CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Cross-Domain Deterrence and Credible Threats

James A. Lewis
Center for Strategic and International Studies
July 2010

The concept of deterrence rests on a series of assumptions about how potential opponents recognize, interpret and react to threats of retaliation. The fundamental assumption is that a correct interpretation by opponents will lead them to reject certain courses of action as too risky or too expensive. The problem is that potential opponents may misinterpret deterrent threats while others may be not feel threatened, and are therefore harder to deter.

The United States faces new kinds of threats to its national security. Conventional military conflict is the least likely threat to the United States. The immediate threats are insurgency and terrorism, and crime and espionage in cyberspace. There is also the potential threat of asymmetric attacks against civil infrastructure, space assets or military forces. There has also been a diffusion of potential opponents, from a single adversary who would at times mirror U.S. actions to a collection of near peer opponents, regional states, and non-state actors.

During the Cold War, U.S. nuclear forces are assumed to have deterred some Soviet actions. It is worth noting, however, that they clearly did not deter lower levels of conflict—espionage, efforts to influence western politics, or the use of proxy forces. Deterrence may have channeled Soviet activities into these nonmilitary challenges, but this suggests that we may be able to deter the kinds of threats and conflicts that are most frequent in the post-Cold War international security environment—conventional attacks and some forms of asymmetric attack— but not terrorism, espionage or state-sponsored crime.

Cyberspace poses a particular challenge for deterrence. State actors are engaged in harmful acts in cyberspace against the United States. However, military force is of limited utility in responding to or deterring actual cyber threats. A U.S. military response to espionage or crime would be a strange departure from international norms regarding the use of force. A retaliatory cyber attack (where the intention is to damage or to destroy, rather than exploit) or retaliation using a kinetic weapon for a cyber attack against countries that have not used force against us or against individuals with criminal rather than political aims, could easily be interpreted as an aggressive and unwarranted act by the international community. The result is to cast doubt on the credibility of a retaliatory threat, weakening any deterrent effect.

Uncertainties over attribution and collateral damage reduce the ability to make a credible threat outside of armed conflict. Since we know the identity of an attacker in perhaps only a third of cyber incidents, and since a skilled attacker will disguise their identity to appear as someone else, the United States could easily attack the wrong target. This almost happened in 1998, when DOD was prepared to authorize a counterstrike against the PLA, whom it assumed was responsible for an "attack," when it discovered that the authors were actually three teenagers in California.

And since we are unable to predict with confidence the scope of collateral damage, a cyber counterstrike could easily damage an ally or neutral party. Deterrence strategies in the Cold War accepted a large degree of collateral damage as necessary for threatening nuclear retaliation. Nuclear strikes would have harmed civilian populations in both NATO and Bloc countries. But the collateral damage from nuclear weapons, although immensely greater, was in some ways easier to predict than the effect of cyber attack – the blast and radiation effect is in the area around impact; in contrast, collateral damage in cyberspace may not be contiguous with a target or even located in the target country. Uncertainty about collateral damage will limit the willingness of political leaders to authorize cyber counterstrikes, further eroding the credibility of a deterrent threat.

One threshold issue for a decision on the use of military force in response to a cyber incident is whether that incident is an act of war. An incident judged to be an act of war could justify a military response. However, to the extent possible, potential opponents will avoid actions that could provoke an American military response, a strategy that erodes or neutralizes some forms of deterrence. No action taken against the United States in cyberspace to date has risen to the level of an act of war. Only an action that caused physical damage or disrupted critical services would begin to rise to a level that would justify the use of force.

The construction of a credible deterrent threat will be difficult in these circumstances. An explicit or implied deterrent threat along the lines of "Stop your citizens from committing crimes or we will use military force against you" will provoke either outrage or ridicule. It would also be an unusual and unprecedented step to use military force in response to espionage (a precedent the United States, itself, might not wish to see created). We could excuse an opponent if, in the face of these limitations, they did not find an American threat to use military force much of a deterrent in cyberspace.

