Surprise, Deception, Denial, Warning and Decision:
Learning the Lessons of History

By
Dr. J.P. (Jack) London, Executive Chairman
CACI International Inc
Dr. Lani Kass, Strategic Corporate Advisor, Senior Vice President
CACI International Inc

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” in Sun Tzu’s Art of War. From ancient Persia, Greece and Rome, through two World Wars, through the first decade of the 21st century, nations and non-state actors have practiced surprise and deception and have fallen victim to them – often with devastating consequences.

The long history and frequent occurrence of surprise and deception suggest that these are essentially psychological phenomena, rooted in human nature and, therefore, inherent in the very nature of force and diplomacy. If so, they will continue to happen across the entire range of human discourse. Our exquisite C4ISR, peerless intelligence, superior data management, and unrivaled training and equipment can only ameliorate – but not erase altogether – the limits of human cognition.

The best intelligence services and most elaborate warning systems have failed to predict war. For example, the Soviet leadership was surprised by the German invasion of June 1941. Israeli intelligence, considered one of the very best, failed to anticipate the Arab attack of October 1973. In between these two events, U.S. intelligence failed on at least five occasions to anticipate attacks on U.S. forces and/or security interests. The record since 1973 is not much better, including 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; the December 1989 Operation JUST CAUSE and the August 1990 Iraqi attack on Kuwait. Operations DESERT STORM, ALLIED FORCE, ENDURING FREEDOM, IRAQI FREEDOM and ODYSSEY DAWN (Libya) – to note just the better known – all involved successful surprise and deception.
On the political/diplomatic front, we have failed to anticipate and prepare for such inflection points as: the fall of the Shah in Iran and the ensuing hostage crisis; the collapse of the Soviet Union and the Warsaw Pact; the genocide in Rwanda and Sudan, leading to the latter country’s partition; the rise of violent Islamist extremism as a global ideological movement; the collapse of the U.S. lending, banking and housing bubble and the ensuing economic downturn; 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 – including the brutal civil war in Syria.

While unpredictable by their very nature, we’ve also been caught unawares by – and unprepared for – such disasters as: meltdowns of two nuclear reactors (Chernobyl in Ukraine in 1986 and, as of this writing, precisely a year ago, the Fukushima reactor in Japan); rising oil prices – now at $110 a barrel; devastating Tsunamis, earthquakes, oil spills (Exxon and BP) and hurricanes – including Katrina – which forever changed our view of domestic disaster preparedness and relief.

Cyber attacks straddle all 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 attack on Iran’s nuclear production facilities, which, perhaps for the first time in history, physically destroyed infrastructure without using kinetic force); others remain unattributed and disclosed only through unauthorized leaks – or written off to natural causes – from faulty fuses/wiring to solar flares. These accumulating warnings notwithstanding, it is a safe bet that if and when a major cyber attack cripples the U.S., paralyzing both our EMS-reliant military and our inter-netted way of life, it’ll be considered a surprise to rival both Pearl Harbor and 9/11.

History – meaning our collective and individual experiences – has not been a good teacher. Superpowers, small nations and non-state actors have all deliberately deceived and been deceived, surprised others and fallen victim to surprise. Deliberate attempts to surprise and deceive rarely fail. For example, each of the great powers involved in WWII was both a victim and a perpetrator: The British were surprised by the German invasion of Norway and the Japanese attack on Singapore; the French were surprised by the German invasion of their country; the Russians by “Barbarossa”; the Americans by Pearl Harbor and by the German counter-offensive in the Ardennes; and the Germans by the Allied landing in Normandy.

Egypt, militarily surprised by Israel in 1956, failed to learn the lesson and was surprised again in June 1967. Israel, having twice managed a surprise attack on Egypt, was in turn surprised by it in October 1973. Its fabled intelligence notwithstanding, Israel was surprised again during the Camp David peace talks and, most recently, by the 2011 Arab Spring, the ousting of the Mubarak regime, and, perhaps most significantly, by the ascent of the Muslim Brotherhood – a closely-monitored group founded in 1928, rooted in fascism and Islamic extremism – across the Middle East and North Africa, thus fundamentally transforming the strategic landscape.

Likewise, since the October 1983 homicide bombing of the Marine Barracks in Beirut, the U.S. has been the target of several high-impact terrorist acts – including the 1993 attack on the World Trade

The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which, like fog or moonlight, often tends to make things grotesque and larger than they really are. Whatever is hidden from full view in this feeble light has to be guessed by talent, or simply left to chance … When surprise is successful, it leads to confusion and breaks the enemy’s courage.

