Dealing With Today's

Asymmetric Threat to U.S. and Global Security

Employing Smart Power

This document is intended only as a summary of the personal remarks made by participants at the March 24, 2009 symposium, "Dealing With Today's Asymmetric Threat to U.S. and Global Security, Symposium Three: Employing Smart Power," co-sponsored by CACI International Inc (CACI) and the U.S. Naval Institute (USNI). It is published as a public service. It does not necessarily reflect the views of CACI, USNI, the U.S. government, or their officers and employees.

September 2009

Contents

Executive Summary **2**

1 Introduction **6**

2 Application of Soft Power Against Asymmetric Threats **9**

2.1 Offensive Dimensions of Soft Power 9

2.1.1 Offensive Soft Power Used by Asymmetric Adversaries 9

2.1.2 American Use of Offensive Soft Power 11

2.2 Defensive Dimensions of Soft Power 12

2.2.1 Sources of Defensive Soft Power 13

2.2.2 Defensive Soft Power Challenges 13

2.2.2.1 Failed and Failing States 13

2.2.2.2 Logistics and Asymmetric Opportunism 13

2.2.2.3 Strategic Communications 14

2.2.3 Exploiting Defensive Soft Power 14

2.3 The Rule of Law in Soft Power 15

2.3.1 As a Foundation for Legitimacy 15

2.3.2 As a Counterterrorism Tool 16

2.4 Soft Power and the Competition to Govern 16

3 Smart Power – From Theory to Practice **17**

3.1 Integrating Soft Power With Hard Power 18

3.1.1 Balance 18

3.1.2 Agility 19

3.1.3 Sustainability 20

3.2 Challenges to Effective Smart Power 21

3.2.1 Maintaining a Flexible Balance 21

3.2.2 Rule of Law 22

3.2.3 Organizational Roadblocks 23

3.2.4 Financing Smart Power 24

3.2.5 Strategic Communications 25

4 The Cyber Domain and the Evolution of Smart Power **25**

4.1 The Challenging Nature of Cyberspace 25

4.2 The Law and Cyberspace 26

4.3 Applying Smart Power to Cyber Threats 27

5 Toward a National Strategy to Meet Twenty-first Century Asymmetric Threats ... **29**

5.1 The Current State of U.S. National Security 29

5.2 The Future of Smart Power and U.S. National Security 30

Appendix A: Synopses of Prior Asymmetric Threat Symposia **32**

Glossary **33**

Acknowledgments **36**

Executive Summary

Prior to the fall of the Soviet Union, most national security challenges facing the United States were posed by nation-states, wielding power based primarily on conventional military arsenals. However, even during the Cold War era, the United States began to understand that there are limits on the efficacy of a powerful military force to achieve non-military objectives.

It became increasingly clear, particularly in the wake of the attacks of September 11, 2001, that the proliferation of irregular actors who migrate fluidly between civilian communities and terrorist organizations – potentially with weapons of mass destruction at their disposal – pose particularly daunting security challenges to the United States. Novel, unconventional threats and enemies can only be anticipated and overcome through the multidimensional and flexible application of *smart power*, the balanced synthesis of hard and soft power.

A consensus has emerged that American smart power is dependent upon an effective and sustainable application of the collective and coordinated strengths of government institutions, the private sector, and America's cultural reach. All must be integrated to meet the asymmetric threats the United States faces today: from violent Islamic extremism, drug trafficking, and nuclear proliferation to economic recession, global poverty, impending natural disasters, and other asymmetric threats.

To contribute to the continuing national discourse as the U.S. government restructures its national security apparatus to meet twenty-first century challenges, CACI International Inc (CACI), along with the National Defense University (NDU, Symposium One) and the U.S. Naval Institute (USNI, Symposia Two and Three), held a series of three symposia to examine and define the asymmetric threat; to encourage a national dialogue on the key elements of a revised national security strategy; and to develop an understanding and framework for effectively implementing smart power.[1]

"It has been well known for years that the old threat response paradigm of the Cold War era no longer fits today's ongoing socio-economic, political, and military security challenges. Add religious, ethnic, and ideological conflicts that cross national boundaries to that mix, and there is no doubt a new response strategy is needed."

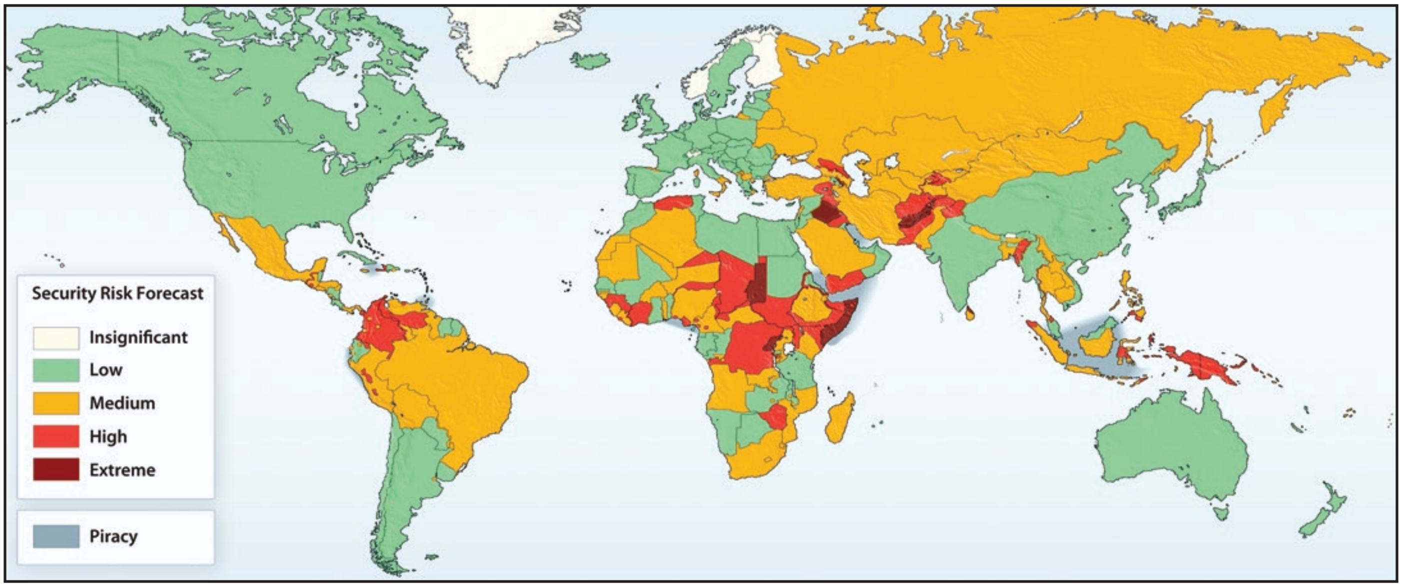
– Jack London

Symposium Three, *Employing Smart Power*, addressed the offensive and defensive components of soft power and explored how the concept of smart power could be implemented in a highly net-centric world, in both the human and technological sense.

Since the first two symposia, held in May and October 2008, a new administration has assumed office with the promise of modifying the national security structure; renewed tensions in the Middle East and widespread piracy off the coast of Somalia escalated global threats; and the worldwide financial crisis worsened to a point not seen since the 1930s. As the Obama administration continues to gather momentum, it is important to ask how power should be structured into a practical national security strategy that will work effectively and best serve the United States, its allies, and the world, now and in the future. While the nation's ability to respond militarily will likely remain dominant, the United States must be aggressive and innovative in seeking opportunities to apply both hard and soft instruments of power in a balanced, harmonized, agile fashion.

America's adversaries are succeeding by using soft power – America and other nations are facing networks of adversaries who already understand the benefits of, and are using, smart power strategies against the West. Military responses have seen only limited and short-term success. Terrorist organizations, such as Hamas, Hezbollah, and Al-Qaeda, recognize the critical importance of soft power as a complement to hard power. They have adopted a strategy of dominating the security and service sectors in contested regions, thereby limiting America's effectiveness in exploiting those sectors.

[1] The findings of Symposia One and Two are summarized in Appendix A: Synopses of Prior Asymmetric Threat Symposia. The published reports on these symposia can be retrieved from http://www.asymmetricthreat.net.



Security risk projections for 2009. The multidimensional and flexible application of smart power, encompassing multiple actors and instruments of power, is required to deter and defeat global asymmetric threats. Graphic courtesy of CACI. Map reference: Control Risks' RiskMap 2009.

They fill a void that the local governments cannot by supplying health, education, and social and welfare services to vulnerable populations. Recipients of these services, therefore, do not necessarily perceive these groups as terrorist organizations, as the U.S. and other foreign governments do.

America must effectively exploit offensive and defensive smart power – There is an important distinction between offensive and defensive projections of power. The distinction is well understood in hard power discussions, but is undeveloped in soft power discussions. *Offensive* soft power deals with shaping preferences and outcomes, while *defensive* soft power deals with diminishing the hard and soft power capabilities of adversaries. Understanding the offensive and defensive projections of soft power is a prerequisite to improving their effectiveness and application to a comprehensive smart power strategy.

Defensive soft power is the least understood aspect of soft power, yet offers great potential in protecting and promoting American security interests. It diminishes or blocks an adversary's soft and/or hard power capabilities by promoting continued loyalty of a population to an individual, state, or organization. While defensive hard power seeks to prevent military incursions of adversarial forces, defensive soft power serves to keep at bay adversarial preferences, objectives, and modes of behavior. Defensive soft power also applies to actions that assist friendly and partner countries to increase *their* soft power. This should not be equated to a nation-building strategy. America, however, can be a participant in developing the potential for nations to be built by their citizens.

America and her allies and partners must win the competition to govern – America is fighting not only a battle of ideas, but also a contest over who can most effectively meet the governance needs of people around the world. Competition between state and non-state forces has taken on new dimensions, particularly when it concerns providing security and delivering social services. If the current government is unable to provide safety and services, the population will have little choice but to turn to a provider who can deliver those things expected of government. This is especially true in failed or failing regimes, but can also be the case in regions with more stable governments.

As a result, such regions offer asymmetric actors opportunities to establish themselves as powers that challenge the authority and co-opt the legitimacy of recognized national governments. Through the application of soft (and smart) power approaches, asymmetric actors have, in many respects, supplanted the normal roles of government. They have done so not to fill a void, but to advance their own causes. In the war of ideas, it is clear that America must be as effective in the governance markets as in commercial markets.

Transition from smart power theory to practice is a key challenge – There is a great challenge in envisaging and executing a transition from *theoretical* smart power to *practical* smart power. While many of the concepts associated with smart power appear fairly simple, they become much more complicated when an attempt is made to apply them to real-world circumstances. This is particularly true when operating in the dynamic interagency and international environment.

An essential element of success in this transition is utilizing networks of institutions and stakeholders from across the entire spectrum of national power. It will require budgetary flexibility, adaptability of organizational cultures, and empowerment. Practitioners of soft and hard power are growing in their ability to work together, but their institutions and institutional stakeholders are only slowly adapting to the new environment.

> *"Hard power wins all wars. Soft power wins the peace. Smart power combines those two."*
>
> *– Ambassador Dell Dailey*

Today, and for the foreseeable future, competition will take place in the context of a network of interactions above, below, and through the state. Therefore, the state with the most connections will be the central player, able to be the global center of the agenda and unlock innovative and sustainable growth. Control of the networks for exchange, debt leverage, aid delivery, travel and migration, healthcare delivery, education, telecommunications, information collection and data analysis, multinational cooperation, and cyberspace are central issues in smart power. What is needed is to stay ahead of the capacity of the enemy to organize and network its capabilities.

Leaders of the Badakhshan Province government and representatives from the private sector, NGOs, USAID, and other donors meet in Faizabad, Afghanistan to plan remedies for problems with roads, security, border access, training, mines, drugs, and agriculture. Photo courtesy of USAID.

Balance, agility, and sustainability are the essence of smart power employment – The smart power blend that will work best in a given situation cannot be determined in advance. The smart power blend will need to vary adaptively as events unfold over periods ranging from days to years. There is a need for balance, agility, and sustainability.

Balance – Delivering balanced hard and soft power within a smart power paradigm does not mean using tools and resources from each equally. Nor does balance imply that every security challenge will require both hard and soft approaches. Rather, balanced smart power refers to the accessibility and coordination of hard and soft resources.

Agility – With technological and operational advancements, the need for agility in conventional warfare has been a given for some time. However, agility in smart power is also essential. First, agility in applying smart power quickly and easily is necessary to match asymmetric actors. Adversaries are agile because they are unhindered by competing bureaucracies and complex approval processes. The near absence of constraints on their freedom of action, coupled with access to modern technology and mobility, makes their use of smart power formidable. Second, agility in thinking and drawing conclusions quickly is necessary in responding to asymmetric scenarios.

