconnected. It includes the inattentive watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed. It includes the contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of. It includes straightforward procrastination, but also decisions protracted by internal disagreement. It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion—which is usually too late. (Unlike movies, real life provides no musical background to tip us off to the climax.) Finally, surprise may include some measure of genuine novelty introduced by the enemy, and possibly some sheer bad luck.[5]

The best intelligence services and most elaborate warning systems have failed to predict war. For example, the Soviet leadership was as surprised by the German

[4] The academic literature on surprise and deception is quite rich, albeit predominantly a product of the twentieth century. Among the best sources are: Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge: Harvard University Press, 1988), updated in 2004 with a chapter accounting for the September 11, 2001 attacks; Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, DC: The Brookings Institution, 1982) and, of course, the all-time classic, Roberta Wohlstetter, Pearl Harbor, Warning and Decision (Stanford: Stanford University Press, 1962).

[5] Wohlstetter, op.cit, p.viii.

invasion of June 1941 as was the United States six months later by Japan's attack on Pearl Harbor. Israeli intelligence failed to anticipate the coordinated Egyptian-Syrian attack of October 1973 and the ensuing oil embargo. In between these two events, U.S. intelligence failed on at least five occasions to foresee attacks on American forces and security interests. The record since 1973 is not much better, and includes the February 1979 Chinese invasion of Vietnam; the December 1979 Soviet invasion of Afghanistan; the September 1980 Iraqi attack on Iran; the April 1982 Argentine invasion of the Falklands, and the August 1990 Iraqi attack on Kuwait. Likewise, Operations Desert Storm, Allied Force, Enduring Freedom, Iraqi Freedom and Odessey Dawn (Libya) all involved successful surprise and deception by the belligerents.[6]

On the political front, the United States failed to anticipate and prepare for such inflection points as the fall of the Shah in Iran and the subsequent hostage crisis; the collapse of the Soviet Union and the Warsaw Pact; the genocides in Rwanda and Sudan; the rise of violent Islamist extremism as a global ideological movement; the collapse of the U.S. lending, banking and housing bubble; escalating deficits and foreign debt, leading to the downgrading of U.S. credit rating; the Euro-zone crisis; the Arab Awakening and its still evolving aftermath, to including the ongoing civil war in Syria and upheaval in Egypt.[7]

While unpredictable by its very nature, the international community has also been caught unprepared for such disasters as the meltdowns of two nuclear reactors (Chernobyl, 1986 and Fukushima, 2011); devastating tsunamis, earthquakes, floods, oil spills (Exxon and BP), and hurricanes—most notably Katrina, which forever changed America's view of domestic disaster preparedness, cross-sector coordination, and relief operations.

Cyber attacks straddle the categories noted above: some are clearly deliberate military attacks (e.g. Russia's on Georgia prior to their 2008 war); some accord plausible deniability and strike at the intersection of force and diplomacy (e.g., the Stuxnet attacks on Iran's nuclear production facilities, physically destroying infrastructure without using kinetic force); others remain unattributed and disclosed only through unauthorized leaks or written off to natural causes. Accumulating warnings notwithstanding, it is a safe bet that if and when a major cyber attack cripples the United States., paralyzing both our inter-netted way of life and EMS-

[6] Roy Godson and James J. Wirtz, *Strategic Denial and Deception: The Twenty First Century Challenge* (New Brunswick: Transaction Publishers, 2004). See also Michael I. Handel, *War, Strategy and Intelligence* (London: Frank Cass and Co, Ltd., 1989) and Ephraim Kam, *Surprise Attack: The Victim's Perspective,* op.cit.

[7] One of the few books dedicated exclusively to diplomatic surprise is Michael I. Handel, *The Diplomacy of Surprise* (Lanham: University Press of America**,** 1981).

reliant military—all hinging on unimpeded access to the electro-magnetic spectrum—it will be considered a surprise to rival Pearl Harbor.[8]

History, in the sense of humanity's collective experience, has also not been a good teacher. For example, each of the great powers involved in WWII was both a victim and a perpetrator.[9] Egypt, militarily surprised by Israel in October 1956, failed to learn the lesson and was surprised again in June 1967. Israel, having twice managed a devastating surprise attack on Egypt, was in turn surprised by it and Syria in October 1973. The ensuing reorganization of its intelligence services notwithstanding, Israel was surprised again by the Palestinian *Intifada* and, most recently, by the demise of the Mubarak regime, which sustained a vital Peace Treaty for 30-plus years.

Likewise, since the October 1983 homicide bombing of the Marine Barracks in Beirut, the United States has been the target of several high-impact terrorist acts, including: the 1993 attack on the World Trade Center; the 1998 bombing of Embassies in Kenya and Tanzania; and the 2000 attack on the USS *Cole* in Aden—all traceable to al Qaeda (AQ). Yet, until September 11, 2001 few Americans knew that AQ has declared war on the U.S. (first in 1996 and again in 1998). Consequently, the 9/11 attacks, the most devastating surprise perpetrated against this nation since Pearl Harbor, caught both the U.S. Government and the American people unaware of the danger and stunned by the consequences.[10]

Most recently, Washington was astounded by the scope, scale and velocity of the Arab Spring. It stood by as erstwhile allies were toppled in Egypt, Yemen, and Tunisia—and shaken at their moorings across the Arabian Peninsula. The ensuing ascent of the Muslim Brotherhood (a closely-monitored group founded in 1928 and rooted in both fascism and Islamic extremism) fundamentally transformed the strategic landscape in a region where vital U.S. interests are at stake. As the full implications of this inflection point unfold, uncertainty remains the only sure thing.[11]

[8] The term "Cyber Pearl Harbor" is widely attributed to Richard A. Clarke, the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism and author of *Cyber War* (New York: Harper Collins, 2010). Secretary of Defense Leon Panetta has also used the term in numerous media views, as well as Congressional hearings.

[9] The best volumes on World War II deception operations are: Thaddeus Halt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Simon and Schuster, 2010); Ben Macintyre, *Double Cross: The True Story of the D-Day Spies* (New York: Crown, 2012; and Anthony Cave Brown, *Bodyguard of Lies* (Guilford: Lyons Press, 2002). More general texts include: Larry Addington, "The Second World War, 1939-1945," *The Patterns of War Since the Eighteenth Century*, 2nd ed. (Bloomington: Indiana University Press, 1994); Victor Davis Hanson, *Carnage and Culture: Landmark Battles and the Rise of Western Power* (New York: Anchor Books, 2002) and John Lynn, *Battle: A History of Combat and Culture* (Boulder: Westview Press: 2003).

