Conference Report
Summary by Dave McIntyre, not yet approved by conference contributors

ANSER Institute for Homeland Security

Homeland Security 2005 Conference

6-7 May 2002, College Park, MD

The Homeland Security 2005 Conference achieved two goals:

- **To elevate the discussion of homeland security issues to the strategic level**
- **To extend that discussion to the mid-term** by looking beyond immediate issues to identify important trends and decisions affecting American homeland security past the next Presidential election year

ANSER's concept of the "strategic cycle" was the organizing framework for the panel presentations at the conference. The strategic cycle's fundamental concept is that strategy has to go beyond planning and the rote setting of priorities and development of policies to achieve goals and to advance interests. Strategy requires establishing a cause-and-effect relationship against a thinking enemy over time. In the case of American homeland security, the desired effect is an atmosphere of deterrence that provides U.S. citizens (and their friends and allies around the world) with both the appearance and the reality of security at home against increasingly capable domestic and international enemies. Such security may be part of a more all-encompassing program to secure American interests internationally and promote freedom, security, and stability worldwide, but the framework focuses specifically on addressing security concerns of Americans at home.

The effect of deterrence is produced by a cause that combines denying an enemy the objective of his attacks with punishment for his aggression. Deterrence based on punishment and denial is further divided into six areas of specific action: prevention, preemption, crisis management, consequence management, attribution, and response. These actions form a strategic cycle that promotes deterrence and restores it if an enemy miscalculates his odds of success and attacks in spite of the deterrence. While many specific strategies and action plans for homeland security may be developed in the future, the ANSER Institute for Homeland Security is confident that those with the greatest chance for success will be grounded in the principles of the strategic cycle. This conference report will summarize the papers and commentaries offered within this organizing framework.

Keynote speakers expanded on this strategic framework through remarks focused on four mid-term issues:

- **Strategy development** by the Office of Homeland Security
- **DoD transformation** for homeland security
- **National organization** for homeland security
- **National imperatives** for homeland security

Welcome

- **Dr. Ruth David,** ANSER CEO, welcomed the attendees and noted that while 9-11 initiated many changes in the United States, the developing program of homeland security could continue to change the structure and the functioning of our government in the future. Dr. David encouraged the attendees to think in longer, more strategic terms and to take full advantage of the presentations, the question-and-answer sessions, and the networking to explore our nation's strategic options from as many perspectives as possible.

- **Col Randy Larsen (U.S. Air Force, retired)** provided a short orientation on ANSER's strategic cycle, with emphasis on the interaction and indivisibility of the cycle. He explained the diffusion of responsibility for parts of the cycle among federal, state, local, and private participants in homeland security and the difficulty of crafting a strategic vision when no one except the president has the authority to issue orders and make them stick. Col Larsen pointed out the key role of attribution and noted that it is a new problem for U.S. strategists and operations, since our enemies in the past have generally been easily identified and well understood. And he emphasized that achieving security against an enemy is different from security against natural disasters, because human opponents are "thinking enemies," who adapt to our security measures. The result is a never-ending cycle where the end and means, as well as the cost and benefit, must be balanced and rebalanced continually in the face of threats to the survival of the nation. Stimulating the debate concerning the many issues associated with this broad national challenge is the focus of this conference. Col Larsen urged the audience to press hard on these issues during the question-and-answer session following each panel.

Deterrence Panel

- Panel moderator **Dr. Peter Roman** introduced the concept of deterrence by recalling the observations of Bernard Brodie, one of the premier architects and proponents of the strategy of deterrence. At the end of World War II and the beginning of the nuclear age, Brodie suggested that the sole role of military power had now become deterrence, since nuclear weapons made war so dangerous that military victory was out of the question. Today the observation may be true for a different reason: First attacks can be so devastating that military response may be irrelevant. Thus, the central issue is how to use the other steps of the strategic cycle to promote and maintain deterrence.

- After an initial warning that real deterrence must be specific in place, time, and threat, **Dr. Barry Posen** offered "a new taxonomy" to help us think about deterrence in this new strategic environment. Plans and actions must adapt, he suggested, depending upon whether the aggressor is a normal state actor, a non-state actor, or a "delusional state actor." This last is an especially useful term, denoting a political group whose values are driven by a belief or political ideology that makes them immune to calculations made by a normal "rational actor." The implication is that deterring such actors may be difficult or impossible and may require a level of effort, degree of risk, and range of actions that the United States finds difficult to mount and sustain.