Sustainability – Contemporary American society is not particularly patient, and the American political system is biased toward providing quick results to constituents. Transitioning to smart power is not synchronized to these political realities, as it takes time to devise, deploy, and achieve results. No one knows how long it will take for a

Electronic warfare officers monitor a simulation test in the Central Control Facility at Eglin Air Force Base, Florida. Portions of their mission may expand under the new Air Force Cyber Command. Photo courtesy of U.S. Air Force.

regional or national smart power strategy to mature, nor is it known how long a smart power contest will last once begun. What is clear, however, is that sustained engagement will be required. America must be not only patient but persistent: engaging, re-engaging, and reinforcing.

Evolution of the cyber domain mirrors smart power evolution – There is no better example of America's need for a timely shift to smart power than the volatile, yet vital frontier of cyberspace, which encompasses almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. A domain that has emerged only in the last 20 years or so, cyberspace includes some of the most contested territory in the war of ideas as well as the (arguably) primary battlefields in asymmetric warfare. It is also a domain that is constantly evolving and where terminology and practices are still to be established. Equally, the roles and responsibilities within and outside the U.S. government for dealing with the cyber domain are yet to be solidified.

Cybersecurity has often been oversimplified as the protection of network data and systems. However, the growing number of attacks on vital financial, government, and military networks has made *cyberterrorism* a national security priority. Strengthening federal leadership and accountability in this area requires clarifying the cybersecurity-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions. However, because of the novelty and rapid evolution of cyber threats, and the lack of agreed-upon terminology, even strategic soft and hard power planners in national security agencies do not fully understand the nature of these threats.

Understanding the asymmetric threats involving cyberspace and the interplay of the elements of smart power provides some of the most useful insights into the demands placed on public and private institutions, and will provide an excellent gauge of the progress in instituting and sustaining the broader national strategy to meet asymmetric threats.

A national strategy to meet twenty-first century asymmetric threats is required – A successful response to the broad array of asymmetric threats requires a "whole of government" approach that combines traditional military power with softer elements of power, such as diplomacy, communications, law enforcement, and commerce.

There is little doubt that smart power should be the driver of U.S. national and global security strategies. But while most senior U.S. leaders are responding to the strategic imperatives of American smart power, there are many implementation issues that remain to be resolved:

1. Implementation – A crucial aspect of the delivery of smart power is determining who will lead, organize, and synchronize the elements of soft and hard power across the government. Existing bodies, like the National Security Council, may provide a starting point. This determination must include interagency functionality and overall responsibility for making smart power work over the long run, independent of administrations.
2. Education – Various agencies have developed best practices that, in many respects, may be adopted and adapted throughout the government as smart power capabilities evolve. However, transition of best practices from one agency to another involves new and evolutionary long-term alignment of resources, authorities, and corporate cultures.
3. Evaluation – Metrics will need to be developed to evaluate both short- and long-term results of smart power initiatives. However, metrics cannot solely be focused on quantitative measurement; they must also gauge opportunities, vulnerabilities, and successes.

4. Collaboration – Smart power is achieved by working within alliances and partnerships – between agencies and departments of the U.S. government, among industry and non-governmental organizations (NGOs), and with allied nations – to create a holistic approach for U.S. national security. Global threats will require global efforts.
5. Anticipation – Asymmetric actors have become quite adept in using smart power tactics and tools, from providing basic social services to launching sophisticated cyber attacks. However, as the U.S. and allies build their smart power momentum, asymmetric actors will proactively adapt their capabilities and plans to counter changes in U.S. and global security. It is imperative not to let them get one step ahead.

Realism, patience, and persistence are essential to America's success – No one knows how long it will take to develop and effectively employ the smart power needed to sustain America's national security in the twenty-first century, and beyond. America faces a great perceptual asymmetry when compared to its asymmetric adversaries: that is, the perception of how long great tasks of enduring value should take. How long should these great tasks retain our interest? While our adversaries see today's struggles as having roots deep in the past and continuing far into the future, America and her institutions have a much shorter frame of reference.

America faces a persistence gap and needs to develop institutional methods that address the indisputable fact that making progress in soft power will take a long time.

The work is well begun, but it has just begun.

"One of the most important lessons of the wars in Iraq and Afghanistan is that military success is not sufficient to win: economic development, institution-building and the rule of law, promoting internal reconciliation, good governance, providing basic services to the people, training and equipping indigenous military and police forces, strategic communications, and more – these, along with security, are essential ingredients for long-term success."

– Secretary of Defense Robert M. Gates

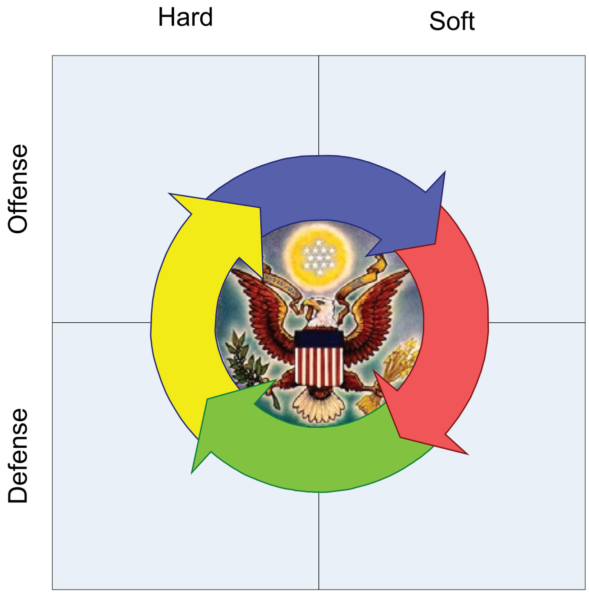
1 Introduction

Prior to the fall of the Soviet Union, most national security challenges facing the United States were posed by nation-states, wielding conventional military power. Notwithstanding technological evolution and the attendant changes in battlespaces and weaponry, the Cold War global security environment generally reflected a strict adherence to traditional, predictable, and symmetrical warfare between nations. Some of these rules of Cold War engagement were codified in the Third Geneva Convention, adopted in 1949 when distinctions between conventional combatants and civilians were more easily drawn than they are today.[2]

During the Cold War era, the United States began to understand that there were limits on the efficacy of military force alone in achieving non-military objectives. Since the fall of the Soviet Union – particularly after the September 11th attacks – it has become increasingly clear that the proliferation of irregular actors who migrate fluidly between civilian communities and heavily armed terrorist organizations poses particularly daunting security challenges. Some of these challenges include difficulties in identifying the legal status of adversaries, as well as the availability of weapons of mass destruction. Novel, unconventional threats and enemies can be anticipated and overcome only through the multidimensional and flexible application of *smart power*.

The United States must restructure its national security apparatus to align hard and soft power resources to meet the critical issues of the twenty-first century, from Islamic extremism, drug trafficking, and nuclear proliferation to economic recession, global poverty, impending natural disasters, and other asymmetric threats. It has also become increasingly clear that these threats will not dissipate in the future. We cannot underestimate the effectiveness of the extremists' efforts. Ideologies from which extremist Islam is driven have taken hold around the world. From the early writings of Sayyid Qutb, to the Iranian Revolution, and to sleeper cells in Western

[2] Scott Stedjan, CACI-USNI Symposium comments.



A comprehensive and integrated response strategy to counter asymmetric threats requires the use of the entire spectrum of America's instruments of power and influence. Graphic courtesy of CACI.

nations, we can see the fanaticism has only gotten stronger.[3] The collective and coordinated strengths of government institutions, the private sector, and American cultural reach must be integrated to counter the full range of asymmetric threats the nation faces today.

The diversity of threats requires a response strategy that spans the "entire spectrum" of America's instruments of influence, from the "hardest of hard [power]"[4] to the softest of soft. The range of these new threats includes "violent extremist movements, the spread of weapons of mass destruction, rising powers with sophisticated weapons, failed or failing states, and increasing encroachment across the global commons (air, sea, space, and cyberspace)."[5] The current global economic downturn has only heightened the complexity of these security challenges. Therefore, these challenges must be assessed and confronted within the particular context in which they emerge, allowing the political, military, social, and cultural conditions to define the threat and the circumstances under which it can be eliminated.[6] In addressing these new challenges, the United States must wield smart power with the flexibility, adaptability, and innovation required to defeat adversaries, while setting benchmarks for efficacy in national defense and adhering to its principles.

In her Senate confirmation hearing in January 2009, Secretary of State Hillary Rodham Clinton described the need for a smart power approach to address these multidimensional challenges that affect the United States and its allies abroad. She described two groups of non-state actors – one that parallels U.S. efforts and works tirelessly to fight poverty, improve health, and expand education opportunities in the poorest parts of the world; and another that participates in terrorism, drug trafficking, and human smuggling activities with no regard for human suffering and the loss of innocent lives across the globe. According to Secretary Clinton, "We must use what has been called 'smart power': the full range of tools at our disposal – diplomatic, economic, military, political, legal, and cultural" – to develop a coherent, integrated national strategy to meet the asymmetric threats the nation faces today.[7]

This sentiment has been echoed by Defense Secretary Robert M. Gates, who has called repeatedly for the United States to commit more money and resources to soft power tools – namely, diplomacy, economic assistance, and strategic communications – because the military alone cannot defend U.S. interests.[8]

> ***"We must use what has been called 'smart power': the full range of tools at our disposal – diplomatic, economic, military, political, legal, and cultural – picking the right tool, or combination of tools, for each situation."***
>
> *– Secretary of State Hillary Rodham Clinton*

[3] Jack London, CACI-USNI Symposium comments.
[4] Hon. Michael Chertoff, CACI-USNI Symposium comments.
[5] U.S. Department of Defense, *2010 QDR Terms of Reference Fact Sheet*, April 29, 2009, http://www.defenselink.mil/news/d20090429qdr.pdf.
[6] Roger Barnett, CACI-USNI Symposium comments.
[7] Statement of Senator Hillary Rodham Clinton, Nominee for Secretary of State, Senate Foreign Relations Committee, January 13, 2009, http://foreign.senate.gov/testimony/2009/ClintonTestimony090113a.pdf.
[8] Joseph Nye, Jr., "The U.S. Can Reclaim 'Smart Power,' " *Los Angeles Times*, January 21, 2009, http://belfercenter.ksg.harvard.edu/publication/18782/us_can_reclaim_smart_power.html.

While the Department of Defense (DoD) is currently the best resourced arm of the U.S. government, there are limits to what hard power can achieve on its own. The most highly trained forces and innovative weapons systems are not intended to perform soft power activities like promoting democracy, ensuring human rights, and fostering the development of civil society. And while the military has been asked to conduct operations of a more diplomatic and humanitarian nature, the Department of State, other civilian agencies, and NGOs are skilled in these areas and focused on these efforts. Succeeding against terrorism and other asymmetric threats means finding a new central premise for U.S. foreign policy that augments the "war on terror" with a commitment to provide for the global good through an integrated hard and soft power strategy.[9]

To contribute to the national discourse as the U.S. government develops this new strategy, CACI International Inc (CACI), along with the National Defense University (NDU, Symposium One) and the U.S. Naval Institute (USNI, Symposia Two and Three), organized and presented a series of symposia to examine and define the asymmetric threat; to encourage a rich dialogue on the key elements of a revised national security strategy; and to develop an understanding and framework for effectively implementing smart power – the balanced synthesis of hard and soft power.[10] The symposium *Employing Smart Power*, co-sponsored by CACI and USNI on March 24, 2009, addressed the offensive and defensive components of soft power and explored how the concept of smart power could be implemented in a highly net-centric world, in both the human and technological sense. While the nation's ability to respond militarily will likely remain dominant, the United States must be aggressive and innovative in seeking opportunities to apply both hard and soft instruments of power in a balanced, harmonized, agile fashion.

This report presents Symposium Three's results and recommendations. Symposium participants discussed the challenges inherent in integrating hard and soft power, finding the right mix of the two, and aligning governmental and non-governmental resources and structures to achieve smart power. It was also agreed that, to be truly effective, soft power should be brought to bear long before and after hard power.

A U.S. Army soldier delivers school supplies as part of a humanitarian assistance program in Afghanistan. Such efforts are vital to the successful application of smart power in countering terrorism. Photo courtesy of U.S. Army.

[9] Ibid.

[10] The findings of Symposium One and Symposium Two are summarized in Appendix A: Synopses of Prior Asymmetric Threat Symposia. The published reports on these symposia can be found at http://www.asymmetricthreat.net.

2 Application of Soft Power Against Asymmetric Threats

It is clear that America is facing *networks* of adversaries who already understand the benefits of, and are using, smart power strategies against the West. The U.S. and other nations have responded with military power, but have seen only limited and short-term success. Conventional hard power is generally ill-suited for asymmetric threats and challenges, such as control of networks for exchange, debt leverage, aid delivery, travel and migration, healthcare delivery, education, telecommunications, information collection and data analysis, multinational cooperation, and cybersecurity.

> ***"In the struggle we are in now and in the twenty-first century, I don't think we are in a position to leave any of these tools in the tool box. I think we have got to get all of those tools deployed and effective."***
>
> *– Former Secretary of Homeland Security Michael Chertoff*

As concluded in the second symposium, the strategic and proactive application of soft power has the potential to thwart these kinds of asymmetric threats over the long run.