[10] Richard A. Shultz, Jr. and Ruth Margolies Beitter, "Tactical Deception and Strategic Surprise in Al Qai'da's Operations," *Middle East Review of International Affairs,* June 2004, pp. 56-79.

[11] The January/February 2012 issue of *World Affairs* Journal offers three distinct perspectives under the joint title "Arab Spring or Islamist Winter," by Michael J. Totten, Hussain Abdul-Hussain, and David Schenker.

These examples demonstrate that all surprises have at least three things in common. First, they are traumatic to the victim. Second, they accord a significant, albeit temporary, advantage to the initiator. Third, they generate a seemingly endless stream of assessments and analyses seeking to determine what happened and why, who was at fault, and how to reorganize the system in order to avoid a similar failure in the future. While the first two attributes apply primarily to military surprises, the third is universally applicable to military, diplomatic, and economic surprises—and even to natural disasters. This pattern will likely endure well into the twenty-first century, even as we continue the quest for technological and organizational solutions that would alert authorities to emerging threats, facilitate warning, improve decision-making, avert surprise, expose deception, and make the nation more resilient, more effectively organized and, thereby, better prepared to deal with their aftermath.

Propositions, Premises and Tenets

Strong, confident nations like the United States lack the natural incentive to employ surprise, denial and deception. Indeed, these are often dismissed as "weapons of the weak." Surprise, denial and deception are the ultimate asymmetric threats because they interfere with one's ability to assess adversary's capabilities and intentions, as well as account for one's own vulnerabilities. In a democracy, this reality further impedes the ability to make timely, effective decisions. Surprise and deception also influence policies and public opinion at home and abroad, thus potentially shifting the balance of power by shaping perceptions in the adversaries' favor.[12]

Surprise, denial and deception exploit natural proclivities and inherent, systemic vulnerabilities, capitalizing on complacency, misperceptions, and self-delusion. Unable to take their opponents head on, asymmetric actors rely on the force-multiplying effects the shock and psychological dislocation that surprise inevitably produces. Defeating these threats—denying them this asymmetric advantage—requires a thorough understanding of the nature of surprise, as well as the resolve to minimize its impact and consequences.

Surprise determines the time, place, and nature of the first engagement. It does not define the ultimate outcome. However, this principle is up for grabs and must be reaffirmed each time by both the target and the initiator. Pearl Harbor both symbolizes and validates this proposition.

[12] The best textbook on the role of perceptions in international affairs remains Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976). See also Yaacov Vertzberger, *The World in Their Minds: Information Processing, Cognition, and Perception* (Stanford: Stanford University Press, 1990).

The Japanese believed that the destruction of the Pacific Fleet would deny the United States the ability to interfere with Tokyo's designs in Asia. Not only were the Japanese wrong about America's capabilities and intentions, the "day that would live in infamy" brought the United States directly into World War II with the stated objective of "unconditional surrender" of not merely Imperial Japan, but the entire Nazi-led Axis. Japanese Admiral Hara Tadaichi, who commanded Carrier Division 5 in the attacks, quickly concluded that: "We won a great tactical victory at Pearl Harbor and thereby lost the war."[13] His prescience was quickly proven by Doolittle's Raid against the Home Islands on April 18, 1942; at the Battles of Coral Sea and Midway on May 4-8, 1942 and June 4-7, 1942, respectively; at Hiroshima and Nagasaki on August 6 and 9, 1945; and, finally, at the surrender ceremony aboard the USS *Missouri* on September 2, 1945—three months after Germany surrendered on May 7.[14]

This pivotal chain of events demonstrates that surprise and deception are means, not ends. To succeed, the initiator must be able to exploit the opportunity thus created. Otherwise, the initial shock might be short-lived and the advantage fleeting. The target is just as likely to recover and respond—often in an asymmetric, if not disproportionate, manner—imposing a price far exceeding the initiator's original cost-benefit calculus.

With this in mind, what follows are ten propositions intended to guide soldiers, diplomats, and decision-makers at all levels, as well as all those who support the endeavor to remain ever vigilant in providing for the common defense.

1. Always conduct a reality check from not only your own perspective but also that of the opponent. Reality always has rough edges, ambiguities, and shades of gray. If everything is crystal clear and consistent with your best-case scenario, and the adversary behaves just like you would in similar circumstances, you are probably being deceived.

2. State assumptions clearly and explicitly. Identify pivotal assumptions, those that if proven wrong would upend your entire approach. Develop a system to periodically revalidate these assumptions, making sure you don't confuse estimates with facts, or hopes with viable courses of action. Remember that any

[13] Herve Haufler, *Codebreaker's Victory: How the Allied Cryptographers Won World War II* (New York: NAL, 2003), p. 127. See also *The Pacific War On Line Encyclopedia,* http://pwencycl.kgbudge.com/H/a/Hara_Chuichi.htm.

[14] Of the many volumes covering the War in the Pacific, see, in particular, D. Clayton James, "American and Japanese Strategies in the Pacific War," in Peter Paret, Editor, *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press, 1986); Russell F. Weigley, "The Strategic Tradition of A.T. Mahan: The Strategists of the Pacific War," *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington: Indiana University Press, 1977); Allan R. Millett and Peter Maslowski, *For the Common Defense: A Military History of the United States of America* (New York: The Free Press, 1994). See also, Paul Fussell, "Thank God for the Bomb," *The Guardian*, July 21, 1989, pp.1-8 and Michael Waltzer and Paul Fussell, "An Exchange on Hiroshima," *New Republic*, Sept. 23, 1981, pp. 13-14.

plan that relies on more than two consecutive miracles and violates more than one law of physics is not suitable—even as a deception or feint.

3. Don't fall in love with any plan, policy, program, or assessment. Don't expect the opponent to cooperate. Have a branch and sequel to address the unexpected along the lines of "what if?" and "what next?" Pay attention to what both adversaries and allies are saying and doing—especially if there is a mismatch between words and deeds. Don't discount indicators just because they point to things *you* would never do. There are no universal standards of rationality or recklessness.

