Rethinking Deterrence
February 2014

Deterrence was the linchpin of U.S. strategy for decades, but the context for deterrence has changed markedly. Instead of a single, near-peer opponent, the U.S. faces an array of possible attackers with differing capabilities and tolerances for risk. In this new context, we need to consider how deterrence can remain an effective guide for policy.

Deterrence requires opponents to compare the benefits of an action against potential cost and the likelihood that such costs will actually be inflicted. There must be credible threats that if a threshold or redline is crossed, it will lead to unacceptable loss. In the Cold War, the threat of nuclear war deterred the Soviets from invading Western Europe and Japan or attacking the U.S. While it was often a subject of debate, the nuclear umbrella set redlines the Soviets could understand and found credible because they were linked to core American interests. To the extent the U.S. has thresholds or declaratory policies today, they are too often surrounded by a mass of caveats, and so vague that some new opponents may not even recognize them as threats.

If opponents do not know what lines they should not cross, it is hard to deter them. "Strategic ambiguity" does not excuse a failure to identify thresholds based on core U.S. interests. Potential opponents will not be deterred if they do not fear retaliation, if they have a greater tolerance for risk or cannot accurately calculate it, or if they dismiss U.S. threats as improbable. Countries likely dismissed a recent Defense Science Board report that suggested cyber attacks would justify a nuclear response. China knows that espionage has never justified a military response. Iran may have wondered how many bank websites it needed to disrupt to trigger nuclear retaliation.

The strength of U.S. armed forces means that countries will seek to avoid military conflict, but neither a nuclear response nor the threat of a conventional attack can deter many of the threats the U.S. faces today. Even nuclear threats did not stop Soviet espionage or regional adventures. Applying old concepts to new problems and using untested assumptions about opponents is easy but unhelpful. The symmetry in doctrine, weapons and risk that made Cold War deterrence effective no longer exists. The U.S. has not done the work of calculating what threats create credible deterrence and how best to communicate this to opponents. If deterrence can be revitalized, it will require clear thinking on the following problems:

1. Aside from deterring nuclear attacks, is nuclear retaliation a credible threat in any other domain of warfare?
2. What is the standard of proof that required before we would retaliate with nuclear weapons? Would this standard of proof require a public presentation in a venue like the UN?
3. A cyber attack might have immediate effect, but it could take days or ever weeks to determine who caused the attack. Is nuclear retaliation affected by the timeliness of attribution? Is nuclear retaliation plausible after several days or weeks of uncertainty? Does the standard of proof increase with time?
4. How do we assure ourselves the cyber attack was not spoofed? How long would that take and what does it do to the plausibility of nuclear retaliation?
5. What are credible redlines or thresholds that the U.S. could make known to influence potential attackers?

These issues point to the central questions for political leaders and policy makers – how useful is deterrence for U.S. strategy and what changes could make it more useful?