Soft power, as coined by Joseph Nye, describes "the ability to shape the preferences of others" and "get others to want the outcomes you want."[11]

There is an important distinction between offensive and defensive projections of power. The distinction is well understood in hard power discussions, but is undeveloped in soft power discussions. *Offensive* soft power deals with shaping preferences and outcomes, while *defensive* soft power deals with diminishing the hard and soft power capabilities of adversaries. Understanding both the offensive and defensive projections of soft power is a prerequisite to improving their effectiveness and application to a comprehensive smart power strategy.

An Indonesian family displays their U.S. flags during a medical and dental support project conducted by the Military Sealift Command hospital ship USNS Mercy *to provide humanitarian and civic assistance.*
Photo courtesy of U.S. Navy.

2.1 Offensive Dimensions of Soft Power

Offensive soft power tools and strategies are not new to American policies. But the U.S. and others must rethink the battlefield as adversaries increase their soft power capabilities. Offensive soft power under Nye's familiar definition entails exerting influence over others by means other than force. But more than that, it is the collective result of positive activities that attracts populations to the U.S. Offensive soft power activities seek to increase the legitimacy and credibility of ideas, goals, policies, and even people. Winning the battle of credibility can also diminish or undermine an adversary's position in areas of potential conflict.

2.1.1 Offensive Soft Power Used by Asymmetric Adversaries

The violent and pervasive images of terrorism in the media typically show the terrorists' use of hard power

[11] Joseph S. Nye, Jr., "The Benefits of Soft Power," *Harvard Business School Working Knowledge for Business Leaders*, August 8, 2004, http://hbswk.hbs.edu/archive/4290.html.

"Soft power is not merely the same as influence … And soft power is more than just persuasion or the ability to move people by argument, though that is an important part of it. It is also the ability to attract, and attraction often leads to acquiescence. Simply put, in behavioral terms, soft power is attractive power. Soft power resources are the assets that produce such attraction."

– Joseph S. Nye

instruments. But there is a less-reported and understood image of soft power in the hands of terrorists that is every bit as threatening.

Terrorist organizations, certainly including Hamas, Hezbollah, and Al-Qaeda, recognize the critical importance of soft power. They have adopted a strategy of dominating the security and service sectors in contested regions, thereby limiting America's effectiveness in exploiting those sectors.[12] Terrorist groups have proven rather adept at providing social and welfare services. They fill a void that the local governments have not filled, supplying health, education, and social and welfare services to vulnerable populations. Recipients of these services, therefore, do not necessarily perceive these groups as terrorist organizations, as the U.S. and other foreign governments do.[13]

For example, education, health, or welfare services distributed through Hamas or by a Hamas-related entity cultivate a reliance on, and a loyalty to, an organization that the U.S. is trying to counter. There is a significant leverage for Hamas because positive feelings are engendered not only in the person receiving the benefit, but also in their immediate and extended family and throughout the whole community. When educational services are provided, there is also the potential to convert the student (and family) to Hamas's cause. Through this strategy, organizations like Hezbollah and Hamas have become the *de facto* governments in large areas of the Eastern Mediterranean. Operating within that sphere of influence, where terrorist groups are perceived as effective providers and compassionate humanitarians, constitutes a problem for the United States that is also recognized by public and private non-governmental organizations.[14]

A U.S. Army soldier reads a book to Iraqi girls during a humanitarian mission in Tikrit. Photo courtesy of U.S. Army.

Another aspect of terrorist organizations' effective use of offensive soft power is the employment of strategic communications against American interests. Terrorists use the media, modern methods of communication, and public relations to disseminate compelling messages to sympathetic audiences, recruit new followers, intimidate opponents, and conduct disinformation campaigns. Their sophisticated techniques include segmenting audiences and tailoring appropriate, timely messages.[15]

Furthermore, the reach of terrorist propaganda into the United States and other countries, typically via the Internet, reveals a weakness that is not easily remedied. This ability is a product of the openness of target (Western) societies, the extraordinary openness of Internet culture, and access to modern information and communications technologies.[16]

The ability of terrorists to project their power through normal defenses comes from their skill in leveraging asymmetric technologies, many of which are no more than

[12] Major General Mick Kicklighter, CACI-USNI Symposium comments.

[13] Mark "Chip" Poncy, CACI-USNI Symposium comments.

[14] Stedjan, op.cit.

[15] Hon. Dell Dailey, CACI-USNI Symposium comments.

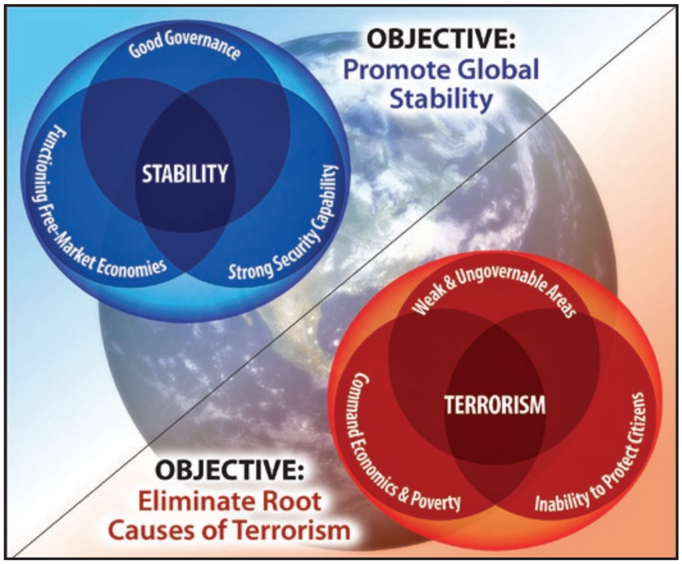
[16] General Larry Welch, CACI-USNI Symposium comments.

the ordinary tools of modern life, from networked personal computers to jet aircraft. Advanced communications technologies and marketing techniques are key examples of smart power strategies used by terrorists against the West. These are strategies that effectively coordinate their soft power and hard power arsenals.

2.1.2 American Use of Offensive Soft Power

While there are promising examples of American use of offensive soft power, the application of this capability is uneven at best. In Iraq and Afghanistan, Provincial Reconstruction Teams (PRTs) have demonstrated the efficacy of initiatives to develop sustainable and transparent governance capabilities, improve security and the rule of law, and promote political and economic development. All of these efforts are in furtherance of what people universally seek: security for their families, access to healthcare, adequate nutrition, and education.[17] This kind of American participation strengthens not only regional and local governmental institutions in volatile areas, but also America's soft power with vulnerable populations.

To counter violent extremism through use of strategic communications, the State Department placed a specialized team to support Regional Strategic Initiatives. There are also innovative soft power activities and programs aimed at shifting the perceptions of target audiences, undermining the terrorists' image, delegitimizing extremist ideology, and diminishing the support provided to extremists. One example of success in this area is the U.S. Ambassadors Fund for Cultural Preservation, which has provided over $13 million since 2001 to cultural heritage preservation projects in developing countries.[18]


OBJECTIVE:
Promote Global Stability
Good Governance
Functioning Free-Market Economies
Strong Security Capability
STABILITY
Weak & Ungovernable Areas
Command Economics & Poverty
Inability to Protect Citizens
TERRORISM
OBJECTIVE:
Eliminate Root Causes of Terrorism

Soft power tools focused on governance, security, and economics work to promote global stability while eliminating opportunities for terrorism to develop. Graphic courtesy of CACI.

Nevertheless, there is much room for improvement. Not only is it important to develop good strategic communications objectives, but it is imperative that words *and* deeds are coordinated in asymmetric conflicts. Actions are as important a communicator as words, and America's adversaries all too frequently watch what the U.S. does and not what it says. This is a complex and dynamic concern for key decision-makers, as changes in actions can signal more intent than is always realized.

While the U.S. government, as a whole, does a good job of defining its strategic communications objectives, it does not follow through in ways that achieve success in the market.[19] For instance, research by U.S. government agencies in Afghanistan has shown that over 90 percent of the population rejects the Taliban. Meanwhile, Afghanis' primary challenges have been the provision of basic necessities, including food, water, and education. These problems on the ground ran counter to some U.S. leaders' conceptual framework for the nature of the struggle and the real threat in Afghanistan. Policymakers learned that accurate situation assessments were essential to properly frame objectives, develop programs, and formulate and deliver messages with a real chance of success.

Program implementation is yet another challenge in applying soft power. The U.S. also built schools in Afghanistan in an attempt to win over the hearts and minds of Afghanis. However, they did so without a means for providing teachers to staff the schools, or books from which to teach. Today these schools in Afghanistan sit empty because American planners failed to think holistically about what was actually needed by the civilian population. NGOs could have supplied valuable information that would have improved the quality of these plans, but they were

[17] Kicklighter, op.cit.

[18] Ibid. and http://exchanges.state.gov/afcp/.

[19] Bruce Sherman, CACI-USNI Symposium comments.

not consulted.[20] Therefore, in order to become as effective as hard power, smart power strategies must be developed with a full life-cycle approach. Had such an approach been taken, these schools could have become a success story for smart power application.

Much remains to be done in refining how America applies offensive soft power and how it communicates that positive application to critical audiences. The message as well as the underlying cross-government communications required to disseminate it are essential components of offensive soft power.[21]

2.2 Defensive Dimensions of Soft Power

Soft power is typically viewed as an offensive tool in American policy. That belief will only limit American security initiatives. Defensive soft power is the least understood aspect of soft power, yet offers great potential in protecting and promoting American security interests. Defensive soft power diminishes or blocks an adversary's soft and/or hard power capabilities by promoting continued loyalty of a population to an individual, state, or organization. As with defensive hard power, defensive soft power is also intended to thwart dangers, and to prevent and defend against attack. While defensive hard power seeks to prevent military incursions of adversarial forces, defensive soft power serves to keep at bay adversarial preferences, objectives, and modes of behavior.

U.S. Ambassador-at-Large for Global Women's Issues Melanne Verveer meets with Afghan grassroots women's organizations, women leaders, and female election candidates. By encouraging improved governance, we help the Afghan government grow its defensive soft power. Photo courtesy of U.S. Department of State.

Understood this way, defensive soft power seeks to achieve either or both of two related and complementary functions: *immunization* and *strengthening*. As an agent of immunization, defensive soft power reduces a population's inclination to be influenced by adversaries, thus weakening their ability to attract people to their cause. As a strengthening agent, defensive soft power increases a group's ability to resist an adversary's use of hard or soft power.

Immunization – Historically, immunizing is exemplified by the loyalty of first-generation Japanese-Americans (Nisei) during World War II. Notwithstanding the impact of Executive Order 9066, under which thousands of Nisei were sent to internment camps during the war, the vast majority of Nisei remained loyal to their adopted country. A contemporary example is the success with which jihadist movements have recruited Muslims from Western Europe compared to their difficulties making inroads with American Muslims. This has been attributed to the more complete acceptance by, and integration of, Muslims into American society.[22]

Strengthening – Examples of increasing a population's ability to resist an adversary also can be drawn from World War II. During this conflict, resistance movements emerged in every country occupied by Nazi Germany. (Germany itself also had an anti-Nazi movement, while the unoccupied British prepared resistance groups in the event of a German invasion.) Resistance efforts included non-cooperation, disinformation and propaganda, the protection of prisoners of war, demonstrations, strikes, sabotage, espionage, and, in some cases, warfare and the recapturing of towns.[23] Contemporary strengthening examples include the Iraqi Awakening movements, where tribal leaders have formed security coalitions. The common thread in these examples is the principle of the defense of "home and hearth." As such, it may not be directly wielded by external actors, such as the United States.

[20] Stedjan, op.cit.
[21] Ibid.
[22] Matthew Levitt, "Radicalization: Made in the USA?" Homeland Security Policy Institute Commentary 03, June 2, 2009, http://www.gwumc.edu/hspi/Commentary_radicalizationintheusa.htm#2.
[23] The establishment of the Office of Strategic Services (the CIA's predecessor) was in part to support European resistance groups.

2.2.1 Sources of Defensive Soft Power

In many respects, defensive soft power emerges as the by-product of a good government that provides "the ability to speak your mind and have a say in how you are governed; confidence in the rule of law and the equal administration of justice; government that is transparent and doesn't steal from the people; the freedom to live as you choose."[24] When a government functions well and meets the needs of the people through good governance, the government increases its offensive *and* defensive soft power, at home and around the world.

The focus on building the capacity of the state is as essential to defeating asymmetrical threats as the services that are provided. When the state is unable to provide basic security and essential services to the population, the loyalty of civilian populations will stray to other actors better able to supply what they need.[25]

2.2.2 Defensive Soft Power Challenges

2.2.2.1 Failed and Failing States

The importance of soft power in failing and failed states is considerable. Failed and failing states, by their very nature, are those that no longer possess the domestic defensive hard and soft power to maintain authority over their citizenry. As a result, such regions offer asymmetrical actors opportunities to establish themselves as powers that challenge the authority and legitimacy of recognized national governments. Through the application of smart power approaches, they have, in many respects, supplanted the normal roles of government and co-opted its legitimate authority. They have done so not to fill a void, but to advance their own causes.