4. Collaborate with all who might provide fresh insights and different perspectives. Keep this circle as diverse and wide as practicable. Help your colleagues by asking the "right" questions. Tell them explicitly what you need to know and why. But be realistic: no existing technology is capable of assessing intentions. Question the *bona fides* of any information—no matter how comforting, convincing, or highly classified.

5. You don't know what you don't know, and what you don't know can spell disaster. Create an organizational climate that allows for alternative viewpoints to be given a fair hearing. Beware of group-think and remember that just because something never happened before does not preclude it from happening. Every precedent was created by someone's act of courage or folly.

6. Trust your instincts and be ready to pay the price that might go with that. Warning is about being safe, not about being right. Beware of the "cry wolf" syndrome, but don't dismiss the bearers of bad news. Sometimes the wolves are really at the gate and "inflammatory rhetoric" indicates a real and present danger.

7. Timely, unambiguous warning is nice to have, but don't count on it. Don't assume or expect that appropriate decisions, authorities and actions would automatically follow. You have plenty of latitude within your own organization. Do what's right, even if you have to stake your career on it.

8. Don't be a victim! It's painful, even if you ultimately win. Never allow the initiator to exploit his initial success. Surprise only determines where and how the first battles will be fought, but it's up to you to revalidate this principle every single time.

9. Don't get complacent. Hubris kills.

10. Guile is neither the opposite of valor nor an effective substitute for capability and capacity, but it saves lives and treasure. It is an asymmetric advantage we forfeit to others at our own peril.

Surprise, Warning and Decision

Asymmetric actors' use of surprise, denial and deception to level the playing field has far-reaching implications. To begin, it is useful to draw a clear distinction between two perspectives inherent in any unequal human interaction: the target's and the initiator's.

For the initiator, surprise is a process or, more precisely, the outcome of a deliberate, often painstaking effort. It is a plan coming together in a concentrated burst of activity, a plan in which everything worked just right to produce the expected result. Having pulled it off, the initiator's mission is to exploit the initial success in order to achieve the desired political, military, economic, or informational objectives.

For the target, surprise is an event: sudden, stunning, traumatic, and humiliating. Surprise catches the victim at his weakest, exposing and exploiting his failings. The after-shocks linger on in the victim's memory, shaping and impacting future behaviors. Assuming the target recovers—an assumption the initiator rarely makes—surprise precipitates a scramble to recover, allocate blame, and reorganize "the system" which failed to warn of the impending disaster. It is only after the fact that the victim becomes aware of what caused the event to happen. In other words, the target learns the makings of surprise only in its aftermath.[15]

Looking at any surprise in retrospect, one tends to be less impressed by the initiator's skill than by what appears as the victim's fatal self-delusion, if not abject blindness. The striking thing about surprises is that one can never quite understand how it could have happened. How could the victim be so oblivious? Indicators of a calamity in the offing are always starker *after* the "unthinkable" has occurred. With 20/20 hindsight, it is much easier to see how one could have anticipated, planned for, and perhaps even deterred or averted the surprise.

In a way, this is akin to putting together a jigsaw puzzle for the third time. Because the individual elements and the overall pattern are familiar, it is easy to pick out the appropriate pieces, in the correct sequence, and fit them into a coherent whole. The task of "connecting the dots," even recognizing the dots, signals and indicators out there, is quite simple once one knows what to look for. To appreciate and learn from the difficulties and uncertainties facing both the actor contemplating surprise and its intended target, one must place themselves in the participants' shoes and consider the situation from their perspective, as the actual events were unfolding.

[15] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Lanham: University Press of America, 2004). See also, John Gooch and Amos Perlmutter, *Military Deception and Strategic Surprise* (London: Cass Publishing, 1982).

In both politics and war, surprise is a difficult, but eminently worthwhile endeavor. Empirical analyses conducted by Sir Basil H. Liddell Hart in the 1930s and by American researcher Barton Whaley (whose masterpiece *Stratagem* was republished in 2008) compellingly demonstrate that surprise and deception reduce casualties and increase the likelihood of success. Deception is also amazingly cost effective. For example, Operation Fortitude, the massive diversion covering the planning and execution of the Normandy Landings, consumed less than one percent of the total expenditures; involved less than 0.2 percent of the dedicated personnel; and less than 0.5 percent of the allocated equipment. Its human toll was six—a miniscule number relative to the estimated 10,000 Allied D-Day casualties. The enduring lesson is that by hiding the real (denial) and showing the fake (deception) one can cause the adversary to misallocate resources, thus increasing the chances of victory at a remarkably low cost. [16]

Because it causes both a psychological and physical dislocation, surprise accords the initiator an obvious advantage. Until the victim recovers, the perpetrator has the initiative at the strategic, operational and tactical levels. In military terms, surprise is a force multiplier, allowing a numerically or technologically inferior force to gain the upper hand—the very definition of asymmetry.

It is important to emphasize that surprise is a matter of degree. Its spectrum ranges from the rare total surprise with the very occurrence of an event (9/11 being the most vivid example) to the more common surprise as to the timing, location, perpetrators' identity, or type of event that was at least considered to be a plausible eventuality. Likewise, the initial impact and lingering effects of surprise are directly correlated with the depth of beliefs that made up the target's original perception of reality. The more ingrained and widely held the assumptions as to whether an event could happen—and, if so, when, where, by whom, and how might it be carried out—the greater the cognitive dissonance when expectations are shattered by a suddenly altered reality. By the same token, the strength and elasticity of the planning assumptions determine both the degree of strategic dislocation caused by an unexpected adverse action, as well as the ability to adapt and recover in its aftermath.[17]

[16] Barton Whaley and Jeffrey Busby, "Detecting Deception: Practice, Practitioners, and Theory" in Roy Godson and James J. Wirtz, *Strategic Denial and Deception: The Twenty First Century Challenge* (New Brunswick: Transaction Publishers, 2004), pp.223-228. Michael I. Handel, *War, Strategy and Intelligence* (London: Frank Cass and Co, Ltd., 1989), p. 381. See also, Deception Research Program, Office of Research and Development, Central Intelligence Agency, *Deception Maxims: Fact and Folklore* (Washington, D.C.: U.S. Government, 1980); Basil Henry Liddell Hart, *Strategy* (New York: Signet Books, 1974); Michael Dewer, *The Art of Deception in Warfare* (New York: Sterling Publishing, 1989),Mark Lloyd, *The Art of Military Deception* (South Yorkshire: Pen and Sword Books, 1997).