New kinds of opponents complicate the ability to deter by threatening a military response. These opponents include near-peer competitor states like China, "unreasonable" regional states like Iran or North Korea, and non-state actors like Al Qaeda. We cannot safely assume that each set of actors has the same tolerance for risk or will have the same reaction to deterrent efforts by the United States. Some opponents may overestimate their strength, and believe that they can succeed in resisting or intimidating the United States. This is an error many have made in the past, and it will likely be repeated again in the future. Some opponents may hold eschatological beliefs that reduce the effectiveness of threats of retaliation. And other opponents will see a deterrent threat as a challenge calling for an aggressive response.

In the new international security environment, deterrent threats could actually increase the chance of conflict. With Iran or North Korea, we may find ourselves in a situation where overly overt deterrence could increase tensions or escalate the risk of conflict rather than deter attack. These countries already perceive the United States as hostile and threatening, so it may be difficult to increase the level of threat to deter them without heightening tensions.

Some opponents may not be deterred by threats of retaliation. When Mao Zedong downplayed the potential for American nuclear attacks, was it bravado and an effort to bluff, or did it reflect a

willingness to accept levels of damage that the United States would consider unthinkable? Mao may have been wrong to consider the United States a "paper tiger," but he may have sincerely believed it in the sense that he discounted the ability of U.S. forces to inflict unacceptable levels of damage. An opponent who discounts the use of force will not be deterred by threats. While China today is a near peer, and likely to be more risk-averse than non-state actors, China under Mao was close to the regional state opponents we face today, such as North Korea or Iran, who may be willing to accept higher levels of damage in any conflict.

Even a more risk-averse China will have a different conceptual framework for conflict and international relations than was the case with the Soviets. China lacks the experience of the Cold War to guide their interpretation of American actions and signals intended to deter. More importantly, some deterrent threats may trigger an escalation of tensions or a violent response. Chinese views are shaped in part by their response to the "Century of Humiliation," which leads them to be both more suspicious and more nationalistic. The primary objective of the Chinese government is regime survival, and Chinese leaders see the collapse of the Soviet Union as a cautionary tale about engaging the United States on its own terms. A threat against the political survival of the Communist party could force China to extreme actions relatively quickly. We have not adequately assessed the distance between threats that an opponent finds to lack credibility and a threat that an opponent may see as raising existential risk. This distance could be smaller than was the case in the Cold War.

Deterrence is less effective in an environment where the United States has more to lose than its opponents Deterrence in the Cold War rested on a higher degree of symmetry in tactics and targets, and this symmetry helped to shape the opponent's calculations of risk. In an anti-satellite exchange, our military capabilities could be severely damaged, while the effect on China, which operates very few satellites, would be marginal. China, Russia and Iran (if it further develops its capabilities) could get considerable benefit from attacking our space capabilities while we would only get marginal benefit from attacking theirs.

This suggests that deterrence in space or cyberspace cannot be "domain limited" and will require threats in other domains, such as saying that an attack on our satellites could lead to an attack on terrestrial targets. A credible threat may require the United States to threaten to retaliate in some other domain, but this brings a risk of escalation of conflict.

Politically or religiously motivated opponents are much less likely than government leaders to be deterred by the threat of retaliatory attack. Opponents like the Iranian Revolutionary Guard do not think like lawyers or technocrats. They think like gangsters or drug lords. Their language is one of coercion and intimidation. They are inured to threats, and may discount or ignore threats against their forces, cities, or populations.

Non-state actors have no capital city or infrastructure to threaten and their willingness to accept risk is much greater than most nation-states. Non-state actors do not face the same political constraints that apply to state actions in cyberspace. Some potential opponents may even welcome retaliation, as it could provide justification and expand support for their cause. Against jihadis and other insurgents, the threat to use force will not deter them from attacking. At best, a threat will shape their planning. These individuals have already accepted a high degree of risk in

pursuit of their aims and, in the case of jihadis, they believe their populations are already under attack, they lack tangible assets that can be held hostage, and they may not fear death as much.