In general, the needs of people living in developing societies are poorly met by governments that are lacking mature processes and institutions and that are struggling to apply too few assets to too many problems. In these conditions, it is easy for groups hostile to democratic interests and stability to achieve success in capturing the minds and hearts of many disadvantaged citizens by supplying services that are normally the province of government, such as water, education, and healthcare.

Afghan men stack bags of wheat donated by the U.S. Agency for International Development (USAID). Photo courtesy of USAID.

Discovering the identities and activities of violent extremists is also particularly challenging in failed and failing states due to the networked business model within which terrorists are masked. Terrorist organizations operate as unsuspected agents of NGOs, who subsequently and unknowingly develop dependencies and reliance on the terror groups.[26]

2.2.2.2 Logistics and Asymmetric Opportunism

The United States and its allies have found it hard to achieve their objectives because of organizational difficulties that impede rapid responses to immediate humanitarian needs. These capability shortfalls provide a window of opportunity to those whose goals include the minimization or negation of U.S. influence. By rapidly supplanting American humanitarian efforts, they obtain greater levels of influence.

Terrorists also co-opt Western soft power assets for their own purposes, aggrandizing their own soft power at the expense of the humanitarian and counterterrorism efforts.[27] In some cases, adversaries hijack humanitarian

[24] President Barack H. Obama, "Remarks by the President on a New Beginning," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09/.
[25] Stedjan, op.cit.
[26] Poncy, op.cit.
[27] Stedjan, op.cit.

> ***"It is important [to] focus on trying to make those countries more responsive to their people in terms of governance, in terms of security, and in terms of development."***
>
> *– Charles "Fritz" Weden*

assets en route to the needy, either in opposition to the U.S., to profit from sales of the goods, or to distribute the stolen goods as charity.

In contested regions, terrorist-sponsored charities also insert themselves between Western NGOs and the populations they wish to serve. NGOs recognize this situation and would avoid funding terrorists given the opportunity. But when terrorists control distribution networks, key resources, and access points, NGOs are limited in their ability to identify and avoid funding terrorist-sponsored organizations.[28] One of the challenges facing America, then, is to find a way to support meritorious social causes and organizations without unknowingly and indirectly supporting terrorism. This is a particular challenge in failed and weak states. Part of the answer may be achieved by deploying information systems that synthesize public, not-for-profit, and private information, enabling informed funding decisions in the pursuit of the most worthy humanitarian causes.

2.2.2.3 Strategic Communications

In Afghanistan, adversaries have effectively used soft power instruments to force the U.S. and its allies into a defensive posture, and in doing so have rendered allied hard power relatively ineffective.[29] A prime example is how the Taliban has effectively driven the news agenda in Afghanistan. By beating American and Western media operations to the punch in getting their information to news agencies in Kabul, the Taliban can spin events to their advantage, reporting to all of Afghanistan and the world, for example, claims that American forces have killed innocent civilians. As a result, the American use of hard power becomes more difficult. The net effect has been that DoD has significantly increased its emphasis on all aspects of soft power, including its use of strategic communications.[30]

U.S. Air Force crew members load informational leaflets into a dispenser to be dropped by plane into southern Afghanistan, part of a strategic communications action to gain support for the Afghan national government. Photo courtesy of U.S. Air Force.

2.2.3 Exploiting Defensive Soft Power

The issues and potential benefits associated with exploiting defensive soft power are considerable. Defensive soft power applies to actions that assist friendly and partner countries to increase *their* soft power. This should not be equated to a nation-building strategy. America, however, can be a participant in developing the potential for nations to be built by their citizens.[31]

Through a variety of economic, social development, and governance efforts, the United States can help strengthen developing states.[32] Capacity-building can not only improve developing governments' ability to provide security and basic needs (including natural disaster response), but it can also reduce the likelihood that insurgencies will find a sympathetic audience within large segments of national populations.

[28] Ibid.
[29] Sherman, op.cit. This is roughly equivalent to the use of hard power capabilities for defense, such as in an anti-missile defense.
[30] Ibid.
[31] General Bryan Brown, CACI-USNI Symposium comments.
[32] Charles "Fritz" Weden, CACI-USNI Symposium comments.

Yet the exploitation of defensive soft power also creates competition between the radicalization and counter-radicalization of populations. Insurgents and other forces of radicalization will try to enlist the disaffected and desperate with "seventy dollars and a mobile phone," while counter-radicalization forces try to provide "opportunities for education and jobs to young men."[33]

Internationally, counter-radicalization is an area of defensive soft power that will require the close cooperation of all of America's institutions: public, quasi-public, and private. [34] The U.S. government is in a delicate position in dealing with the issue of counter-radicalization in a credible fashion. In fact, there are some legal questions concerning First Amendment freedoms that may determine just how active the government can be in counter-radicalization.[35]

In the international arena, the State Department's Regional Strategic Initiative (RSI) is a flexible network of coordinated country teams designed to address the challenges of terrorism. The RSI is designed to develop common regional approaches that lessen or limit the gaps between and within the national legal systems where asymmetrical actors can most easily maneuver.

RSI uses smart power, working with American ambassadors and interagency representatives in key terrorist theaters of operation, to collectively assess the threat, pool resources, devise collaborative strategies, and make policy recommendations to Washington and the host states. RSI strategy groups have now been held in eight regions of the world: Southeast Asia, Iraq and its neighbors, the Eastern Mediterranean, the Western Mediterranean, East Africa, trans-Sahara, South Asia, and South America.[36]

The successful exploitation of defensive soft power requires multifaceted, long-term approaches. Both international and domestic efforts need to be networked, bottom up, and inherently localized to the needs of each community.[37] They must also be combined with capacity-building initiatives to ensure lasting results.

2.3 The Rule of Law in Soft Power

2.3.1 As a Foundation for Legitimacy

In a global security environment increasingly characterized by threats from lawless non-state actors, it is perhaps paradoxical that the rule of law remains a linchpin of America's national security strategy, just as it was during the relatively more predictable Cold War era. While the law restricts the capacity and flexibility to wield power, it can serve as a formidable tool in preserving peace and stability.[38] Although legal rules may constrain the use of force or the freedom to act under certain conditions, law ultimately provides a foundation of legitimacy and structure for both domestic and foreign activities.[39] Defense Secretary Robert Gates noted that "[one] of the most important lessons of the wars in Iraq and Afghanistan" was that the rule of law is an "essential ingredien[t] for success" in those regions.[40]

Establishing effective law enforcement in Iraq is essential to the country's future. Here, an Iraqi Police Academy instructor straightens the beret of a recruit before a graduation ceremony. Photo courtesy of U.S. Army.

[33] Sarah Childress, "Somali Insurgency Grows, Roiling President's Peace Effort," *Wall Street Journal*, May 28, 2009, http://online.wsj.com/article/SB124346144044959953.html.
[34] Spencer S. Hsu, "Obama Integrates Security Councils, Adds New Offices," *Washington Post*, May 27, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html.
[35] Chertoff, op.cit.
[36] Ibid.
[37] Dailey, op.cit.
[38] Barnett, op.cit.
[39] Ibid.
[40] Secretary Robert M. Gates, Landon Lecture, Kansas State University, November 26, 2007, http://www.defenselink.mil/speeches/speech.aspx?speechid=1199.

By providing a legitimate mechanism for change through responsive government institutions, the rule of law minimizes the need or incentive for individuals to seek assistance and redress from terrorist and other extralegal organizations with interests that are antithetical to peace and stability.

2.3.2 As a Counterterrorism Tool

Solid domestic and international legal frameworks are essential underpinnings and tools for individual nations in the broader international community as they fight against terrorism.[41] For example, the rule of law can serve as an invaluable soft power tool in combating the threat to global and national security posed by terrorist financing networks and activities. The Treasury Department's Office of Terrorism and Financial Intelligence was created for just this reason, to combat the illicit financing of terrorist institutions.[42]

Law enables U.S. government authorities to gather financial information to discover the sources and methods of financing terrorism. The law can also facilitate a broader strategy and specific policies to combat a range of terrorist threats supported by illegal financing, such as money laundering and organized criminal activities. Further, through international and domestic law, such as the International Emergency Economic Powers Act, assets may be frozen and seized to thwart terrorist financing and related activities.

2.4 Soft Power and the Competition to Govern

America is fighting not only a battle of ideas, but also a contest over who can most effectively meet the governance needs of people around the world. This is especially true in failed or failing regimes, but can also be the case in regions with more stable governments.

Competition between state and non-state forces has taken on new dimensions, particularly for domination in security and the delivery of social services.[43] If the current government is unable to provide safety and services, the population will have little choice but to turn to a provider who can deliver those things expected of their government.[44]

Additionally, if the national government and international community do not offer the possibility of economic development based on free enterprise rather than on criminal activity, there will be no shortage of other governance competitors offering alternative financial models based on either criminality or Hugo Chavez's form of state-run enterprises.[45]

In this new paradigm, air dominance or information dominance may be trumped by social service dominance. Failure to adequately and effectively pursue and develop soft power can contribute, ultimately, to the replacement of one government by another.

As consumers of governance services, populations will look to effective competitors to meet their needs. In the war of ideas, it is clear that America must be as effective in the governance markets as it is in commercial markets.

Hezbollah volunteers fill food trays with rice before delivering them to refugees in Beirut. Hezbollah runs a sophisticated network of schools, clinics, and social services deeply rooted in the Shiite Muslim community. Photo courtesy of AP Photo/Hussein Malla.

[41] Dailey, op.cit.
[42] Poncy, op.cit.
[43] Hon. James Gilmore, CACI-USNI Symposium comments.
[44] Stedjan, op.cit.
[45] Chertoff, op.cit.

3 Smart Power – From Theory to Practice

Full, active, and flexible integration of the diverse sources of national power is the essence of smart power. A combined hard and soft power strategy allows nations to best secure themselves against continuously changing and progressively more dangerous asymmetric threats. Yet there is a great challenge in envisaging and executing a transition from *theoretical* smart power to *practical* smart power.[46]

While many of the concepts associated with smart power appear fairly simple as ideas, they become much more complicated when an attempt is made to apply them in real-world circumstances. That is particularly true when operating in the dynamic interagency and international environment.[47] General James Jones, the National Security Advisor, recently described the scope of the change that these environments require: "We must understand the terms 'national security' and 'international security' are no longer limited to the ministries of defense and foreign ministries; in fact, it encompasses the economic aspects of our societies. It encompasses energy. It encompasses new threats, asymmetric threats involving proliferation, involving the illegal shipment of arms and narco-terrorism, and the like."[48]

Developing a smart power-based strategy will require the development of wholly new capabilities and the effective synchronization of existing capabilities to counter a rapidly changing threat environment. At the end of the Cold War, many successful smart power solutions were abandoned as expensive and irrelevant to a presumed emerging era of peaceful competition. It has become evident, however, that many of those capabilities not only needed to be retained (such as those relating to strategic communications and humanitarian assistance), but also need to evolve.

A U.S. Army soldier hands out school supplies to children after they've received medical services during a humanitarian assistance mission in Afghanistan's Kapisa Province. Photo courtesy of U.S. Army.

Critical to exposing the wider range of smart power instruments available to the United States is determining how and when the two types of power are balanced, integrated, and synchronized between the major U.S. government departments and other national institutions to counter any given asymmetric threat.

Leaders charged with the application of the diverse elements of American national power are now gravitating toward integrated smart power solutions. But the effective integration of smart power resources and approaches must also be characterized by the kind of empowerment that grants individual actors freedom of action, and permits them the speed and agility to respond with hard or soft power, or more often, with an effective combination of both. These responses must conform to a strategy while remaining unencumbered by the shackles of layered bureaucracy.

While the U.S. has the capabilities to develop a smart power-based national security strategy, America's leaders and citizens must now rise to the challenges of innovation and trust that such a strategy requires. As USNI Chief Executive Officer Thomas L. Wilkerson has said, "We have reached a stage where we are determining in the twenty-first century whether we are all going to be victims or whether we are all to be activists, accountable for our actions. That is not a small thing, and it has directly to do with our ability to use the full dimensions of national power."[49]

[46] Major General Thomas Wilkerson, CACI-USNI Symposium comments.
[47] Poncy, op.cit.
[48] James Jones, "Remarks by National Security Adviser at 45th Munich Conference on Security Policy - Council on Foreign Relations," February 8, 2009, http://www.cfr.org/publication/18515/.
[49] Wilkerson, op.cit.

The U.S. military regularly delivers USAID emergency relief supplies worldwide. Photo courtesy of USAID.

3.1 Integrating Soft Power With Hard Power

Full integration of hard and soft power requires the integration of not only the tools each actor brings to the table, but also budgetary flexibility, adaptability of organizational cultures, and empowerment. Practitioners of soft and hard power are growing in their ability to work together, but their institutions and institutional stakeholders are not nearly so progressive.