Clausewitz, On War
Center; the 1998 bombing of U.S. embassies in Kenya and Tanzania; and the 2000 attack on the USS Cole in Aden – all traceable to al Qaeda. Yet, until September 11, 2001 few Americans were aware of the fact that this militant organization has declared war on the U.S., making America’s citizens and global interests its stated targets. Thus, the 9/11 attacks on the World Center and the Pentagon – 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.

All the example cited above demonstrate that surprise attacks have at least three things in common: first, they are always traumatic to the victim; second, they accord a significant, albeit temporary, advantage to the initiator; and third, they generate a seemingly endless stream of assessments and analysis seeking to divine what happened and why, who was at fault, and how a similar failure could be avoided 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 21st century, even as we continue to search for solutions that would alert us to threats, facilitate warning, improve decision-making, avert surprise, expose deception, and make us more resilient, better organized, and prepared to deal with their aftermath.

In the course of this Symposium, we'll look at surprise from both the victim’s and the initiator’s perspective, seeking to identify the common characteristics – and implications – typical of all surprises. We'll try to understand the who, what, when, why and how (4WH) of surprise, deception, denial and warning. We'll also look at ways to strengthen our threat assessment and Indications and Warning (I&W) systems and facilitate better decision-making in peace, crisis and war.

The Symposium is oriented to the interface between intelligence, military strategy and policy making writ large. Accordingly, we'll examine how strategic and operational surprise are achieved using a combination of active (deception) and passive (security) measures. We'll also consider how best to foil these efforts through effective intelligence, surveillance, reconnaissance, data fusion and decision superiority. Throughout, our focus is on the critical linkages between technology and cognition, and their long-term implications for U.S. security.

Our discourse is based on the proposition that strong, confident nations lack the natural incentive to employ surprise, denial and deception – indeed, these are often dismissed as “weapons of the weak.” This is why surprise, denial and deception are the ultimate asymmetric threats: they exploit our natural proclivities and inherent vulnerabilities, capitalizing on vanity, complacency and self-delusion. Unable to take their opponents head on, these actors rely on shock and psychological dislocation as force multipliers. Defeating them requires understanding the nature and impact of surprise, as well as developing the means to minimize its impact and consequences. For surprise only determines the time and place of the first engagement. It rarely determines the ultimate outcome. That said, this principle is up for grabs and must be reaffirmed every single time – by both the victim and the initiator. Likewise, guile is not the

---

The task that the intelligence people face today is vastly more difficult in my view than it was [during the Cold War]. We are dealing with closed societies that have developed all kinds of skills in denial and deception; we're dealing with societies that have benefited from [the] size and problems we've had in the release of classified information about how we do things, which makes denial and deception much easier for others.... [Rogue states are] not only trading technologies for powerful weapons, they're also trading technologies and knowledge about how to deny and deceive.

Secretary of Defense Donald Rumsfeld
September 17, 2003
opposite of valor – nor a good substitute for it – but it saves lives. It’s an asymmetric
advantage we forfeit at our own peril.

With this in mind, what follows is a set of rules useful to both warriors and diplomats,
decision-makers and those who support their endeavors in remaining ever vigilant in
providing for the common defense.

1. You don’t know what you don’t know, and what you don’t know can be a disaster.

2. If the situation is crystal clear, and everything you see fits your expectations, hopes and plans,
you are probably being deceived.

3. Surprise is the ultimate asymmetric threat because it exploits weaknesses and capitalizes on
vanities.

4. Don’t confuse estimates with facts. The level of classification is not a good indicator of reliability,
relevance or validity of the information you receive.

5. There are no universal standards of rational behavior (or stupidity). Just because you wouldn’t do
something doesn’t mean someone else won’t.

6. Don’t fall in love with your plan, policy or estimate of the situation. Expect the unexpected and
be able to imagine the worst. Hope is not a viable strategy!

7. Beware of group-think. Give a fair hearing to alternative viewpoints, even if this means admitting
you might be wrong.

8. Warning is about being safe, not about being right. Trust your instincts, be ready to pay the
price that goes with that, and don’t punish those who “cry wolf.” Sometimes the wolves are really at
the gate and a threat is more than just “rhetoric.”

9. Timely, unambiguous, warning is nice to have, but don’t count on it. Don’t assume (or expect)
that appropriate political decisions and authorities would automatically follow warning. You’ve got a
lot of latitude in your own organization. Use it and do what’s right.

10. Stuff happens. So does surprise. Don’t be a victim.