Given the difficulties of making credible threats, improving U.S. cyber deterrence may require something other than increasing military capabilities. Deterring some kinds of attacks may require "stigmatization"— the creation of a credible international norm that says some forms of attack (in space or cyberspace) run counter to accepted international behavior. . The use of nuclear weapons was stigmatized, but it may be more difficult to stigmatize less destructive forms of attack or to extend stigmatization to all forms of attack in a particular domain (e.g., kinetic anti-satellite attacks, which leave damaging debris, could be stigmatized; in contrast, a blinding laser attack, which affects only the target satellite might still be seen as legitimate).

Cyber deterrence could benefit from greater attention to defense. Increased attention to defense and resiliency could reduce the perceived gains of an opponent from cyber attack, thereby changing an attacker's decisions in ways that are not achievable by threatening reprisal or retaliation, and decreasing the chances for successful attack and increasing the costs of detection.

Better defenses could be reinforced by multilateral understandings on acceptable behavior in cyberspace – explicit norms or obligations. A norm that establishes state responsibility for the private actions of its citizens could make it more difficult for Russia to plausibly deny its involvement in attacks on Estonia. Just as nations feel a degree of constraint from norms and agreements on nonproliferation, establishing explicit international norms for behavior in cyberspace would affect political decisions on the potential risk and cost of cyber attack.

The United States could increase the likelihood of success for a deterrent strategy by indicating constraints on its own military activities, as it did with the Soviets during the Cold War. Fear of U.S. capabilities drives some opponent actions, and misperceptions of U.S. activities are used by opponents in internal debates to justify a "response" to U.S. aggressiveness or "hegemony." The United States would need to identify not only what it would be willing to give up, but what it would want from opponents in exchange. This kind of negotiating process would help to establish "bounds" for cyber conflict.

Deterrence can be buttressed by creating an ability to 'signal' an opponent about potentially risky behavior. These signals could include implicit warnings created by changes in force status or readiness posture) concern over opponent behavior, by developing tacit understandings on 'redlines' and thresholds, by implicit or explicit understandings among potential opponents, and by public statements about intentions. Signaling cannot occur in a vacuum however – the opponent must sufficiently understand U.S. doctrine and practices so that they can correctly interpret the signal. The U.S. has not built this understanding for cyber conflict. It is not even clear if potential opponents share a common lexicon of terms for cyber warfare. Common understandings are necessary as they allow for both credible threats and for tacit communication with an opponent. Developing such understandings could make cyber conflict easier to prevent or manage.

Perhaps the most difficult question is whether deterrence is now a victim of its own success. The United States has successfully deterred attack by conventional military forces. More than this

may not be possible. The United States today has overwhelming military force at its disposal. Our opponents strive to avoid conventional warfare or strategic exchanges with the United States, as these would be costly and likely result in defeat. Near peer opponents, either by intent or by a desire to avoid risk, shy away from actions that could reasonably justify the use of military force by the United States. While near peer action in cyberspace is damaging, it has remained below the threshold of an act of war, has not involved violence, and could not be considered an act of aggression under international law. We can claim success in the ability of our extraordinary military capability to produce deterrence in some domains, but in other aspects of conflict, including cyber conflict, opponents may be unresponsive to threats to use military force.

The constraints that limit the value of deterrence would change with the onset of conflict. Experience suggests that even without extensive "tutoring" by the United States to develop a shared conceptual framework and lexicon, there is some fundamental level of deterrence that new classes of opponents will intuitively understand. However, deterrent threats, especially cross-domain deterrent threats that are credibly communicated, could be useful in shaping opponent choices on tactics, targets and weapons in conflict.

Deterrence is politically attractive. It does not require engagement with other nations and winning their consent to norms or constraints. It does not require the investment and regulation required for better defense. But its utility in cyber conflict will be much more limited that in the past. Deterrence based on military force is still valuable for dissuading opponents from undertaking certain kinds of attack, but this may need to be buttressed by political actions that go beyond classic, force-based deterrence. This points to the need for engagement, norms, and understandings on a framework for cyber conflict.