Traditional government approaches will also often be counterproductive. We cannot expect trained and deployable personnel from Defense and State to go in and train a Ministry of Health; that has to be done by people who have skills coming out of Health and Human Services. Neither can they deploy to train the staff of a Ministry of Finance; that takes skills coming out of Treasury.[50]

Concurrent to meeting that challenge, the resources and authorities of government agencies must be aligned. The U.S. government has a vast array of ongoing and simultaneous capabilities and actions. However, it is not as good at leveraging the various moving parts, the expertise, and the current authorities addressing the national security challenges. Yet this is exactly what needs to be done.[51]

The solution is not the creation of a smart power hierarchy, but rather for integrative, networked efforts with needed capabilities outsourced to those within the smart power network who can best apply those capabilities. Networked smart power is a direct analog of globalized business processes – processes which could be used to describe the manufacture of any modern product in the global economy.[52] It is not a top-down process but rather a bottom-up process, which will often be more difficult and time-consuming to put into place, and will require enhanced sensitivity.

Terrorist groups have learned the benefits of networking and employed them to their advantage. In many ways, September 11th was a classic demonstration of this kind of outsourced, networked warfare. The original planning took place in South Asia; the terrorists were trained and recruited, in part, in Europe; the financing came from the Middle East; and the execution occurred in the U.S. It did not depend on a government to act, nor did it require a defense industrial base.[53] The 2008 Mumbai attacks also showed that networked terrorist operations are not exclusive to large-scale threats.

The most effective practitioners of smart power will be states and non-state actors with the most connections – those who are able to be the global center of the agenda and unlock innovative and sustainable growth. Control of the networks for exchange, debt leverage, aid delivery, travel and migration, healthcare delivery, education, telecommunications, information collection and data analysis, multinational cooperation, and cyberspace becomes fundamental to the effective integration of soft and hard power.[54]

3.1.1 Balance

The increasingly asymmetric threat environment has shifted America's center of gravity away from hard power toward soft power. The U.S. has learned that it cannot solely employ hard power when its adversaries are effectively employing smart power.

Yet while responding to the recent demonstrations of the limitations of hard power and the successes of soft power, America must not neglect its hard power imperatives.[55]

[50] Levitt, op.cit.
[51] Ibid.
[52] Chertoff, op.cit.
[53] Ibid.
[54] Ibid.
[55] Barnett, op.cit.

Hard power is an essential complement to soft power, whether in a failed state, in the breakdown of society's normal structures (e.g., due to a natural disaster), or in a region in conflict. The U.S. needs to align smart power to operate across the entire spectrum of conflict.

Balancing hard and soft power within a smart power paradigm does not mean using tools and resources from each equally. Nor does balance imply that every security challenge will require both hard and soft approaches. Rather, balanced smart power is the accessibility and coordination of hard and soft resources.

During the Cold War era, America's hard power and soft power instruments essentially were deployed on independent, parallel tracks. The same was true of the Communist Bloc's instruments of hard and soft power. America's strategic nuclear forces and Voice of America broadcasts were not exercised in close coordination any more than were the Soviet strategic nuclear forces and the Bolshoi Ballet. While together the instruments of hard and soft power represented the whole of the confrontation between East and West, they were not applied holistically in any confined time and place.

Defense Secretary Robert M. Gates and Secretary of State Hillary Rodham Clinton testify during the Senate Appropriations hearing on proposed war supplemental appropriations. Photo courtesy of Scott J. Ferrell/Congressional Quarterly/Getty Images.

Today, America's asymmetrical threats require the holistic and closely coordinated application of soft and hard power in confined places and times. The responsibilities of the organizations charged with the application of soft and hard power will overlap, and the U.S. will need to move with great agility from one to the other and back again.

For example, there will need to be much closer coordination between USAID, the Export/Import Bank, and the Treasury and Commerce Departments to provide economic support and developmental assistance, and to partner with the private sector and NGOs. While the tactic of moving back and forth between nuclear bombardments and jazz concerts seems somewhat absurd, there is real utility in moving back and forth between the hard power of Special Forces operations against terrorist groups and the delivery of medical and educational services in areas where a weak national government is ineffective.

3.1.2 Agility

With technological and operational advancements, the need for agility in conventional warfare has been a given for some time. However, agility in smart power is also essential.

First, agility – as in the ability to apply smart power quickly and easily – is necessary to match asymmetric actors. Adversaries are agile because they are unhindered by competing bureaucracies and complex approval processes. Their force is designed to be adaptive, agile, and optimized to use the inherent strengths of hard and soft capabilities. The near absence of constraints on their freedom of action, coupled with access to modern technology and mobility, makes their use of smart power formidable.

The fact that terrorist business models are agile, outsourced, and distributed should be of great concern. They invalidate legitimate but weak governments, fill their capacity voids, and provide health, education, and

> ***"We need to align [the] capacity of our agencies in the U.S. government. We need to align our capacity with our capability, with our resources, with our authorities."***
>
> *– General Bryan D. Brown, USA (Ret)*

President Barack Obama meets with members of his Cabinet at the White House. Photo courtesy of the White House.

social and welfare services to vulnerable populations. Soft power practitioners, particularly humanitarian organizations, desire to use existing social and welfare networks to promote humanitarian relief in places like Gaza and Southern Lebanon without empowering the terrorist organizations that are responsible for the disasters in those parts of the world. But that becomes increasingly difficult when the terrorists control those networks, and, consequently, the recipients do not perceive them as terrorists. Hamas and Hezbollah are probably the most compelling examples, but they are certainly not the only nefarious actors that are adept in applying these approaches.

Further complicating the situation are criminal statutes that prohibit Americans from providing material support to terrorist organizations.[56] These well-intended laws prevent U.S. soft power entities from competing in many soft power venues, thereby ceding the soft power battlespace to adversaries. America's objective must be agility that exceeds that of the terrorists, who have demonstrated the capability to seamlessly blend hostile acts with the effective provision of social welfare services.

Second, agility – as in the ability to think and draw conclusions quickly – is necessary in responding to asymmetric scenarios. A flaw in U.S. soft power initiatives has been the persistent focus on "our own priorities about what we think the people need, what will win us the most hearts and minds today, not necessarily what the people want themselves or what the people have said they need."[57] An essential guiding principle to agencies working in the soft power domain is that organizations need to understand that they are not doing things *for* people: they are doing things *with* people.[58] Situational awareness will only come from understanding and agilely responding to the markets, audiences, and conditions that prevail in a given country or conflict. Without this type of agility, U.S. strategies and initiatives will have at best limited success.

Agility is needed in all applications of hard and soft power capabilities and will only come from balanced and synchronized interagency efforts. Existing institutional structures and processes will need to be transformed – even reinvented – with the right mix of capabilities, authorities, resources, and understanding.

3.1.3 Sustainability

Contemporary American society is not particularly patient, and the American political system is biased toward providing quick results to the electorate. Smart power is not synchronized to these political realities, as it takes time to devise, deploy, and achieve results.[59] No one knows how long it will take for a smart power strategy in a region or country to mature, nor is it known how long a smart power contest will last once begun. What is clear, however, is that sustained engagement will be required. America must be not only patient but persistent: engaging, re-engaging, and reinforcing. Otherwise, people and institutions will forget.[60]

Although less challenging than the changes needed to reconstitute and redeploy American smart power, governmental changes made in response to 9/11 can provide some gauge of the timescale involved. Several

[56] Poncy, op.cit.

[57] Stedjan, op.cit.

[58] Weden, op. cit.

[59] Ibid.

[60] Brown, op.cit.

years after organizational changes were initiated, the Treasury's Office of Intelligence and Analysis, the Department of Homeland Security, the National Counterterrorism Center, and the Office of the Director of National Intelligence are all only now beginning to get traction in learning how they work internally and how they work for others.[61] Also still at the early stages of the learning curve are specialized organizations that operate within interagency and international environments.[62]

While these organizations learn and grow in capability, extremists enjoy degrees of freedom in the battlespace, and are able to consolidate their successes before American smart power initiatives have a chance to yield positive results. Moreover, even when successfully deployed, the results of smart power will not be clear-cut and absolute. The asymmetrical problems and threats will not be quickly solved or defeated.

Today, metrics for smart power are unknown, undeveloped, and in many cases, unquantifiable. Cases where there have been quick, clear-cut, favorable results, perhaps as seen recently in Iraq, may be short-lived and entirely dependent on the continued application of hard power to create an environment where soft power efforts are free to safely operate. Furthermore, when the hard power element is removed, there may be a considerable degree of backsliding. In any case, even with the most successful application of soft power, the results may be far from the ideal of America's needs, wishes, and desires.

Regardless of these limitations, a smart power-based strategy is most likely the best long-term response to a diverse range of the security threats America faces. Action at all levels of government and effective leadership will be required to rally sustained support for these efforts.

3.2 Challenges to Effective Smart Power

America's security requires a twenty-first century renaissance of smart power and a recognition that national defense is a whole-government responsibility. A number of factors must be continually considered and reevaluated to achieve a situationally appropriate balance in the availability of hard and soft power resources and in their application for offensive and defensive purposes.

3.2.1 Maintaining a Flexible Balance

Developing and maintaining a flexible and balanced smart power-based security system will require all agencies of government to adapt their approaches and priorities. As actions are initiated to shift from overwhelmingly hard power structures and military-centric approaches to smart power, there is a potential that the United States will overshoot the mark.[63] There have been concerns that leaders will weaken hard power capabilities too much and too early, without getting the necessary soft power capabilities in place. Even when those soft power capabilities are fully in place, however skilled and nuanced America's exercise of smart power may become, the potential to deploy effective military forces immediately and overwhelmingly, anywhere, must be preserved.

Even the current successes in relearning counterinsurgency carry the danger of becoming an unquestioned orthodoxy, a far-reaching remedy for all of America's security challenges, and a distraction from other threats, challenges, and strategic debates.[64] The importance of preserving the credible deterrence that effective military capabilities provide is particularly evident today. In current conflicts, the effectiveness of military forces in maintaining the level of security was a prerequisite for the success of softer, smarter components of U.S. power. The United States has witnessed very clearly, in Iraq and Afghanistan, the necessity of holding in reserve and deploying, if necessary, sufficient military power to defeat potential and actual terrorist and other asymmetric

> ***"What you want to do in your plans and in your systems is build in flexibility. Flexibility is structural."***
>
> *– Roger Barnett*

[61] Levitt, op.cit.
[62] Poncy, op.cit.
[63] Barnett, op.cit.
[64] Celeste Ward, "The Pentagon's Obsession With Counterinsurgency," *Washington Post*, May 17, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051502069_pf.html.

A U.S. Air Force member teaches children dental hygiene during a humanitarian mission to Nicaragua. Photo courtesy of the Department of Defense.

threats.[65] Without this capability, it would be impossible to retain stability and security within these nations. Thus, American smart power cannot lose sight of the efficacy of using hard power to address threats posed in emerging safe havens of terrorism and in areas around the globe where governments are unwilling or unable to manage threats within their borders.[66]

In developing a comprehensive national smart power capacity, balance and synchronization are immensely important. There are concerns that integration may unduly blur the distinction between military and civilian, public and private.[67] It is important to keep certain activities within the organizations that are best able to conduct them. For example, even the most capable military should not be responsible for governance initiatives or long-term humanitarian aid. In some cases, integration can generate more problems than it solves, creating security risks for civilian agencies, independent organizations, and humanitarian actors whose effectiveness is linked to providing assistance in an independent and impartial way. That kind of independence demands non-alignment with any government or warring party, and a clear divide from the military.[68]

Finally, organizations and processes that direct smart power must be regularly reviewed and updated to bring smart power into sustained, effective, flexible reality. Concurrent with changes in presidential administrations, the DoD conducts a Quadrennial Defense Review (QDR). These reviews are forward-looking analyses that estimate future requirements and shape the Department's capabilities and strategies to deal with the current and future threat environments. For smart power to be relevant, similar reviews will need to be extended to achieve a "whole of government" security review to guide the development of smart power.

3.2.2 Rule of Law

In a nation founded on the rule of law, smart power approaches must succeed within national and international legal contexts. A challenge for America's best legal minds in the coming years is the construction of a legal foundation that provides flexibility in concerted action across America's diverse instruments of national power. There must be an appropriate legal paradigm to enable full synchronization of smart power capabilities. A prime example of the legal challenge is in information sharing, particularly in the financial sector. It has been noted that "if we are in the business of applying financial information in a way that helps us understand who the bad guys are, that financial information needs to be integrated with intelligence, with commercial information, with criminal information, [and] with regulatory information."[69] The United States, however, has yet to establish the comprehensive legal framework necessary to formalize the integration of this information. As a result, occasional successes in this area result more from the persistence of concerned agencies or officials, rather than systematic processes.

Additionally, law has the potential to serve as a valuable smart power tool in combating the asymmetric threats America faces in the air, sea, outer space, and cyberspace – the borderless "global commons" that nation-states share.

[65] Chertoff, op.cit.
[66] Ibid.
[67] Barnett, Stedjan, op.cit.
[68] Stedjan, op.cit.
[69] Poncy, op.cit.