- **Col Bob Kadlec (U.S. Air Force)** focused on the need to prepare for a terrorist attack based on the conclusion that advances in science and technology are making the strategy of offense

increasingly easy and attractive. His short-term example laid out the dangers of a smallpox attack and the considerations for the three potential responses: vaccinate the entire population, vaccinate part of the population (first responders, the military, etc.), or vaccinate none of the population. Unintended consequences of homeland security decisions are pointed up by the possibility that in an effort to protect the entire population, a nationwide vaccination program could result in as many as 800 deaths due to adverse reactions. Future biological attacks (using "designer diseases" created by DNA modification, for example) could pose even more difficult challenges. Thus, while deterrence is essential, so is preparation for action if—or when—deterrence fails.

- **Mr. Leon Fuerth** reinforced the need for deterrence and placed it in a broader, more hopeful context, arguing that the best deterrence takes place over time by "transforming the enemy." This approach requires a full and robust engagement worldwide and demands that the United States set an example in international cooperation and participation. This is not an easy path; it requires a vision of success, the inclusion of allies, and the will to prevail in a protracted commitment of resources—including military personnel—around the world. But it can succeed, Mr. Fuerth contends, if the United States can remain patient and engaged in the face of uncertainty.

Prevention Panel

- Moderator **Dr. Dave McIntyre** set the scene by pointing out the complexity of the issue. He said that prevention requires that we decide
  - What or whom we need to defend—America, or Americans?
  - What or whom we need to defend against (direct attack from ballistic missiles? indirect cyber-attacks on the economy? chemical, nuclear, or radiological attacks on the population?
  - The balance of cost and benefit we are willing to achieve (protection and cost rise in a steep curve; perfect protection requires that we subordinate all other activity and spend everything we have)

  Thinking through this challenge requires orderly, systemic thought, a broad framework (such as the strategic cycle), prioritization, and practical solutions (a few of which were offered by panel members).

- **Dr. Jonathan Tucker** suggested that we might draw lessons from the Israeli experience in combating terrorism. His five categories for review were
  - The criticality of accurate, specific intelligence on the individual terrorists and supporters
  - The use of infrastructure attack as a strategy (fighting the whole terrorist system—from finances to recruitment, from leaders to foot soldiers)
  - The importance of hardening the defense of what the United States calls "critical infrastructure" (with many of his examples drawn from Israeli efforts to secure their airline industry)

- The necessity of a proactive program to strengthen the psychology of the population to resist attacks (terrorism personalizes the risk; defense must do the same to gain popular support)
- The need for international cooperation, which means publicly making the case for counterterrorism

He offered two examples from the Israeli experience for consideration:

- The use of civilians as an extension of law enforcement and intelligence—80% of terrorist attacks are thwarted, frequently by observant citizens
- The focus on individual actors and not "the system"—Israeli airports screen people; U.S. airports screen baggage

- **Adm James Loy**, Commandant of the U.S. Coast Guard, prepared a paper but was unable to attend. **Rear Adm Terry Cross**, director of Coast Guard operations, attended in his place and delivered the paper. Admiral Loy's paper made it clear that there is no silver bullet to secure the homeland, noting that a determined enemy will always be able to make it into our country with some type of threat. Admiral Loy suggested how the Coast Guard could fit into a national structure that will no doubt be required in response to the pending national strategy. For the Coast Guard that means building defenses as a series of rings (distant from U.S. shores) and as layers (defense in the air, on the surface, and under the surface). The point is that no single set of defenses will provide security. The admiral used the example of a city water system to explain his approach to security, noting that water purity is provided by a whole series of filters and procedures—not just a single filter at the kitchen sink. Similarly, we need a layered approach to homeland security.
- **Dr. Gordon Adams** responded by reinforcing Mr. Fuerth's message that homeland security starts overseas and requires vigorous engagement. Dr. Adams said that the primary challenge is one of coordination with international partners, among federal agencies, between states and the federal government, between states and private institutions, and between state and local governments. He also marked for close attention the issue of how the Department of Defense needs to be organized and the growing challenge of cyber-defense. These challenges will not be met by thinking about them, but by directed action that encourages—and in some cases forces—broad cooperation.

