

# Framing Deterrence in the Twenty-First Century

On 18–19 May 2009, the Air Force Research Institute (AFRI), the Royal United Services Institute (RUSI), and King's College, London, cosponsored a conference entitled "Framing Deterrence in the Twenty-First Century" at the RUSI facilities in London. As the AFRI director, I was honored to join with Michael Clark, the RUSI director, and Prof. John Gearson, director, Centre for Defence Studies at King's College, to cohost the two-day event. The changes in the international environment since the terrorist attacks on the United States in 2001, in Madrid and London in 2004 and 2005 respectively, and the emergence of new and ill-defined challenges to peace and stability in the world made the subject of deterrence of great interest to participants from Europe and the United States.

Our discussions over the two days confirmed our assumptions about the relevance and timeliness of the topic; namely, that it is vital to our collective national interests that our policy makers receive the best advice possible about this subject. Nevertheless, there are possibly more questions than answers in the field of deterrence studies. Those who expect quick, concise, and immediate practical answers from this area are destined to be frustrated by the highly conceptual tone of the products of deterrence conversations. Others may experience similar frustration as the conversation quickly turns to notions of nuclear deterrence, arms control and limitation, and counterproliferation. There are, however, several insights that can inform policy discussions.

First, deterrence may not apply to all situations. Some adversaries are probably not likely to be deterred by any practical means at the disposal of state actors—such challenges must be either contained or eradicated. Also, some situations defy deterrence because they are too dynamic or too ambiguous.

For those situations in which statecraft does apply, there are situations that can and should be shaped without resorting to the conflict inherent in deterrence interactions. This implies that states adopt comprehensive, whole-of-government approaches that are relevant to the global security environment. In such a context, states should focus and tailor their strategies according to the demands of the threat. Perhaps equally important, the

complexity of the challenges we face requires strategies based on partnering with those who share similar worldviews and goals. Their perspectives and resources may add appreciably to the collective ability to cope with challenges across the globe without requiring that any one state bear the full burdens and risks associated with deterrence strategies.

Second, for those situations where deterrence may apply, policy makers must determine the appropriate instruments that work in concert with military preparation to ensure that the object of deterrence has the capacity to receive, understand, and value the deterrent aims of the policy. Additionally, deterrence success depends on being able to assess the adversary's behavior and likely countermoves. Without such assessment measures, deterrence will remain a theoretical construct with little relation to actual conditions as they exist in the adversary's camp. Further, and this is somewhat counterintuitive, deterrence also depends on the adversary assessing your intentions and your actions to reach the same conclusions that you want reached. In other words, much must go right for deterrence to work, but in most cases the consequences of failure nevertheless justify the attempt.

Third, there may be ways to deter a wide range of adversaries. To do so, however, requires developing an understanding of these actors' motives and values. To the extent that criminals, insurgents, terrorists, and other groups that represent challenges to state and international security value political goals and outcomes, they may possess levers of vulnerability that states can hold at risk and thus can use for deterrence purposes.

Fourth, as long as states possess nuclear weapons and as long as there are states that seek to proliferate weapons of mass destruction (WMD) and delivery technologies, deterrence remains a valid strategic approach. Where states have acquired such systems, deterrence is the dominant paradigm that provides a foundation for governing interaction with competitors. This serves as a crude reminder that great-power wars are a bad idea. For those states that seek to acquire nuclear or WMD capabilities, deterrence strategies provide a robust set of theories and approaches to use to delay or prevent proliferators from developing and deploying such systems.

In addition to the observations above, the participants identified three significant areas that require new thinking and research. The assumptions behind extended deterrence must be updated for the emerging security environment. During the Cold War, the number of nuclear powers was somewhat constrained by the combination of scientific and technical challenges of producing nuclear weapons, counterproliferation efforts, formal

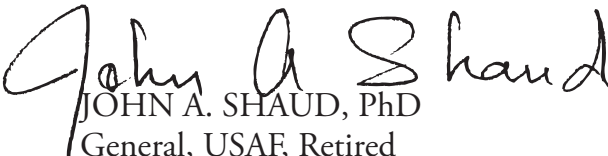
arms-control agreements, and the confidence that the great powers would protect their allies from attack. This last cornerstone of deterrence has always relied on the belief that the great powers would respond appropriately and credibly to aggressive moves against their partners. Should this notion of extended deterrence erode, the result could be a destabilizing arms race with the accompanying increased risk of conflict.

The potential dangers stemming from failure of extended deterrence are magnified by our lack of understanding of how deterrence applies to securing cyberspace. Our reliance on cyber capabilities and the absence of legal, ethical, and forensic frameworks makes this new domain one of the most volatile and vulnerable components of national security today. Adversaries are adept at leveraging cyber capabilities to probe and to launch attacks across the breadth and depth of our societies while states remain in a reactive posture. Developing theories and frameworks to help deter cyber adversaries could prove to be one of the most important conceptual projects of the early twenty-first century.

Finally, while the existence and roles of states as the primary actors in the international system will likely remain for the foreseeable future, other actors have also demonstrated the ability to influence the system. Policy makers will need better tools for assessing the motives, roles, and capabilities that nonstate actors possess. Some of those actors will need to be deterred using a wide range of strategies and capabilities—not using exclusively military or nuclear options. At present, however, our understanding of the scope of these tasks appears to be quite limited.

The collaboration between AFRI, RUSI, and King's College was an excellent opportunity to exchange ideas with some of the brightest strategists and thinkers in the world today. We learned that, in contrast to popular impressions in many circles that deterrence was an outdated Cold War concept, it remains a vital strategic tool for government and military leaders charged with national security. The weakness is not in the concept of deterrence; it is in our lack of studying the theory in light of the present context. As Department of Defense and Air Force leaders evaluate our strategic postures in the coming months, those who have thought seriously about deterrence, in all its aspects, should contribute their perspectives. Our strategies must be characterized by a sophisticated understanding of the best mix of options for dealing with the challenges and threats we face today and will face in the future. I look forward to seeing products and ideas from the London conference in future issues of *Strategic Studies Quarterly*.

More importantly, I look forward to seeing our national policies informed by those who have thought long and hard about how to integrate deterrence into our defense structures.



JOHN A. SHAUD, PhD  
General, USAF, Retired  
Director, Air Force Research Institute