Delegates from throughout Iraq convene for the Iraqi National Conference. Photo courtesy of James Gordon/Wikimedia Commons.

Within these areas, the law can become a critical tool, although the challenges in properly identifying, articulating, and applying legal standards are especially formidable.

Unfortunately, America's conceptualization of the cyber threat and how to counter it is lagging. While there is increasing recognition of, and institutional responses to, cyber threats, there is currently no adequate and agreed-upon language to discuss cybersecurity.

Uncompromising precision in the use of language in laws and related guidance is a critical enabler in combating new and evolving threats. Simply put, "if you can't define the problem, you can't really address it and overcome it."[70] Carefully defined terminology, for example, helps describe key threats to global and national security, most notably "violent Islamic extremism." That threat has been defined as "an ideology which has a definite world view, one that rejects toleration for any competing ideas and one that envisions an end state of political domination of at least some part of the globe through totalitarian government that would at least use the rhetoric of religion as a justification."[71] A definition reflecting this degree of thoughtfulness and care can heighten our awareness of actual and potential threats, and maintain our focus on their underlying causes and outward manifestations.

The law also can constrain the use and effectiveness of smart power tools and strategies. These limits are generally viewed as impediments on the use of force, such as rules of engagement and arms control. The legal constraints are moral as often as they are operational. Whereas the U.S. and most other nations do not target civilians or use certain kinds of weapons (e.g., chemical), terrorists feel free to do so and see such constraints as weaknesses. And so the battlefield is tilted because "the bad guys don't have any of those constraints."[72]

A solid legal domestic and international framework is, then, essential to all nations in the fight against terrorism.[73] There must be cooperation in changing and improving the international legal regime so there are no weaknesses in a networked world, where the failure to control terrorism in one country can have implications in another country.[74]

3.2.3 Organizational Roadblocks

It has been suggested that if the national apparatus for countering asymmetrical threats were measured against the standards of the Capability Maturity Model, Integrated (CMMI) for software engineering, for example, it would be clear that America works by heroism and exception, i.e., at CMMI Level 1, the lowest level.

A significant part of smart power is in developing an intelligent resource-authority allocation.[75] However, even when a department has sufficient resources, it often lacks the authority necessary to employ them effectively. Other departments have sufficient authority but lack resources. Ideas about leveraging the elements of national power tend to be shaped by proponents in terms of their parent agencies, where they come from, and what their particular authorities are in terms of offensive and defensive tools.[76]

> ***"It's wonderful to have these dialogues about integration to smart power. It's a little more difficult to say who is going to pay the bill. And right now we are in the process of looking at that very deeply."***
>
> *– Major General Thomas Wilkerson, USMC (Ret)*

[70] Chertoff, op.cit.
[71] Ibid.
[72] Barnett, op.cit.
[73] Dailey, op.cit.
[74] Chertoff, op.cit.
[75] Levitt, op.cit.
[76] Ibid.

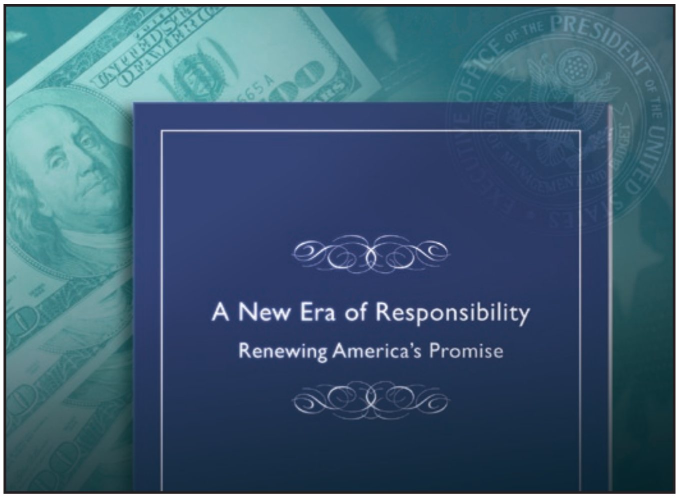
Insular departments, agencies, and non-governmental entities have, over time, developed unique cultures that are as foreign to each other as the nations in which smart power must be employed. In many of these departments, working and deploying as part of a coordinated smart power effort is not part of the corporate culture. Their organizational designs lack the needed reward systems, and deploying the right people takes them so far out of their career patterns that it becomes an overall detriment to their long-term career survival. For smart power to be employed, smart power people must have incentives and rewards to encourage participation and give smart power long-term sustainability.[77]

There also is "reorganization fatigue" to consider. Many new departments and agencies are beginning to get traction and are just now discovering how they best operate. However, there is no appetite for further reorganization and no money to do it.[78]

3.2.4 Financing Smart Power

The impact of global economics, along with the U.S. capability to influence that critical venue, holds major implications for the development of smart power. "If you study economic history, you know that power follows capital."[79] America has lost a tremendous amount of economic power in the past 16 months with the loss of several investment banks and the considerable financial resources that have been allocated to reviving the economy. While the U.S. economy has begun to show signs of recovery, it will take some time before losses are restored.

The ongoing financial crises and the consequential limits on federal financial resources will also affect the priorities in the U.S. budget well into the future. As a result, there is a manifest lack of appetite for additional reorganization in counterterrorist and related organizations.[80] When Secretary of Defense Robert Gates recently made major shifts in the defense budget to "rebalance this department's programs in order to institutionalize and enhance our capabilities to fight the wars we are in today and the scenarios we are most likely to face in the years ahead, while at the same time providing a hedge against other risks and contingencies,"[81] he immediately faced opposition. *The New York Times* editorialized that while he had "made tougher choices than his predecessor," he "did not go far enough."[82] Members of Congress with constituent defense industries voiced a different kind of opposition.



America's ability to finance smart power initiatives is critical to the success of any smart power approach. Graphic courtesy of CACI.

At the same time, while advocating smart power approaches, Secretary Gates has repeatedly stressed that he is not willing to sacrifice defense budget authority to other departments so that they can bring smart power to fruition.[83] While acknowledging that "non-military foreign-affairs programs remain disproportionately small relative to what we spend on the military and to the importance of such capabilities," and that "there is a need for a dramatic increase in spending on the civilian instruments of national security – diplomacy, strategic communications, foreign assistance, civic action, and economic reconstruction and development," he asserted that he would be "asking for yet more money for Defense," not less.[84] In a system where departments of government compete for limited resources, and the fortunes of local economies (and Congressional careers) often rise and fall on continuous streams of defense funding, the budgetary component of change can be one of the most difficult.

[77] Kicklighter, op.cit.
[78] Levitt, op.cit.
[79] Andrew Cochran, CACI-USNI Symposium comments.
[80] Levitt, op.cit.
[81] Secretary Robert M. Gates, "Defense Budget Recommendation Statement," April 6, 2009, http://www.defenselink.mil/speeches/speech.aspx?speechid=1341.
[82] "Mr. Gates's Budget," *New York Times*, April 8, 2009, http://www.nytimes.com/2009/04/08/opinion/08wed1.html.
[83] Wilkerson, op.cit.
[84] Gates, Landon Lecture, op.cit.

3.2.5 Strategic Communications

In addition to all the other asymmetries, there is also an asymmetry in perceptions. Regardless of how objective U.S. actions may be, they are seen differently through the eyes of America's adversaries. This is true in cases of strong action and no action alike. The cultural *zeitgeist* of Americans and that of asymmetric adversaries is so different that there is little understanding of our adversaries' sensibilities, and their perceptions of America's. Furthermore, it is by no means certain that more or better communications would allay these differences in perception.[85]

A long-term strategy to develop understanding and to progressively mitigate negative perceptions will require a more strategic approach to communications. This means building the expertise to execute a thoughtful, strategic campaign plan to inform a broad audience, both domestic and international, of the nature of the threat and build the case for action. As in any effective long-term strategy, education is an essential component. DoD understands this, as it spends more on training than any other government agency.[86] A critical component of strategic communications is the requirement for more education in our values as a democratic nation. This should be one of the central themes of our nation's communications campaign plan.

The U.S. Air Force deploys cyber networks for executing critical air operations worldwide. The effective use and protection of these assets is key to the evolution of smart power. Photo courtesy of U.S. Air Force.

4 The Cyber Domain and the Evolution of Smart Power

There is no better example of America's need for a timely shift to smart power than the dangerous, yet vital frontier of cyberspace. A domain that has emerged only in the last 20 years or so, cyberspace includes some of the most contested territory in the war of ideas as well as the (arguably) primary battlefields in asymmetric warfare. It is also a domain that is constantly changing, and where terminology and practices are still evolving. Equally, the roles and responsibilities within the U.S. government for dealing with the cyber domain have yet to be solidified.

Understanding the asymmetrical threats involving cyberspace and the interplay of the elements of smart power provides some of the most useful insights into the demands placed on public and private institutions, and will provide an excellent gauge of the progress in instituting and sustaining the broader national strategy to meet asymmetrical threats.

4.1 The Challenging Nature of Cyberspace

Cyberspace is a borderless "global commons" that all actors, including nation-states, share. From personal use to business platforms and military applications, the reliance on cyberspace is only accelerating. Yet the ubiquitous nature of cyberspace is what makes users so vulnerable. Unlike traditional threats that are tangible and predictable, cyber threats can have virtually any shape or source, and pose many unforeseeable dangers.

The dangers of cyber threats are heightened by the disparity between the growing dependence on reliable access and operations in cyberspace and the low cost,

> ***"You now need to deal with Microsoft and machetes at the same time."***
>
> *– Warren Phillips*

[85] London, op.cit.
[86] Warren Phillips, CACI-USNI Symposium comments.

The U.S. Air Force monitors cyber networks to maintain strategic communications worldwide. Photo courtesy of U.S. Air Force.

availability, and widespread capabilities detrimental to the dependence on cyberspace.[87] Exacerbating the threat is the low cost and pervasiveness of highly advanced information technologies, which make it impossible to focus solely on large state actors.[88] Anyone with the ability to buy, barter, steal, or borrow access to infrastructure is capable of becoming a cyber threat.

However, language to adequately describe new threats in the cyber medium has not yet been broadly agreed upon. As a result, a consensus as to what constitutes a cyber attack is not at hand.[89] This lack of a commonly accepted cyberspace vocabulary is particularly problematic because U.S. information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries and government, are being increasingly and aggressively targeted by a growing array of state and non-state actors.[90]

Because comprehensive terminology and rules for cyberspace have yet to be developed, even articulating cyberspace threats and identifying options for countering them is extremely difficult.[91] The development of a precise, detailed cyber vocabulary is the first step toward meaningful discourse about cyber threats, and the smart projection of soft and hard power necessary to counter them.

4.2 The Law and Cyberspace

America has typically faced threats coming from land, air, sea, and even outer space. Within these areas, the rule of law has been a critical tool to define and deter threats. Unlike these traditional battlefields, cyberspace remains largely unregulated. While there is a hunger for quality governance in physical space, the opposite has oddly been the case for cyberspace.[92]

It seems likely that progress in setting rules for cyberspace will come through the national security community, especially the Departments of Defense and Homeland Security.[93] However, because of the novelty of cyber threats, their rapid evolution, and the lack of agreed-upon terminology to describe them, even strategic soft and hard power planners in national security agencies do not fully understand the nature of these threats.

Applicable legal regimes may involve both national and international principles. Thus, the air above and seas adjacent to a sovereign nation may be regulated by that nation's laws, at least to certain distances, and international laws primarily apply to outer space and open seas. Although these legal frameworks are cumbersome, antiquated, and frequently ambiguous, they nevertheless provide a common legal lexicon for affected nations to use in defining issues, and a rule set with which national and international actors must comply in resolving them.

> ***"Cyberspace is not static. Cyberspace is constructed. It is dynamic. It changes constantly. It changes with human activity … There are lots of aspects of cyberspace where asymmetric threats or asymmetry is particularly important."***
>
> *– General Larry Welch, USAF (Ret)*

[87] Welch, op.cit.
[88] Chertoff, op.cit.
[89] Welch, op.cit.
[90] London, op.cit.
[91] Chertoff, op.cit.
[92] Poncy, Welch, op.cit.
[93] Welch, op.cit.

Cyberspace 101

- Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Common usage of the term also refers to the virtual environment of information and interactions between people.
- Cyberspace is pervasive – permeating land, sea, air, and space – and dynamic – constructed, but changing constantly with human activity.
- Widely accepted terminology and legal frameworks regarding cyberspace, cybersecurity, and cyber threats have yet to be established.
- National security aspects of operating in, through, and from cyberspace include the following:
  1. Constructing and sustaining cyberspace,
  2. Ensuring America's freedom of action within cyberspace,
  3. Denying adversaries the freedom of action within cyberspace, and
  4. Creating effects within cyberspace and into other domains.
- Cybersecurity is a new priority in national security and will offer insight into applying smart power overall.