Keynote Luncheon Speaker

- **Dr. Richard Falkenrath** looked toward the release of the National Homeland Security Strategy, now in development, and suggested a number of themes to expect:
  - A fiscally conservative approach to national spending focused on specific outcomes (no blank check for raiding the treasury)
  - A requirement for cost sharing with state and local communities
  - Interest in reinforcing federal plans with non-federal options, such as using the insurance industry to establish intelligent guidelines and distribute risk rather than creating massive new federal offices to do so

- Awareness of the fact that risk cannot be reduced to zero, and the need to deliver that message to the public so that our open society does not disappear in response to future attacks
- A concerted effort to balance prevention, protection, and response without establishing one overriding priority, since that would produce a corresponding weakness that terrorists could exploit

The bottom line at this point is that we are settling in for the long term against an unpredictable challenge, so we need both direction and flexibility, as well as care that we do not waste precious resources.

Preemption Panel

- **The Hon. Frank Kramer** began by noting that although our enemies are formidable, "they aren't ten feet tall"—we can improve protection, and we *can* preempt some threats before they arrive. One key question will be "What standard do we use for preemption?" Kramer offered two thoughts from current law that might be extended to homeland security issues: evidence of a conspiracy to commit a crime, and reasonable doubt as a standard for action. We will face continuing threats, and we will need to preempt—so we need to sort out now the guidelines we might use, and not make them up in the passion of the moment.
- **The Hon. Lawrence Korb** offered a simple but useful framework for thinking through specific situations:
  - Are we organized, trained, and equipped for the mission?
  - Do we have legitimate standing to take preemptive action?
  - Is the threat worth the cost of preemption? And do we understand that the cost is likely to be long term as well as short term and may cut us off from the support of key allies and supporters?

  In short, preemption may be possible and justifiable, but it entails long-term consequences that should not be regarded lightly.
- **Dr. Michael O'Hanlon** furthered the debate by offering examples of preemption—some with positive outcomes, some with unexpected and unpleasant consequences. Of particular interest were the generally successful results associated with "beheading" of terrorist organizations by attacking the leadership. The Red Brigade was offered as an excellent example, although it is difficult to sort out whether their demise was the result of an effective counterterrorism campaign or simply changing times. On a personal note, O'Hanlon answered the frequent rhetorical question "What has really changed since 9-11?" He feels he speaks for many when he says one big change is the willingness to run risks in the area of civil liberties in order to promote homeland security.
- **Rear Adm Richard Cobbold** (Royal Navy, retired) provided a commentary with a foreign perspective on the issues of preemption, noting that the past three years have marked a sea change in the way in which terrorism has been used and perceived. Until 1998, asymmetric threats were used primarily as a tactic—a way of moving negotiations forward in order to

gain a "seat at the table" and greater political power. Irish Republican Army actions against Great Britain demonstrate this approach—frequently deadly, but focused on negotiating a desired political outcome. Since then, however, asymmetric threats have changed character, becoming a strategic threat to the continued existence of some nations, such as Israel and the United States. The threat must now be viewed in this light, which justifies bolder action, perhaps including preemption. But not all countries in the world (especially in Europe) recognize this change and the new requirement for action it engenders. The United States needs a more concerted effort to explain its position, even when it is politically, militarily, or morally justified.

Afternoon Keynote Address

- **The Honorable Peter Verga** provided a timely insight into the thinking of those developing the Department of Defense responses to terrorism and calls for assistance in the area of homeland security. He noted that Defense Department participation has expanded to include three areas: combat operations within the United States, managing the consequences of a major attack, and temporary support to civil authorities. In all these areas, Defense Department participation is more robust than anticipated a few years ago. However, the Defense Department continues to provide support, not the lead, in all these areas. Even in combat operations, the principal decisions will be made by civilian elected officials, and military forces (from the National Guard operating under state control to regulars in national service) will operate in support. However, those support requirements may be significant, and when support is called for, time may be of the essence. Consequently, high-level planning and the ability to prioritize requests and resources will be essential to the Defense Department effort. The recently established Northern Command will have primary responsibility for these efforts, although many specific details concerning authority and relationships remain to be worked out. What is certain, however, is that the Defense Department will be an active player, but a partner and not a leader in the effort.