[17] For an in-depth discussion see Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (New York: Pergamon Press Inc., 1982); Colonel John Hughes-Wilson, *Military Intelligence*

The issue of warning reflects the uneasy intersection of policy, intelligence, strategy, operations, and decision-making writ large. At its most basic, warning is information pointing to an emerging threat. That information is collected and processed by the intelligence agencies and transmitted to decision-makers for action. Warning, therefore, is the vital link connecting intelligence assessment with countermeasures designed to face the looming threat.[18]

Theoretically, then, warning is the antithesis of surprise—an effective antidote to it. If forewarned means forearmed, warning should avert surprise. By the same token, surprises result from failure to issue and react to advance warning. Yet, to paraphrase Karl von Clausewitz, everything in policy and war is simple, but the simplest things are difficult. And anticipating an impending disaster might be the most difficult task of all. Crises are generally preceded by a period of international friction, signaling mounting tensions. Often, there is an explicit declaration of hostile intent, as was the case with al Qaeda. Conventional military actions usually require extensive preparations, which are difficult to conceal. Nonetheless, the historic record of anticipating conflict is pretty dismal. Why is it so—even in this era of 24/7/365 electronic monitoring, high-speed computers, and sophisticated reconnaissance and surveillance technology—is worth exploring in greater depth.

The first and probably most important aspect to note is the manner in which humans, as well as machines built and used by humans, process data. Heuristics refers to experience-based approaches to problem solving. When time is of the essence—as it almost always is in national security decision-making—an exhaustive search for and thorough evaluation of information are often deemed impractical. Heuristic methods are used to speed up the analytical process through linear pattern formation, intuitive judgments, and "educated guesses."

More fundamentally, humans process all incoming information through a perceptual prism, comprised of their culture, assumptions, biases, and experiences with the most recent being the most vivid and, thus, most impactful. This prism determines which data would even be noticed and factored in and which inputs would be filtered out or ignored altogether; what weight and importance each piece of data would be accorded; which patterns would the information be arrayed into; and, ultimately, which judgments and conclusions will be derived.

Figure 1 is a model of how humans—as well as systems and processes designed and employed by humans—digest, sort, and order data. These multi-faceted, iterative and highly dynamic processes take place literally in a blink of an eye in the human brain and at the speed of light in modern computers.

Blunders and Cover-Ups (New York: Carrol & Graff, 2004); Jon Latimer, *Deception in War* (Woodstock: John Murray Publishers: 2003).

[18] John W. Bodnar, *Warning Analysis for the Information Age: Rethinking the Intelligence Process* (Washington, D.C.: Joint Military Intelligence College, 2003).

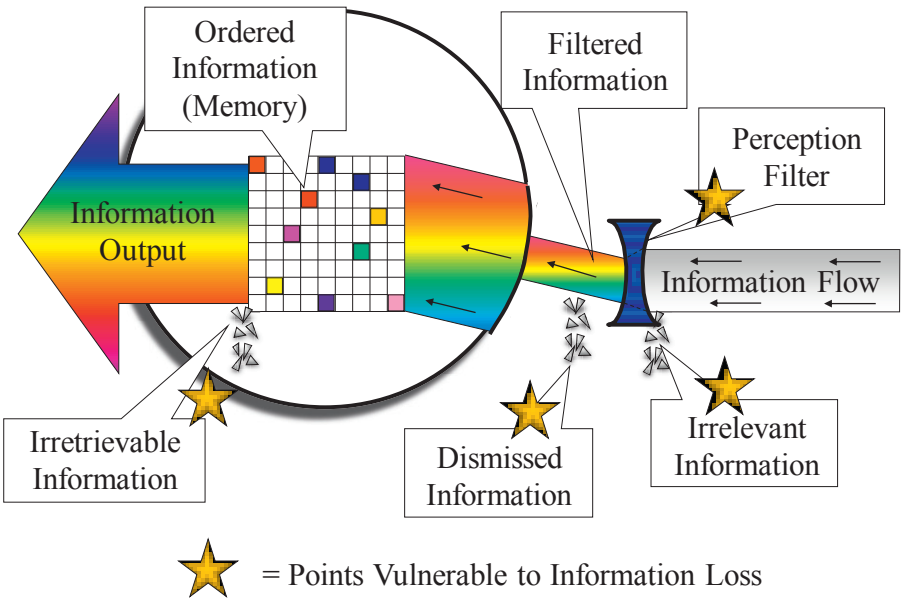

Figure 1: Model for Processing and Ordering Information

Within this natural, if rarely recognized, process are specific points of vulnerability where new information is filtered out, dismissed as irrelevant, ignored, or simply left fallow. Insofar as the perceptual prism is dynamic and new facets are formed as inputs are sorted into the patterns that constitute memory, such information becomes irretrievable. This goes a long way towards explaining why collecting vast amounts of data does not necessarily lead to better situational awareness and decision superiority; why we tend to repeat the past's errors, and why recording lessons is so fundamentally different from actually learning from experience.

Surprise "short-circuits" this process. It forces the target to quickly come to grips with biased perceptions, erroneous assumptions, and flawed pattern formation. This disruption generates two sets of possible outcomes, dependent on the degree of surprise and the time available to adapt: 1) change in perceptions and a new, flexible information flow, allowing appropriate decisions and actions, and 2) cognitive dislocation and persistent paralysis.

It is the latter case wherein the target becomes a victim. The deeper the surprise, the stronger the going-in assumptions, the more rigid the processes, and the more valuable the information that has been lost along the way, the higher the potential for cognitive dissonance and, consequently, the more persistent the

ensuing paralysis. By the same token, time is a critical factor in the target's ability to adjust to the new reality. This is why some nations manage to recover and prevail in the aftermath of a devastating surprise, while others are left with little choice but to accept defeat. The United States in the wake of Pearl Harbor; the Soviet Union after the June 1941 German invasion; Israel in the wake of the Egyptian and Syrian assault on Yom Kippur in October 1973, and the United States after 9/11 are prime examples of the agility and adaptability necessary to persevere and shape the war's final outcome—despite initial setbacks. Their opponents' fate demonstrates how dislocation, systemic dysfunctions, and persistent rigidity accounted for their ultimate defeat.