Therefore, the United States must assert its leadership in encouraging cooperative international efforts to enhance the international legal regime in ways that recognize that the failure to control terrorism in one country can have implications in another.[94]

The very nature of the actors most likely to pose threats in cyberspace – "people who pride themselves on not paying attention to rules and having open architectures" – renders this challenge all the more daunting.[95] Cyberspace appears to be particularly resistant to the incorporation of a system of deterrence; the inherently amorphous nature of this environment makes it difficult to determine who should be deterred and for what cause, and how a nation-state should properly retaliate when deterrence fails.[96] As the Commander of the U.S. Northern Command recently observed, "It's harder to define what an act of war might be in the cyber world."[97]

Indeed, determining what constitutes a "threat or use of force" or "armed attack" – events that, under international law, trigger the right to self-defense – is substantially more complex when the activity in question is carried out through information or telecommunication infrastructures, rather than with conventional kinetic power. Current international legal norms, of course, were developed long before the creation of cyberspace, and legal evolution, rarely a rapid process, is particularly incremental in the international setting.

Despite these obstacles, legal rules, expressed with precision and properly applied, remain an indispensable means of imposing upon cyberspace the norms that will lend to that environment the predictability and stability upon which security depends.

4.3 Applying Smart Power to Cyber Threats

Cybersecurity has often been oversimplified as the protection of network data and systems. However, the growing number of attacks on vital financial, government,

[94] Chertoff, op.cit.
[95] Ibid.
[96] Ibid.
[97] John Kruzel, "Anticipating Threats Key to Success, NORTHCOM Commander Says," American Forces Press Service, January 29, 2009.

and military networks has made cyberterrorism a national security priority.

There are four aspects of operating within cyberspace that are important to national security: (1) constructing and sustaining cyberspace; (2) ensuring freedom of action within cyberspace (including during times of duress); (3) denying freedom of action to adversaries; and (4) creating effects within cyberspace into all domains.[98]

Yet only the first is unique to cyberspace. As has been noted, the other three are "exactly the same objectives that we have in the other domains; that is, freedom of action, including under duress; denying freedom of action to adversaries; and creating effects in, through, and from those domains. So we know a great deal about objectives in cyberspace because they are identical to our objectives anywhere else."[99] Therefore, similar to other asymmetric threats, there should be an existing inventory of smart power approaches and tools applicable to cybersecurity.

Recognizing the importance of cyberspace and the limits of existing cybersecurity resources and structures, President Barack Obama recently announced the creation of a "cyber czar" to oversee a public-private campaign to confront escalating cyber threats, and DoD recently established a new numbered Air Force headquarters, under the Air Force Space Command, that will focus on the cyber mission. The President also ordered a 60-day, comprehensive, "clean-slate" review of U.S. cybersecurity structures and policies. Noting that cyberspace "underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security," the review concluded in part that strengthening federal leadership and accountability in this area "requires clarifying the cybersecurity-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions."[100]

The government's cybersecurity plans will likely provide a timely example by which the development and implementation of a greater smart power-based national security strategy can be expected.

[98] Welch, op.cit.
[99] Ibid.

[100] *Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

AFNOC Mission
Execute AFNETOPS/CC authority to command and control the operation and defense of the AF Network
AFNetOps C2 Relationship
SIPRNET

An Air Force team updates anti-virus software for Air Force units to assist in the prevention of cyberspace hackers. These airmen will be the operators on the ground floor of the new Air Force Cyberspace Command. Photo courtesy of U.S. Air Force.

5 Toward a National Strategy to Meet Twenty-first Century Asymmetric Threats

5.1 The Current State of U.S. National Security

During the symposia series, it became clear that a successful response to the broad array of asymmetric threats would require a whole-government approach that combines traditional military power with softer elements of power, such as diplomacy, communications, law enforcement, and commerce. An integrated national security strategy would also involve leveraging partnerships with non-government entities, industry, academia, and foreign partners to diffuse asymmetric threats in the short-term and prevent long-term challenges in the future. The U.S. must utilize all resources – hard and soft, defensive and offensive – in order to be successful against dedicated, capable, and multifaceted threats.

The first two symposia concluded that:

- One U.S. government strategic process should be established that would produce an integrated national asymmetric threat strategy. This way, the U.S. could effectively communicate a unified description of the asymmetric threats and the objectives of the integrated national asymmetric threat strategy to the American public.
- This new strategy would also have to increasingly incorporate soft power. To do so, America's Cold War soft power institutions must be reinvigorated or replaced to meet today's asymmetric threats. While Congress has initiated steps to strengthen the soft power capabilities of federal government departments, more needs to be done.
- A truly integrated national security strategy will synchronize both hard and soft power appropriate for each situation, and will adjust as the particular threat evolves.

In the third symposium, a clearer picture of implementing a smart power-based national security strategy emerged:

- As part of a national security strategy, both the offensive and defensive dimensions of soft power must be exploited. Offensively, the U.S. can employ a variety of diplomatic, development, and cultural initiatives to win the "battle of credibility." Defensively, the U.S. can co-opt adversaries' hard and soft power capabilities by immunizing and strengthening against these adversaries' influence.
- America's adversaries are succeeding using smart power, and America must do the same to effectively compete. Asymmetrical actors, such as Hamas and Hezbollah, pursue smart power strategies (e.g., dominating the security and service sectors) that limit America's effectiveness in applying them.
- Today and for the foreseeable future, this competition will take place in the context of a network of interactions above the state, below the state, and through the state. It is necessary to stay ahead of, and counter the capacity of, adversaries to organize and network their capabilities. Therefore, effective smart power will be innovative and networked, as the state with the most connections will be the leading player in global security.
- Smart power strategies must be balanced, agile, and sustainable. Balance refers to the accessibility and strength of all hard and soft power resources, not an equal application of each. Agility refers to the flexible and timely response to equally agile and changing asymmetric threats. U.S. institutions and processes will need to change accordingly. Finally, both smart power capabilities and results must be designed to be sustainable, as asymmetric threats are long-term challenges.
- There will be considerable challenges in implementing smart power ideas. How can a long-term balance of hard and soft power strategies and capabilities be maintained? The (rule of) law is a potent soft power tool, but will need to be updated to enable the effective implementation of smart power strategies and intra-agency cooperation. This also relates to the reorganization of American government institutions that are not necessarily prepared to initiate and accept

such potentially large-scale changes. The shift to a smart power structure will require metrics and effective communication to the public as a long-term solution. And as a result of the continuing global financial crisis, there are questions about how these efforts will be financed.

- Cybersecurity is a new challenge that has been addressed with minimal long-term established organizational roles and responsibilities. U.S. progress in dealing with the challenges of cybersecurity is a particularly good gauge of the government's progress in meeting smart power objectives.

The significance of cyberspace and the asymmetrical threats to national security that are associated with cyberspace are of such importance that this will be the subject of the next Asymmetric Threat Symposium.

5.2 The Future of Smart Power and U.S. National Security

There is little doubt why smart power should be the driver of U.S. national and global security strategies. But while most senior U.S. leaders are responding to the strategic imperatives of American smart power, there are many questions about how smart power will work:

1. Implementation – A crucial aspect of the delivery of smart power is determining who will lead, organize, and synchronize the elements of soft and hard power across the government. Existing bodies, like the National Security Council, may provide a starting point. Whatever idea evolves must include interagency functionality and overall responsibility for making smart power work over the long run, independent of administrations.
2. Education – Various agencies have developed best practices that, in many respects, may be adopted and adapted throughout the government as smart power capabilities evolve. For instance, the Department of State has, at Secretary Clinton's direction, instituted a "Quadrennial Diplomacy and Development Review … to explore how to effectively design, fund, and implement development and foreign assistance as part of a broader foreign policy."[101] However, transition of best practices from one agency to another involves long-term alignment of resources, authorities, and corporate cultures in new and evolving ways.
3. Evaluation – Metrics will need to be developed to evaluate both short- and long-term results of smart power initiatives. These metrics must focus not only on quantitative measurement but also gauging opportunities, vulnerabilities, and successes. While literacy rates can demonstrate the effectiveness of education programs, for example, how will wider-ranging effects be identified, reported, and used?
4. Collaboration – Smart power requires working within alliances and partnerships – between agencies and departments of the U.S. government, among industry and non-governmental organizations, and with allied nations – to create a holistic approach for U.S. national security.[102] Global threats will require global efforts.
5. Anticipation – Asymmetric actors have become quite adept in using smart power tactics and tools, from providing basic social services to sophisticated cyber attacks. However, as the U.S. and allies build their smart power momentum, how will adversaries respond? While unable to match the scale and scope of

> ***"The challenges of the twenty-first century are increasingly unconventional and transnational, and therefore demand a response that effectively integrates all aspects of American power."***
>
> *– U.S. President Barack Obama*

[101] Hillary Rodham Clinton, "Foreign Policy Address at the Council on Foreign Relations," http://www.state.gov/secretary/rm/2009a/july/126071.htm.
[102] Ibid.

> American smart power capabilities, both violent and non-violent adversaries are typically more agile and responsive. Asymmetric actors will proactively adapt their capabilities and plans to changes in U.S. and global security. It will be imperative not to let them get one step ahead.

Realism, patience, and persistence are essential to America's success. Today, no one knows how long it will take to develop and effectively employ the smart power needed to sustainably achieve America's national security in the twenty-first century, and beyond. America faces a great perceptual asymmetry when compared to its asymmetric adversaries. While our adversaries see today's struggles as having roots deep in the past and continuing far into the future, America and her institutions have a much shorter frame of reference. America faces a *persistence gap*, and in planning how to apply soft power and smart power needs to develop institutional methods that address the indisputable fact that making progress in smart power will take a long time.

And the work has only just begun.

Appendix A: Synopses of Prior Asymmetric Threat Symposia

Symposium One, *Dealing With Today's Asymmetric Threat to U.S. and Global Security*, co-sponsored by CACI and the National Defense University (NDU) in May 2008, brought together thought leaders from government, industry, and academia to discuss and define asymmetric threats to U.S. and global security. Panelists and keynote speakers explored the nature of the asymmetric threat and examined U.S. capabilities and weaknesses relevant to these evolving challenges. The symposium participants focused the majority of their discussions around issues related to terrorism and Islamic extremism. However, there are myriad asymmetric threats that must be examined further in developing a strategy to meet these national security challenges. The report of the Symposium One proceedings highlighted some of these dangers – terrorism and nation-state aggression; economic decline and diminished U.S. credibility around the world; narco-terrorism and drug trafficking; nuclear proliferation; pandemic disease; insufficient natural, medical, and energy resources to meet world demand; and unpredictable actions of the disenfranchised and disadvantaged who may be swayed to support an anti-establishment or anti-U.S. agenda.

Symposium participants identified the need and made a recommendation for an "Integrated National Asymmetric Threat Strategy" that would combine traditional hard power techniques with a wide range of non-military instruments of power. This first symposium concluded that hard power alone is inadequate and that the United States must bolster strategies and applications of economic, public diplomacy, health, education, commerce, judicial, and political policies. There was a consensus among symposium participants that such policies and strategies must be integrated along with hard power to realize both the strength of America and to meet the complex asymmetric threats of the twenty-first century.

Symposium Two, *Enhancing and Applying Soft Power*, co-sponsored by CACI and the U.S. Naval Institute (USNI) in October 2008, focused on the key elements of soft power – e.g., diplomacy, healthcare, education, the economy, and rule of law – that must be incorporated into a broad-based national strategy to combat asymmetric threats. Symposium participants concurred that an integrated national strategy must include soft power elements prominently in order to be successful in meeting today's challenges. A primary objective of Symposium Two was to stimulate a dialogue that would bring not just defense and weaponry into play, but also diplomacy, cultural and educational tools, and resources. It envisioned the soft power America could wield by developing infrastructure – building roads and schools, and digging wells in places like Afghanistan – with the goal of creating opportunities for a better, more secure future.

Through focused panels and keynote addresses, it became clear that soft power is very relevant for meeting and defeating the asymmetric threats we face. Participants observed that the image of the United States has declined in recent decades and that anti-American sentiment has continued to grow worldwide, particularly in the Middle East and Asia, and even in several European countries. This is due in large part to misinformation or a lack of knowledge about U.S. diplomatic and economic support activities around the world. Panelists also noted that these activities are not, but should be, communicated internally to the American people themselves. In addition, symposium participants further discussed the current structure of government and offered ideas for rebuilding capabilities, reorganizing resources, and reprioritizing missions – similar to the Goldwater-Nichols Department of Defense Restructuring Act of 1986 – to further advance the integration and coordination of soft power with a new national security strategy.

Glossary

Asymmetric Threat – A broad and unpredictable spectrum of risks, actions, and operations conducted by state and non-state actors that can potentially undermine national and global security.

Asymmetric Warfare – Combat between two or more state or non-state actors whose relative military power, strategies, tactics, resources, and goals differ significantly.

Bioterrorism – The deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants.

Cold War – A historical period between the mid-1940s and the early 1990s characterized by a continuing state of conflict, tension, and competition, evolving out of World War II, that pit the United States and its Western allies against the Soviet Union and its satellites. While the two sides never directly fought one another, conflicts occurred through military coalitions, espionage, weapons development, invasions, propaganda, and competitive technological development, including the space race.