Supper Keynote Address

- **Congressman Mac Thornberry** turned his attention to the critical nuts-and-bolts issues of organizing for homeland security. An active voice in the homeland security debate for several years and the author of proposed legislation in the field long before 9-11, Rep Thornberry has most recently submitted a bipartisan bill with Sen Lieberman to provide a firmer basis and stronger authority for Governor Ridge and his successors. In reviewing the needs for better organization and clearer lines of authority, Thornberry identified four areas critical to our nation's success: organization of a lead office in the Administration, organization of federal budget requests and expenditures, organization for research at both government and private facilities, and organization within Congress to improve effectiveness and reduce the chances of parochialism in this important issue. Noting that we are very early in this entire process and recognizing that any action will likely alienate some participants in the current process by transferring their power and authority, he called nonetheless for both short-term action and long-term changes in the face of this major challenge to the safety of our citizens and the viability of our nation.

Crisis and Consequence Management Panel

- In urging that the next panel focus for a bit on cyber-issues, **Mr**. **Phil Lacombe** noted that while he liked the concept of the strategic cycle, in reality all parts of it are operating at all times, because cyber-attacks are taking place all the time. In fact, he argued, looking at cyber-defense issues is good preparation for looking at other security issues in the new world we face because cyber-infrastructure is *critical* (no network = no operations), yet no single agent or agency is in charge. Who owns the Internet? Who is responsible for securing it? for managing it during crises? for restoring it after attacks? How do you secure critical infrastructure when the responsibility is shared and no one has the authority to make decisions or takes actions to secure the whole? The answer is still emerging, but sharing information (vulnerabilities and good ideas) is clearly key.

- In pushing our vision of cyber-security issues forward to the mid-term**, Ms. Jody Westby** examined the implications for the changing demographics of the Internet. While noting that English remains the dominant language of the web, she pointed out that today fewer than 50% of Internet users live in the United States and that the fraction is growing smaller by the day as the web begins to penetrate the less developed world where billions of potential users live. While no one really exerts control of the Internet today, it is strongly influenced by its origins and the language and culture of its primary users. As diversity increases, the United States will exert less influence and run the risk of losing its guaranteed availability (what she calls geo-cyber-stability) as well as its current market advantage. (As more and more multilingual users log on, for example, multilingual marketers of ideas and products will have an advantage in an accelerating spiral that eventually marginalizes English-only users.) Additionally, the growing number of users means access for a growing number of bad actors, every one of whom can impact the entire infrastructure. Finally, she noted that the United States is already losing its ability to influence the distributed information base on the Internet because of the growing impact of foreign laws. In short, the United States faces a future in which its access to and use of an electronic network that has become essential to American business and American government are increasingly in doubt.

- While **Mr**. **David Keyes** agreed with the assessment of growing U.S. dependence on the cyber-network for day-to-day survival and expressed concern over the potential enemies—organized and disorganized—who could damage our day-to-day public and private operations. But he expressed doubts that any attack would make the cyber network a *primary* target, just because the carnage would be too small and too short in duration to merit the risk of U.S. response. Instead his concern is the changing environment for cyber-operations, which will see increasing tensions in a number of areas: security vs. privacy; civil considerations vs. military considerations; “search and security” operations vs. “search and destroy.” In all of these areas, actions and policies will be driven by a body of laws that are increasingly outdated and struggling (and right now failing) to keep up with the changing environment. This is not a reason for undue pessimism—answers to these challenges are possible, and a number of government studies have offered viable solutions. However, none of them has really worked so far because of inadequate funding. Models of the combination of cooperation and control required include the Y2K center and Fannie Mae (in the lending industry). Public-private partnerships grounded in current laws will be the foundation of a secure cyber-future.

- **Ms. Jamie Gorelick** began by noting three difficult challenges in promoting the cyber-security of the homeland:
  - We are increasingly technology reliant
  - Our security depends upon a number of cyber-resources the government does not control
  - We do not really know the extent of the threat

  On this last point, she believes the greatest future danger will be from loosely affiliated threats that operate independently but with the common goal of crippling the United States. Reprising a theme struck the previous day by Col Kadlec, she suggested that technology is outrunning our ability to control it so quickly that an electronic Pearl Harbor is inevitable. Fortunately, she maintains, some solutions are possible. Unfortunately, they were identified as long as five years ago but neither action nor funding followed.