Figure 2 illustrates why the lessons of experience rarely last and surprise continues to occur. The readiness to open the mental, institutional and technological apertures and the ensuing ability to absorb and integrate new information in new ways are usually short-lived. Soon after the crisis that shocked the system and induced new behaviors passes, stability and "business as usual" become the natural default. The transformed behaviors become the new normal; newly created "memory boxes" become stale or irrelevant; complacency inevitably sets in. This allows determined adversaries to find new opportunities to exploit the target's comfort with and confidence in the "fixes" that have been introduced into the collection, analysis, and decision-making system. Absent constant vigilance and adaptation to ever-evolving threats, fixes become fixations, generating new vulnerabilities to be exploited both symmetrically and asymmetrically.[19]

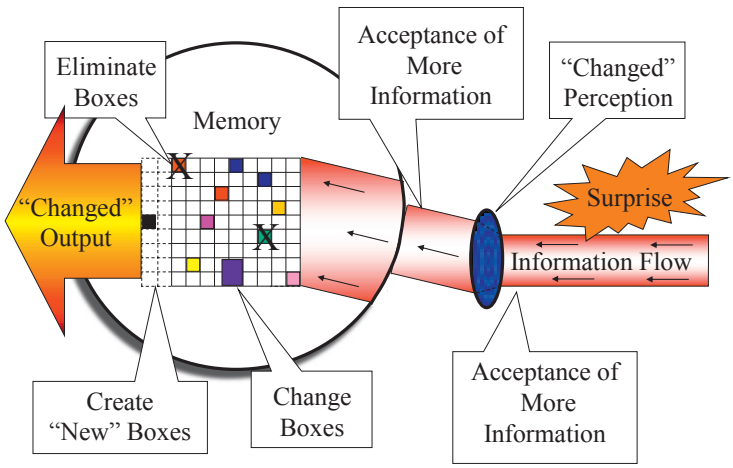

Figure 2: Changes to Processing and Ordering Information

[19] Colin S. Gray, "Thinking Asymmetrically in Times of Terror," *Parameters*, Spring 2002, pp. 5-14.

Throughout history, leaders at all levels have operated with limited information and constrained situational awareness. Today, decision-makers are suffering the embarrassment of riches, virtually drowning in data delivered at a velocity and volume far exceeding their ability to absorb. The United States must continue to develop systems that are not just network-centric, but knowledge-centric. These systems would integrate data in a manner consistent with natural neurological patterns, presenting information in a format that enables timely, logical decisions. To this end, we must fully harness the power of machine-to-machine interface, freeing up human resources for activities where intellect and esprit remain indispensable.

Warning and decision superiority further demonstrate this dilemma. Indications and Warnings are collected, processed, evaluated, and disseminated by the Intelligence Community—a highly complex, largely closed system, comprised of individuals, groups, organizations, technologies, and processes. The people who make up the system are subject to biases and preconceptions that define their perceptual prism—the mental lens through which each human processes information. Inputs that could become warnings are interpreted by diverse groups and hierarchies who shape content, detail, and level of urgency—well before the warning is delivered to decision-makers for action.[20]

Whether a warning was actually issued—and, if so, by whom and when—is an interesting element of the post-mortem and institutional finger-pointing that usually follow surprise. While such claims might be personally or organizationally gratifying, they are ultimately irrelevant. Warning means nothing if decision-makers fail to act. Such failure might occur for any number of reasons. It might reflect a natural reluctance to deliver or accept bad news, and the equally understandable preference for consensus—versus a direct challenge to authority or dissent from conventional wisdom. Action might also be delayed due to often justifiable concerns that overt counter-measures and steps to enhance readiness might actually be mistaken as aggressive and provoke the adversary. Last and perhaps most pernicious, inaction might mirror the primordial inability to imagine the full nature and magnitude of a looming threat.

These perspectives shed new light on the often-discussed distinction between "intelligence failure" and "policy fiasco."[21] To use a recent example: there is little doubt that the surprise attacks of September 11, 2001—and the in-depth inquiries that followed—weighed heavily in the Intelligence Community's and

[20] Mark M. Lowenthal, *Intelligence: From Secrets to Policy, 5th edition* (Washington, D.C.: CQ Press, 2012). See also Cynthia M. Grabo, op.cit and Jonathan S. Lockwood, op.cit.

[21] Russell G. Swenson, *Intelligence Dissemination: A Key to Strategic Warning* (Washington, DC: Defense Intelligence College, July 1994), pp. 1-18. See also, Daniel F. Landers, "The Defense Warning System," *Defense Intelligence Journal*, Spring 1994, pp. 21-32.

Executive Branch's reaction to mounting indications and warnings that Iraq was pursuing weapons of mass destruction (WMD). Reflecting those concerns, the first *National Security Strategy* issued by the Bush Administration in September 2002 highlighted the policy of "anticipatory action," designed to forestall hostile acts "even if uncertainty remains as to the time and place of the enemy's attack." In other words, the declaratory policy of the United States was to avert surprise through preemption.

Throughout 2002, the Bush Administration sought Iraqi compliance with U.N. Security Council Resolutions, while holding out the possibility of U.N Chapter VII ("all means necessary") action if Iraq did not comply. Addressing the U.N. General Assembly that September, President George W. Bush stated: "The Security Council Resolutions will be enforced … or action will be unavoidable." In October 2002, the "Joint Resolution to Authorize the Use of United States Armed Forces against Iraq," reiterated that "it should be the policy of the United States to remove the Saddam Hussein regime and promote a democratic replacement" through "any means necessary."

The Administration's intent was formally stated in a March 17, 2003 ultimatum to Saddam Hussein and his sons to leave Iraq within 48 hours. "Their refusal to do so," President Bush said, would "result in military conflict…we will tear down the apparatus of terror…the tyrant will soon be gone." Operation Iraqi Freedom was launched three days later.[22]

No WMDs were found in Iraq and, within months of toppling the regime, the focus of the U.S.-led coalition shifted to the more open-ended and demanding mission of securing the environment while helping establish governance through counter-insurgency operations. As casualties mounted and the war came to be seen as a costly, multi-year occupation, public opinion turned dramatically. In February 2003, 64 percent of Americans had endorsed military action to remove Hussein from power. By May 2007, 55 percent believed that the war had been a mistake. President Barack Obama was elected in November 2008, promising, among other things, to end this "unwise" and "dangerous distraction." On December 18, 2011, the last of U.S. troops pulled out of Iraq, even as the country continued to convulse in sectarian violence. [23]

While debates as to the respective roles played by intelligence and policy have largely ended in an uneasy truce, Iraq continues to cast a long shadow on U.S. views of other looming threats. Most notably, the Iraq WMD debacle has become a key facet in the prism through which Iran's quest for nuclear capability is viewed. If 9/11 is perceived as a failure to connect the dots and respond in a timely manner, Iraq is widely viewed as over-reaction to what now, in hindsight, is seen as faulty analysis. The policy toward Iran reflects the desire to find a middle path that avoids both extremes. If so, it is worth noting that the propensity to procrastinate is

[22] Congressional Research Service Report: *Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress*, March 28, 2008.
[23] Ibid.

directly proportional to the time one believes is available. The inescapable corollary is that warning time is wasted time, unless action is taken.

