Strategy After Deterrence

> "A military is built to fight....and focus on fighting and fighting to win."
> Xi Jinping at the 19th Party Congress

One dilemma (among several) for American strategic thinking is the still-powerful influence of the dead hand of Cold War thought. If there are historical precedents for the current situation, it is not the somewhat static bipolar competition of the last century, but instead some combination of 19th Century great power competition and the rise of aggressive authoritarianism in the 1930s. Yet we continue to try to apply Cold War ideas to strategic challenges, including cybersecurity, and chief among these is the concept of deterrence. What does deterrence mean in an international environment where:

- Opponents have spent years developing strategies to circumvent America's deterrent capabilities.

- They perceive the U.S. as strategically inept and believe it can be outmaneuvered in ways that reduce the risk of retaliation.

- Cyberspace has become the chief domain for conflict, and, unlike nuclear weapons, whose use was to be avoided, cyber "weapons" are used on a daily basis in ways that do not pose existential threats.

We need to discard Bernard Brodie's assertion that "the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them." Nuclear weapons create a ceiling that countries stay below in their use of force and coercion. While nuclear weapons reduce the likelihood of major war between nuclear-armed powers, they do not prevent conflict. If anything, conflict among major powers is increasing, albeit in new forms.

Authoritarian regimes challenge the U.S. and the West. They use coercive actions (force, the threat to use force, and cognitive manipulation) to advance their interests while staying below an informal threshold that, if crossed, would risk triggering a damaging response. There were similar thresholds in the Cold War, but technological and political changes make low-level conflict more effective and enticing.

Cyberspace is one of the principle arenas for the new conflict. The persistent weakness of cyber defense makes cyberspace a relatively low cost, low risk arena for coercion and "almost-force." It also mean that a cyber strategy centered on defense will be inadequate. However, cyberspace is not the only arena for conflict.

Our strategic competitors - Russia, China, and Iran - have created tactics that allow them to pursue their strategic goals while managing the risk of direct military engagement. They use cyber, threats, influence operations, and the positioning of military forces that provide advantage while managing the risk of conflict with the U.S. The expansion into the South China sea or the occupation of Crimea are examples. If opponent intent was initially to push back against the

United States, they now see an opportunity to gain regional dominance and (especially China) and reshape global rules and institutions in ways that favor their interests.

It appears (pace recent actions against Iran) that our opponents may believe that it is possible to take certain action against U.S. interests without retaliation. A Russian interlocutor with ties to the FSB said, "After the [2016] election interference, we waited for the U.S. response, and were surprised when nothing happened." A Chinese general, when asked about the risk of engaging with the U.S. in cyberspace replied that the U.S. had "great capabilities, no will." If opponents believe that the risk of warfare with the U.S. can be managed and that the U.S. will not use nuclear weapons except in response to an existential crisis, they will test the limits of what can be done to harm U.S. strategic interests (or determine if there are any limits at all).

This testing takes place in an increasingly conflictual environment. This conflict is over political and economic influence (things that technological leadership can provide). The Cold War is not a useful precedent. Then, two powerful opponents confronted each other and, while avoiding general conflict, engaged in proxy war, testing, and occasionally bellicose verbal confrontations, and were deterred from direct conflict by the threat of nuclear war. Nuclear deterrence works as well now as it did in 1990, but the game of strategy has shifted.

Brodie and other nuclear strategists assumed that nuclear weapons would never be used. In contrast, cyber "weapons" are used on a daily basis. This sets the context for signaling and deterrence. Possessing a powerful cyber force and have it glower at opponents from the sidelines does not deter and the signal this sends, no matter what words accompany it, is unpersuasive.

Engagement is the best way to change this. Defining what is unacceptable requires pushing back. This cannot be one-off actions, but part of a larger campaign to constrain opponents and advance national interests, accompanied by planning on how to manage the risk of retaliation. For cyberspace, the assumption that underlies persistent engagement is that sharp rebukes, "painful, but temporary, and reversible" will reset opponent analysis of the benefits of continued cyber actions against the U.S.

Credible threats are at the center of any strategy to counter opponent action. Opponents actions show that they are not deterred in key areas, and believe they can take damaging actions without risk if they stay below the implicit thresholds that their actions and our responses have defined. Possessing powerful military forces is insufficient, given opponent efforts to develop and use strategies to circumvent them, and there has been a steady erosion of the U.S. position in Europe, Asia, the Middle East and Africa. The pivotal moment for cyber conflict was the Syria redline debacle in 2010. After that incident, we saw for the first time coercive political actions against targets in the American homeland. Administration efforts to rebuild credibility after 2010 were probably undercut by the indecision over the 2016 interference, and things have not improved greatly since then.

Contrast the current situation with the Cold War. U.S. threats or signals to deter the Soviets were credible. The U.S. had fought and won a global war to defend Europe, firebombed cities, and ultimately used nuclear weapons. This history shaped Soviet thinking about conflict with the U.S. Credible threats were linked to a clear retaliatory threshold. Eisenhower’s declaration that nuclear weapons would be used if there were “trustworthy evidence of a general attack against the West” set a clear threshold linked to American interests. That threshold still holds (more or less), but it is not sufficient to stop opponents as they have carefully thought about how to circumvent the nuclear threat.

The U.S. has had the luxury for thirty years of not facing serious competition and this hampered the development of strategy. It lacks strategies to reverse opponent strategic gains. The U.S. cannot expect to conquer or defeat opponents. Regime change has not worked well, and there has been no serious thought about what regime change in Russia or China would mean for U.S. interests and global stability- it is hard to see any outcome that would be positive. We have opponents who are not going away and who are not going to stop using coercion to seek change that serves their interests. This is where the similarities to the 19th century are of greatest use in reassessing strategy.

Drawing from the example of 19th Century competition, one way to achieve this is sustained low level engagement that mirrors the tactics of our opponents, which are designed to control escalation without forsaking coercive effect. Sustained engagement does not come without risk, but the days in which the U.S. faced no strategic risk are over. The task is to engage and manage the risk of escalation without denying the need for more assertive strategic actions.

There are a number of corollary requirements for this task that include redefining national interests, reconsidering the utility of our current force posture and weapons acquisitions (which often date to the last century), building the mechanisms for direct diplomatic engagement on security issues with strategic opponents, and developing and funding non-military strategies for confrontation and competition. These are things that the U.S. has not had to do for decades and, as it is currently organized, may not be able to do at all absent major reform.

Opponents must be persuaded that the risk of harming the U.S. and its interests through coercive action is too great. There is still a credibility "deficit,' and they will only be persuaded of this if they see concrete actions, not signals, words, or threats. Ultimately, the U.S. will need to define how to use engagement to actively advance its national interests, based on the lessons of engagement (and assuming the U.S. can redefine its interests in some meaningful way).

The British historian Paul Kennedy, whose work on the fall of the British Empire is often applied (inappropriately) to the United States, made an interesting point on why empires fail - it is not that they do not recognize problems, it is that they continue to apply old solutions that worked well in the past to new problems where they are no longer effective. The sooner we replace deterrence, signaling and all the other accoutrements of nuclear strategy as a guide for strategy the better it will be for defending U.S. interests.