  To address the mounting threats, Ms. Gorelick first recommends establishing a single government entity with the legal authority, technical capability, and bureaucratic size and weight to take on the mission and produce results. Such an organization would be a hybrid, including law enforcement expertise and military capabilities and instincts in order prepare for attack and then hunt down attackers. Beyond this, cyber-security of the homeland will require an active public-private partnership. The key link is provided by informed CEOs of corporations—alerted to the dangers, motivated by incentives to cooperate and adapt, informed by sharing best practices industry-wide. The driving force for such activism can be the insurance industry, with laws and rates promoting voluntary compliance. Additionally, cyber-security requires an improved legal framework, with exceptions to the Freedom of Information Act, changes to antitrust laws, and promises of corporate confidentiality when working with the government. Some changes would be very significant, such as changes to the Fourth Amendment, which makes it difficult for the U.S. military to respond to an attack that passes through a U.S. terminal. In short, positive actions can produce greatly increased cyber-security, but they will require the right organizational structure, the right information exchange, and the right market incentives—all of which the government should be promoting more boldly.

  Finally, Gorelick emphasized that defense alone will never be enough—cyber-security demands that we find a way to fight back, to mount offensive operations against attackers. (In terms supplied by the ANSER Institute, deterrence must include both denial and punishment.)

Attribution Panel

- **Mr. John Gannon** laid the groundwork for this panel by pointing out that confidence in the ability to attribute an attack underlay all else in the U.S. effort against the Soviet Union during the Cold War—only because we knew the identity of the attacker (or potential attacker) were we able to conduct the detailed analysis required to produce an adequate deterrent. In the 9-11 attack, by contrast, the anonymity and flat organization of the terrorist network defeated our $30 billion intelligence hierarchy. (For example, we still do not know who launched the anthrax attack last fall.) This element of the strategic cycle must be addressed if we are to produce deterrence or security for our homeland in the future.

- **Dr. Jay Davis** proposed that we borrow a logical and time-tested approach to thinking through the challenge of attribution:

  - Doctrinally, what do we want to know? (Sometimes exclusion can be as important as identification.) What do we want to do? (Make war or prosecute?) With whom will we do it (domestically and internationally)? How much of our own capability are we willing to reveal?
  - Operationally, what process do we use? How do we articulate it to others? How do we educate, train, and practice? What is a credible timeline that we might pursue?
  - Tactically, what can we actually do? What should we actually do?

    Each answer impacts all the others.

  In conducting attribution, we should be prepared to work with former enemies or maybe even potential enemies if our interests coincide and to recognize that industry may provide some of our best information. We do have considerable experience in this field, if we can find a way to collect and synthesize it.

  Recommendations:

  - Put one U.S. government agency in charge—Dr. Davis recommends the FBI
  - Establish a senior, independent (and technically competent) panel reporting directly to the president on especially dangerous issues (attribution for biological and nuclear weapons)
  - Make a concerted effort to educate senior people on the need and capability for attribution
  - Recognize the importance of international legal issues and begin facing up to these influences and constraints now

- **Dr. Jeff Hunker** grouped the problems of cyber-attribution as follows:

  - Attributing an attack to a specific source (machine)
  - Attributing that machine to a specific individual or organization
  - Attributing a specific intent to that individual or organization

  The bottom line, he suggests, is that it is impossible to guarantee attribution as the Internet is currently designed. Better technology will not solve the problem, because it is a design issue, not a hardware or software issue. The only solution for proper cyber-attribution is the creation of a new, secure Internet, with access provided to those willing to comply with standards ensuring attribution. Noting that the current Internet culture (no constraints, absolute freedom, including freedom to prey on others) is as big a problem as the technical problem, he believes that the culture cannot be changed and that the solution is to exclude from the critical infrastructure all except trusted agents who can be identified. (In subsequent conversations, Hunker suggested that the problem of creating a second web is not as great as it would seem at first glance, because not all elements have to be rebuilt from scratch. Some elements—public databases, transmission means, etc.—can be shared. The issue is to restrict access to critical functions to those willing to make their identities known. Essentially, the

old system would continue for most users and overlap in some ways with the new system that protects critical users.)

Keynote Luncheon Speaker

- Beginning with the admonition "If you don't know where you are going, any road will get you there," **Congressman Chris Shays** noted that eight months after 9-11, "That's where we are." Calls for homeland security have been hijacked, he charges, by existing organizations, and resources needed for important issues are not always going to the right places. The current approach to intelligence too often confuses means with ends—too often sees producing an intelligence product as the only responsibility of the intelligence community, instead of accepting some responsibility for the utility of the information and quality of the decisions made as a result. This new age with its new challenges requires new thinking, and his chief concern is that too much of the status quo will survive. Rep Shays embraced the ANSER strategic cycle as a good starting point for analysis, going on to note that we must treat the American people like adults, informing them that future attacks are a near certainty—the issue is not "if" but "when, where, and with what magnitude."