Denial and Deception: The Keys to Surprise

Given the United States' global interests and alliance commitments, adversaries have a major incentive to use denial and deception against U.S. intelligence collection and analysis. If warning is denied or delayed, a *fait accompli* might preclude timely action to avert the threat. Terrorist and criminal networks are especially reliant on—and adept at—denial and deception at all levels. Proliferators of WMDs and advanced weapons systems, as well as illicit narcotics and people traffickers, are also highly incentivized to avoid detection by modern intelligence, surveillance and reconnaissance—the "unblinking ISR eye."[24]

There is limited understanding of the unique ways in which nations and non-state actors view denial and deception as force-multipliers. The United States and its allies are likely to be faced with Russian-style efforts to hide the real and show the fake, regardless of the tenor of East-West relations.[25] Iran's ongoing efforts to literally bury its nuclear facilities in deep underground installations—while professing that its massive complex is designed for the peaceful purpose of producing energy and medical isotopes—are prime examples in this regard. Meanwhile, China has been very consistent in employing surprise, denial and deception as asymmetric means to thwart U.S. interests in a region it aspires to claim as its own sphere of influence.[26] Likewise, AQ manuals and even a cursory Internet search clearly demonstrate that these asymmetric tools and relatively inexpensive enabling technologies are easily accessible to terrorists, narco-traffickers, and assorted criminal organizations. [27]

Deception is critical to achieving surprise. Combined, surprise and deception produce a synergy, significantly increasing the chances of success. Indeed, denial and deception are usually clues—and, thus, warnings—of hostile intent. Simply put, why would anyone bother to mask or obfuscate something that is legitimate and harmless? The elements of deception—the false depiction of reality—one would want to show an adversary are quite simple:

[24] David A. Kay, "Denial and Deception Practices of WMD Proliferators," *The Washington Quarterly*, Winter 1995, pp. 83-105.

[25] Richard N. Armstrong, *Soviet Operational Deception: The Red Cloak,* Defense Technical Information Center DAI-PMH Repository, 1989, http://www.dtic.mil/dtic/tr/fulltext/u2/a211726.pdf.

[26] David Andrew Graff, "The Dao of Deception: Unorthodox Warfare in Historic and Modern China," *Journal of Military History,* July 2007, pp. 910-912.

[27] "Special Dispatch—Jihad and Terrorism Studies," The Middle East Media Research Institute (MEMRI), Feb. 10, 2002, No. 344, pp. 1-4. For more current translations and analysis see www.memri.org and www.siteintelgroup.com. See also, Richard H. Shultz and Ruth Margolies Beitter, op.cit.

- Your capabilities and vulnerabilities are different than they really are;
- You intend to do something else than expected;
- You intend to do it elsewhere;
- You intend to do it in a different manner;
- You intend to do it at a different time;
- You know more (or less) about your competitors than you really do; and/or
- Their actions are more (or less) fruitful than they really are.

Confirming an opponent's expectations is always easier than trying to change his perceptions. Therefore, a good deceiver "helps" the adversary build a false picture of reality by providing consistent, reinforcing clues, through multiple channels, using the target's behavior as feedback to modulate these inputs. The aim is to cause the adversary to commit the critical errors that will serve one's own plan; increase an opponent's susceptibility to our actions; and deny him the opportunity to capitalize on our vulnerabilities.[28]

Successful denial and deception, as well as timely warning and decision, hinge on an accurate understanding of the capabilities and limitations of Command, Control, Communications, Computers, Intelligence, Reconnaissance (C4ISR)—both one's own, as well as the adversary's. If collection and analysis sources, methods and processes are known, an adversary might be able to avoid or delay detection, thus buying time and enhancing the chances of achieving surprise. Likewise, insight into adversaries' decision-making processes creates opportunities for controlling the flow of information, adding misleading information, and otherwise distorting perceptions.[29]

Strategic Implications

All strategic planning is based on a set of assumptions. Surprise occurs when core assumptions are proven wrong. History is replete with examples of militaries and intelligence communities that failed due to their inability to validate assumptions, adopt new concepts, transform organizational culture, or leverage breakthrough technologies. But militaries and intelligence services do not fail by themselves. Failure occurs in the context of an overall, national fiasco, caused by systemic problems that fall into three distinct but related categories:

- *Failure to Anticipate* the nature of and trends within the strategic environment; the character of the opponent; one's own will and resolve; the

[28] Lt. Gen. Bernard E. Trainor, USMC (Ret.), "Deception," *Marine Corps Gazette*, October 1986, reprinted October 25, 2011, www.mca-marines.org/gazette/deception.
[29] Joseph W. Caddwell, "Deception 101, US Army War College Monograph," Strategic Studies Institute, December 2004. *See also,* Paul Rossa, "The Denial and Deception Challenge to Intelligence" in Roy Godson and James J. Wirtz, op. cit., pp. 223-228.

impact of technology—be it disruptively new or employed in unexpected ways; and failure to anticipate the second and third-order effects of both action and inaction.

- *Failure to Learn* from experience—both one's own and others'. Selective reading of history is particularly pernicious here, as is mistaking "lessons recorded" with lessons actually learned.