Counterinsurgency – Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency.

Counterterrorism – Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism.

Cybersecurity – The protection of data and systems in networks that are connected to the Internet.

Cyberterrorism – The unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives.

Diplomacy – The art and practice of conducting negotiations between representatives of groups or states and the handling of affairs without arousing hostility. Often includes the practice of promoting foreign policy objectives and influencing foreign audiences and opinion makers.

Energy Security – An umbrella term that covers various concerns linking energy, economic growth, and political power. Concerns include energy infrastructure, demand, diversity of energy supplies, new energy reserves, revenues, energy prices and markets, risks associated with terrorism and war, and the use of energy as a weapon.

Failed (Failing) State – A sovereign government that cannot or will not perform basic functions to sustain a country, generally due to fractious violence or extreme poverty. A failed state is characterized by the lack of legitimate authority to make collective decisions and the inability to physically control its territory and establish security, provide public services, and interact with other states as a full member of the international community.

A failing state refers to a weak or ineffective government with eroded ability to provide public services, control its territory, provide security, and interact within the international community.

Goldwater-Nichols Act – The Goldwater-Nichols Department of Defense Reorganization Act of 1986, sponsored by Sen. Barry Goldwater and Rep. Bill Nichols, was a major reorganization of U.S. defense institutions and processes. Operational authority was centralized through the Chairman of the Joint Chiefs as opposed to the service chiefs. The chairman was designated as the principal military advisor to the President, National Security Council, and Secretary of Defense. The act established the position of vice-chairman and streamlined the operational chain of command from the President to the Secretary of Defense to the unified commanders.

Hard Power (Kinetic) – The use of military and/or economic force or coercion to influence the behavior or interests of other political bodies. It most commonly refers to the use of military force.

Health Threat – A composite of ongoing or potential enemy actions; adverse environmental, occupational, and geographic and meteorological conditions; endemic diseases; and employment of nuclear, biological, and chemical weapons (including weapons of mass destruction) that have the potential to affect the short- or long-term health (including psychological impact) of a given population.

Insurgency – A condition of revolt against a government that is less than an organized revolution but more than a simple belligerency.

Intelligence – The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

International Development – The multidisciplinary practice of creating sustainable solutions to challenges caused by poverty and the lack of resources in a country or region. Development efforts are generally geared toward improving and increasing economic growth, social welfare, civil society, governance, private sector development, and environmental and natural resource management.

Narco-terrorism – Terrorism fueled by the sale of illegal narcotics.

National Security – A collective term encompassing both the national defense and foreign relations of a nation relating to the protection of its interests. These include preserving the nation's political identity, framework, and institutions; fostering economic well-being; and bolstering an international order that supports the vital interests of that country and its allies. National security is the foundation for the development of valid national objectives that define national goals or purposes. U.S. Ambassador George Kennan offered perhaps the most succinct definition: "the continued ability of [a] country to pursue its internal life without serious interference."

National Security Act – The National Security Act of 1947 mandated a major reorganization of the foreign policy and military establishments of the U.S. government. The act created many of the institutions that Presidents found useful when formulating and implementing foreign policy, including the National Security Council, the Central Intelligence Agency, and the Defense Intelligence Agency. The act also caused far-reaching changes in the military establishment. The War Department and Navy Department merged into a single Department of Defense under the Secretary of Defense, who also directed the newly created Department of the Air Force. However, each of the three branches maintained their own service secretaries.

Non-governmental Organization (NGO) – A private, self-governing, not-for-profit organization dedicated to alleviating human suffering and/or promoting education, healthcare, economic development, environmental protection, human rights, and conflict resolution and/or encouraging the establishment of democratic institutions and civil society.

Nonproliferation – Those actions (e.g., diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls) taken to prevent the proliferation of weapons of mass destruction by dissuading or impeding access to, or distribution of, sensitive technologies, material, and expertise.

Non-state (Actors) – Individuals and groups that participate in international affairs, including the private sector, private sector associations, grassroots/community-based organizations, women's groups, human rights associations, non-governmental organizations, religious organizations, trade unions, universities and research institutes, the media, etc. In a security context, the term also includes terrorist groups and other violent organizations.

Nuclear Terrorism – The use, or threat of the use, of nuclear or radiological weapons in acts of terrorism, including attacks against facilities where radioactive materials are present.

Peace Building – Stability actions, predominately diplomatic and economic, that strengthen and rebuild governmental infrastructure and institutions in order to avoid a relapse into conflict.

Peacekeeping – Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement.

Public Architecture – The use of architectural resources in the public's interest. This includes the design, construction, location, and use of diplomatic buildings and cultural centers.

Rule of Law – A substantive legal principle that all citizens are subject to the judicial decisions in their states, as well as those of the courts of a state, and that such decisions are the result of constitutional principles.

Security – A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Smart Power – An integrated national security strategy that effectively and efficiently combines both hard and soft power appropriate for the specifics of each situation, and that adjusts as the particular threat evolves.

Soft Power – The ability to shape the preferences and influence the behavior of others to accomplish desired outcomes. It typically derives from the attractiveness of a country's culture, political ideals, and policies.

Stability (and Reconstruction Operations) – An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

State (Actors) – A politically organized body of people usually occupying a definite territory and having a particular character.

Strategic Communications – Focused government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.

Sustainability – The ability to meet present needs without compromising the ability of future generations to meet their needs, particularly related to environmental and natural resource management.

Terrorism – The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorist – An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Terrorist Groups – Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatening violence in pursuit of their political, religious, or ideological objectives.

Acknowledgments

Symposium Participants *(alphabetical order)*

Roger Barnett, Ph.D.
Professor Emeritus, U.S. Naval War College, Newport, Rhode Island; Author, Asymmetrical Warfare: Today's Challenge to U.S. Military Power

Bryan D. Brown
General, USA (Ret); Business Consultant

Honorable Michael Chertoff
Former Secretary of the Department of Homeland Security

Andrew Cochran
Founder and Co-Editor, "The Counterterrorism Blog"

Paul M. Cofoni
President and Chief Executive Officer, CACI International Inc

Ambassador Dell Dailey
Lieutenant General, USA (Ret); Coordinator for Counterterrorism, U.S. Department of State

Dr. Matthew Levitt
Senior Fellow and Director, The Washington Institute's Stein Program on Counterterrorism and Intelligence

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Dr. Warren Phillips
Professor Emeritus, University of Maryland; CEO/COB, Advanced Blast Protection; CACI Board of Directors

Mark "Chip" Poncy
Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury

Bruce Sherman
Director of Strategic Planning, Broadcasting Board of Governors

Scott Stedjan
Senior Policy Advisor for Humanitarian Response, Oxfam America

Charles "Fritz" Weden
Senior Field Advisor, USAID Office of Transition Initiatives

Lawrence Welch
General, USAF (Ret); President and CEO, Institute for Defense Analyses

Thomas L. Wilkerson
Major General, USMC (Ret); Chief Executive Officer of the U.S. Naval Institute

Authors

Hilary Hageman
Executive Director, Legal Division, CACI International Inc

John Plant
Business Operations Manager, CACI International Inc

Philip M. Sagan, Ph.D.
Executive Director, National Solutions Group, CACI International Inc

Deborah Sutton
Business Development Lead, CACI International Inc

Advisors

Louis Andre
Senior Vice President, CACI International Inc

Bert Calland
Executive Vice President, CACI International Inc; Vice Admiral, USN (Ret); former Deputy Director, CIA; former Deputy Director SOP, NCTC

Paul M. Cofoni
President and Chief Executive Officer, CACI International Inc

Chas Henry
Executive Director of Communications, U.S. Naval Institute

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Dr. Warren Phillips
Professor Emeritus, University of Maryland; CEO/COB, Advanced Blast Protection; CACI Board of Directors

Bill Reno
Lieutenant General, USA (Ret); Consultant, CACI International Inc; Former CEO, The Wexford Group International

Editors

Z. Selin Hur
Publications Principal, CACI International Inc

Michael Pino
Publications Principal, CACI International Inc

Graphic Design and Layout

Steve Gibson
Creative Director, CACI International Inc

Chris Impink
Graphic Artist, CACI International Inc

Stan Poczatek
Senior Designer, CACI International Inc

Publisher and Editor-in-Chief

Dr. J.P. (Jack) London
Executive Chairman, CACI International Inc; Former CEO, CACI International Inc

Communications Executive

Jody Brown
Executive Vice President, Corporate Communications, CACI International Inc

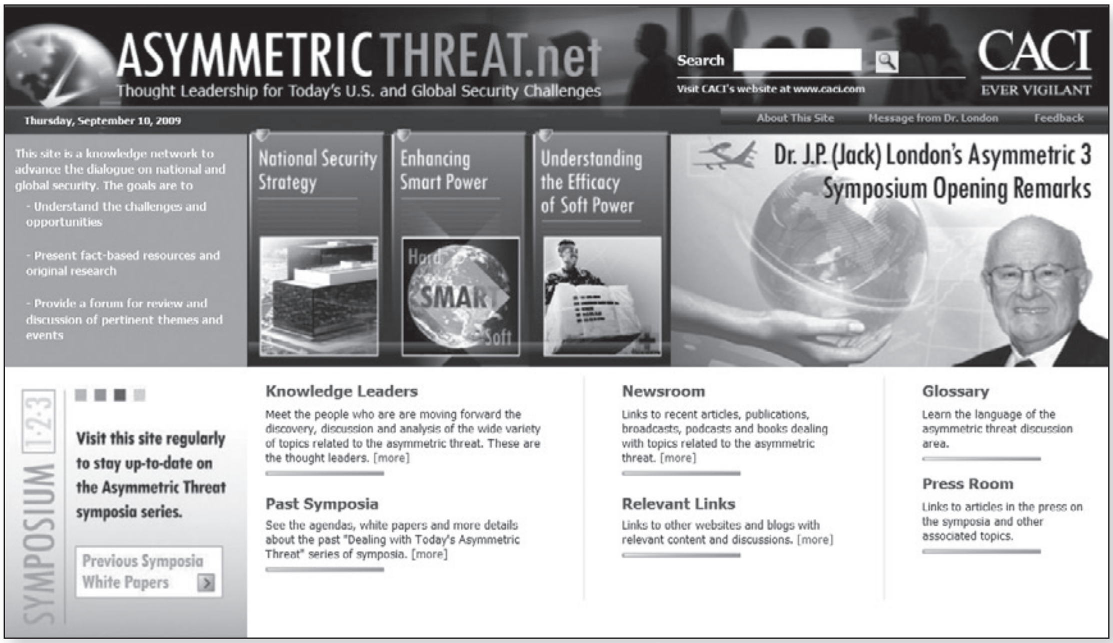
Program Manager

Philip M. Sagan, Ph.D.
Executive Director, National Solutions Group, CACI International Inc

Symposium Three, *Employing Smart Power*, was held on March 24, 2009 at Fort Myer, Arlington, Virginia.

For more information on the Asymmetric Threat symposia series, visit

http://www.asymmetricthreat.net


ASYMMETRICTHREAT.net
Thought Leadership for Today's U.S. and Global Security Challenges
Search
Visit CACI's website at www.caci.com
CACI
EVER VIGILANT
Thursday, September 10, 2009
About This Site
Message from Dr. London
Feedback
National Security Strategy
Enhancing Smart Power
Understanding the Efficacy of Soft Power
Hard
SMART
Soft
Dr. J.P. (Jack) London's Asymmetric 3 Symposium Opening Remarks
SYMPOSIUM 1·2·3
Previous Symposia White Papers

This site is a knowledge network to advance the dialogue on national and global security. The goals are to

- Understand the challenges and opportunities
- Present fact-based resources and original research
- Provide a forum for review and discussion of pertinent themes and events

Visit this site regularly to stay up-to-date on the Asymmetric Threat symposia series.

Knowledge Leaders

Meet the people who are are moving forward the discovery, discussion and analysis of the wide variety of topics related to the asymmetric threat. These are the thought leaders. [more]

Past Symposia

See the agendas, white papers and more details about the past "Dealing with Today's Asymmetric Threat" series of symposia. [more]

Newsroom

Links to recent articles, publications, broadcasts, podcasts and books dealing with topics related to the asymmetric threat. [more]

Relevant Links

Links to other websites and blogs with relevant content and discussions. [more]

Glossary

Learn the language of the asymmetric threat discussion area.

Press Room

Links to articles in the press on the symposia and other associated topics.

The site includes downloadable white papers from each symposium and serves as a knowledge network to advance the dialogue on national and global security, presenting resources and original research, and providing a forum for review and discussion of pertinent themes and events.

September 2009

U.S. NAVAL INSTITUTE

U.S. Naval Institute
291 Wood Road
Annapolis, Maryland 21402
(410) 268-6110
www.usni.org

CACI
EVER VIGILANT

CACI International Inc
1100 North Glebe Road
Arlington, Virginia 22201
(703) 841-7800
www.caci.com