  A vote for war is unnecessary at this point, Rep Shay asserted, since "we have been at war for 30 years. It stares you in the face." The larger issue is whether our action will be strong enough to revive deterrence. Clearly our past actions encouraged the failure of deterrence on 9-11. As a result of our weak response in the past, "What were the terrorists thinking when they attacked us? Probably that we would sue them." Only proper action overseas and at home—only a robust response and innovative advancement of homeland defense—can restore deterrence and secure America's future. Rep Shay concluded with several vignettes of American responses to 9-11 in his district, noting that the American people are not vindictive, but action oriented: they want their government and their leaders (public and private) to get on with the business of punishing our enemies, denying them further success, and restoring a world of deterrence.

Response Panel

- The **Hon Bob Gallucci** launched the final panel of the conference by posing no statements or positions, only questions:
  - What is most difficult about response?
  - What difference does it make if the threat is WMD? (Maybe a big one difference the need and willingness to respond.)
  - What difference does it make whether the enemy is a state or non-state actor?
  - What is the relationship between response and deterrence? (How exactly does one produce the other?)
  - What if certain attribution is impossible?
  - What is special about biowarfare? Would we break the Non-Proliferation Treaty to respond to a biological threat or biological attack? Would we go nuclear?

- Is there anything we can do to respond to an attack immediately?
- What damage will we be willing to accept as a response to our response?

- Focusing on U.S. response to a cyber-attack, **Mr. Lawrence Castro** echoed previous concerns that technology was providing attackers with tools faster than defenders could adapt. The result, unless something changes, will most certainly be an attack on computer assets critical to U.S. life and security. The problem with defense alone is that it really does not deter (this would especially be the case if, as others asserted during the conference, the possibility of mounting an effective defense is slim). Our future security depends upon offering a viable alternative, made public enough for potential aggressors to know that they face a swift and certain response. For this, we need to think logically through the most likely attacks, including "red teaming" our own plans and analysis. Then we need to develop a declared computer operations strategy and the capability to reply in kind to any attack. And we need these changes now.

- **Mr. Frank Gaffney** generally agreed but focused on our current situation and noted that there are no good options in the world of response. "How did we get into this fix?" he asked. "How did we make ourselves both vulnerable and attractive for attack?" The answer he poses is that "we embraced defenselessness as our defense," accustoming potential enemies to a weak response that made attacking us almost cost free. The threat of retaliation is always better than the reality, but when the threat proves inadequate, we are left with ugly choices like the ones before us: "Will we retaliate? Against whom? How?" Seeing some value to ambiguity in answering these questions at this point, he urged that we steel ourselves for the difficult days ahead and move immediately to revitalize our nuclear arsenal (including a return to testing nuclear weapons) and design new conventional and nuclear weapons that would make a fitting response easier. In short, prepare ourselves and others for the certainty of a continued response beyond the war in Afghanistan while preparing additional options for the president.

- In reviewing the previous speakers on her panel and some of the previous speakers of the two-day conference, **Ms. Judith Miller** strongly endorsed Mr. Castro's call for a careful review of the specific threats we face and the impact they might have, with special emphasis on challenging our own work with "red teams." The rigor of the process is especially important, she noted—we must subdivide problems across boundaries of jurisdiction, authority, etc.; we must find ways to address horizontal problems with horizontal solutions. This need for broad analysis and solutions extends beyond Mr. Castro's call for a cyber-strategy and should be replicated in every area of homeland security (including biological, chemical, nuclear, radiological, and conventional threats as well).

  Making careful use of words, Ms. Miller pointed out the danger of diffusing the moral clarity of our response if we are too loose with the concept of "retaliation." Response is legal and justified, she repeatedly assured the audience—it is both possible under international law and advisable as a strategy. We just have to be careful in the way we conceive and articulate that response. As an example, she noted that the response to 9-11 has been widely accepted (if not always supported) around the world. It also appears, at least up to this point, to have been effective. So determining to make future measured responses is an acceptable course of action. But we will be well served to think through the potential challenges and our potential

responses ahead of time, rather than try to design an effective reply from scratch—and without benefit of a rigorous analysis of the best course of action and the potential outcomes.

End