- *Failure to Adapt* behaviors, concepts and institutional constructs to the ever changing domestic and international dynamics, as well as to evolving adversarial operational, technological, and/or doctrinal innovations. Failure to validate pivotal assumptions and adjust accordingly falls in this category as well.[30]

In contrast, victory comes to those who foresee, recognize and act upon emerging changes in the strategic environment. Thus, the first strategic implication is: beware of complacency and the perils of strategic myopia. The lack of foresight which led the British to conclude after the Second Boer War (1899-1902) that, henceforth, the Empire's armed forces needed to prepare for nothing but counterinsurgency was quickly exposed as fallacy in the blood-soaked trenches of Somme and Verdun. The corollary strategic implication is: beware of concepts—however valid for a specific time and place—becoming dogma and stifling fresh thought.[31]

The strategic inferences are readily apparent: First, aggressors tend to assume risks that seem irrational and improbable to the intended victim. This leads to strategic dislocation and, potentially, catastrophic failure. Second, reputation and credibility born of past successes might not suffice as a deterrent. Third, current exigencies must be balanced with future requirements. Any single-focus approach bears a huge opportunity cost. The rest of the world has not taken

[30] For a brilliant, in-depth discussion see Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 1990).

[31] History is replete with examples of disasters born of a lack of strategic prescience. The U.S. Army after the Civil War spent 30 years fighting Native Americans, only to struggle to deploy a brigade 80 miles off the coast of Florida, against Spain in Cuba. Similarly, Britain and France post-1815 let their militaries atrophy—while their hubris blossomed—resulting in a blood bath in the Crimean War and near-existential disasters in the two World Wars that followed. Likewise, in the wake of their spectacular victory in the June 1967 Six Day War, the Israel Defense Forces rested on their laurels, ceased innovating, and focused on policing the newly acquired territories, secure in the soon-to-be-proven fallacy that past successes and strategic depth will deter any future conventional threat. Six short years later, in early October 1973, Israel was fighting for its very survival on the Syrian and Egyptian fronts, having fallen victim to strategic surprise masterfully orchestrated by the seemingly defeated foe.

a time out while the United States tended to Iraq and Afghanistan. Fourth, while successes and failures are both relative, they are binary in the eye of the beholder. Specifically, for a great power like the United States, there is no such thing as "minor setback." Anything less than a clear success—perceived as such by friend and foe alike--will echo in the interconnected global village and feed the narrative of America as "the giant with feet of clay."

A compelling description of what failure might look like is as important as a crisp articulation of the desired outcome. The latter describes how we want the situation to be after the mission is accomplished. The former lays out the undesirable alternative end state—the consequences of a mission left undone. Yet, imagining failure is simply not in America's—or any nation's—DNA. Consider the following truism: the only certain thing about war is that one side will lose. Yet, since time immemorial, nations and armed groups have gone to war with nothing but a picture of victory imprinted in their minds. Saying that "failure is not an option" is, thus, nothing but an exhortation. In truth, failure is an ever-present possibility.

Debacles-in-the-making develop over time, usually with plenty of opportunities to notice and rectify the downward spiral. What prevents the needed course correction are systemic deficiencies, wishful thinking, as well as the ingrained human ability to adjust to a "new normal"—the shifting baseline of what is deemed acceptable.

At its core, the inability to conceive anything but a resounding success is a failure of the imagination. It is also a natural defense mechanism. Humans tend to repress or explain away the ever-present potential for failure. Bad experiences are particularly tempting to forget. Yet imagining what failure might look like is a necessary step in laying out the foundation for success.

For a nation whose security is predicated on an enduring strategy of dissuasion, the most fundamental risk is failure of deterrence. Deterrence is a function of capability, will and credibility and exists in the eye of the beholder. Its success or failure is measured only in the breech. To mitigate the risk, we must retain a modern, agile and well-trained military, a responsive, collaborative interagency, and a responsible, engaged private sector. We also need to evolve new deterrence concepts suitable for asymmetric actors deemed "undeterrable" in the Cold War construct. [32]

[32] George P. Shultz, William J. Perry, Henry Kissinger, and Sam Nunn, "Deterrence in the Age of Nuclear Proliferation: The doctrine of mutual assured destruction is obsolete in the post-Cold War era," *The Wall Street Journal*, March 7, 2011, http://online.wsj.com/article/SB10001424052748703300904576178760530169414.html; Amatzia Baram,"Deterrence Lessons From Iraq: Rationality Is Not the Only Key to Containment," *Foreign Affairs,* July/August 2012, http://www.foreignaffairs.com/articles/137693/amatzia-baram/deterrence-lessons-from-iraq; Robert G. Joseph and Keith B. Payne, "On Deterring Iran," *National Review*, June 25, 2012, http://www.nationalreview.com/articles/303826/deterring-iran-robert-g-joseph.

Strategic risk can also mount through the accumulation of shortfalls in recapitalization and modernization; stale strategic and operational concepts; and failure to revitalize organizational ethos, outdated structures, sector boundaries, and hierarchical relationships. America's future success depends upon its ability to adopt new, relevant concepts and technologies, suitable to the dynamics of the strategic environment.

National Imperatives

Today's confluence of global trends foreshadows significant challenges to the nation's security. The world is at an historic inflection point, demanding an equally comprehensive transformation. The future strategic environment will be shaped by the interaction of globalization, economic disparities and competition for resources; diffusion of technology and information networks whose very nature accords unprecedented ability to cause wide-scale damage; and systemic upheavals impacting state and non-state actors and, thereby, international institutions and the world order. The following are salient features of this increasingly complex, dynamic, lethal, and uncertain environment:

- Violent extremism and ethnic strife—a global, generational, ideological struggle;
- Proliferation of weapons of mass destruction and empowering technologies;
- Rising peer competitors with voracious appetites for resources and influence;
- Predatory and unpredictable regional actors;
- Increasing lethality and risk of intrusion by terrorist and criminal organizations;
- Systemic instability in key regions (political, economic, social, ecological);
- Unprecedented velocity of technological change and military adaptation;
- Availability of advanced weapons in a burgeoning global marketplace;
- Exponential growth in volume, exchange and access to information;
- Greatly reduced ability to retain high-level national security secrets; and
- Extremely rapid decay rates for any domain advantage.

These dynamics are closely intertwined with the changing character of warfare. Having experienced—or vicariously learned—the cost of challenging the United States head-on, would-be adversaries are developing asymmetric approaches to

circumvent America's core advantages, while undermining international support and domestic resolve. [33]

The unprecedented lethality and effectiveness of Western militaries deter opponents from massing on the battlefield, driving them to adopt distributed and dispersed operations. They find maneuver space and sanctuary in dense urban areas, ungoverned hinterlands, and loosely regulated information and social networks. These adversaries pose a significant challenge to America's vital interests at home and abroad.

Meanwhile, ascendant powers—flush with new wealth and hungry for resources and status—are posturing to contest U.S. superiority. These adaptive competitors are also translating lessons from recent conflicts into new concepts, capabilities and doctrines tailored to counter U.S. strengths and exploit vulnerabilities.[34] Consequently, the United States and its allies face an unprecedentedly varied array of threats, ranging from existential to potentially crippling perils.

Existential threats are risks to America's way of life as a democratic society with a functioning economy, governance, public services, and infrastructure. By definition, the result of an existential threat is that the United States, as we know it, ceases to exist. Among such threats are: large-scale nuclear attack; biological attack against people and/or food supply chain; total cutoff of energy; massive cyber attack—to include electro-magnetic pulse (EMP)—which brings our way of life to a standstill; rapidly spreading pandemic overwhelming all services; natural disaster on an unimaginable scale; weaponized, disruptive technology that threatens extinction or long-term paralysis (e.g., bioengineered pathogens or plasma weapons).

Among existential threats to allies—possible, but unlikely to the United States—are: foreign invasion; genocide; violent regime change resulting in civil or cross-border war; famine (natural or man-made), climate change leading to mass migration.

Existential threats should be distinguished from crippling threats which severely affect a segment of society, a geographic region, or an isolated portion of the country's infrastructure. A crippling threat is recoverable, although the recovery

[33] Thomas Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul: Zenith Press, 2004).

[34] Consider, most notably: Anti access/Area denial weapons and operational concepts designed to limit U.S. freedom of action, potentially placing Carrier Battle Groups and Amphibious Forces at unacceptable risk; "Generation 4-plus" aircraft, like the Chinese J-29, that could challenge America's aging fleet and, potentially, air superiority; Increasingly lethal, integrated air defense systems that could negate weapons and tactics used to suppress or destroy these systems; Proliferation of surface-to-surface missiles with growing range, precision, mobility, and maneuverability—capable of delivering both conventional and non-conventional payloads; Proliferation of unmanned aerial systems capable of conducting low observable, persistent, intrusive missions in both lethal and non-lethal modes; Resurgence of offensive counter-space capabilities; Increasing ability of even marginal actors to observe and track the disposition of U.S. assets through widely-available, inexpensive commercial means; Attacks through cyberspace are already creating tactical, operational and strategic effects at low cost and with relative impunity.

could be long and painful. A synchronized series of crippling threats could become existential, if the government and the private sector fail to break the chain of cascading effects.

The list of possible crippling threats is quite long and could include: localized radiological explosions ("dirty bombs"); threats to essential commodities such as water, fuel, food, medicine, etc.: geographically isolated natural disasters; isolatable low-order nuclear, chemical, or biological attacks; large-scale refugee flow into southeast or southwest United States; blockage of major transportation nodes; sporadic cyber attacks on communications infrastructure, stock exchange, power grid, and petro-chemical plants; synchronized terror attacks on high-value, high-prestige targets, massive public unrest and economic collapse.

Even if the United States continues to successfully dissuade major competitors, their advanced equipment is proliferating worldwide. America and its allies must also be vigilant to adversary breakthroughs in fields such as cybernetics, nanotechnology, biotechnology, electromagnetic spectrum physics, robotics, advanced propulsion, etc. No one should assume that the next military revolution will originate in the West. Indeed, the hub of innovation in science and engineering education has shifted eastward. Therefore, the United States must anticipate innovative combinations of traditional and new concepts, doctrines, weapons, and disruptive technologies.

From this point forward, the United States should expect to be challenged in all domains, including in and through space and cyberspace, as well as on land, at sea, and in the air. Perhaps for the first time in history, the ability to inflict damage and cause strategic dislocation is no longer proportional to capital investment, superior motivation and training, or technological prowess. Consequently, the Nation is in dire need of a holistic approach that balances today's exigencies with the far-reaching implications of looming threats. Time is not on our side. Indeed, the window of opportunity is shutting fast because ever-lower technological and financial entry costs favor our competitors.

The U.S. military's non-negotiable commitment is to provide forces proficient across the full range of military operations to protect the United States, its values, interests and allies; deter conflict and prevent surprise; and, should deterrence fail, prevail against any adversary. The Joint Team must enhance its own asymmetric advantages while retaining the ability to safeguard the Homeland, assure allies, dissuade opponents, and inflict strategic paralysis on adversaries.[35]

During an era in which the national debt is itself a major security threat, all Services should avoid duplication in acquisition, procurement, manning, and operations. To this end, the series of cross-Service initiatives already underway—

[35] *The National Military Strategy of the United States of America, Redefining America's Military Leadership*, 2011, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.

aimed at generating both savings and synergies—should continue to expand.[36] The Department of Defense should also enhance collaboration with the Departments of State and Homeland Security, the Intelligence Community, law enforcement, other Interagency, and private sector partners to facilitate a more effective orchestration of all elements of national power.

America's strategic partnerships are more important than ever. The United States must strengthen its coalitions, attending to interoperability among allies. Building these relationships is both an engine of progress and prosperity, as well as a potent instrument of America's diplomacy in an interconnected world.[37]

The shared touchstone of the virtues enshrined in the Constitution and a single, unifying purpose "to provide for the common defense" must remain unchanged. The United States will have neither the buffer of time nor the barrier of oceans in future conflicts. The character, tempo and velocity of modern warfare already severely test the military's ability to anticipate and adapt. Therefore, redefining the interagency and the private-public relationship is an urgent national security requirement—not a luxury we can defer. It is also a duty to bequeath a dominant, agile, responsible joint, interagency, and public-private team to those that will follow in service to the nation. Rising to this challenge is not a choice. It is both a shared responsibility and an urgent national imperative.

[36] The U.S. Navy's and Air Force's Air-Sea Battle is a good example. General Norton A. Schwartz, USAF & Admiral Jonathan W. Greenert, "Air-Sea Battle**:** Promoting Stability in an Era of Uncertainty," *The American Interest*, February 20, 2012, http://www.the-american-interest.com/article.cfm?piece=1212.

[37] Robert M. Gates, "Helping Others Defend Themselves: The Future of U.S. Security Assistance," *Foreign Affairs,* May/June 2010, http://www.foreignaffairs.com/articles/66224/robert-m-gates/helping-others-defend-themselves; Admiral James G. Stavridis, USN, *Partnership for the Americas: Western Hemisphere Strategy and U.S. Southern Command* (Washington, D.C.: NDU University Press, 2010).