Reconsidering Deterrence in Cyberspace
October 2013
James A. Lewis, Center for Strategic and International Studies[1]

The paradox for cyber deterrence is that while the U.S. has the most advanced cyber forces in the world, their ability to deter opponents is negligible. Deterrence has failed in cyberspace. We have not deterred cyber espionage by many countries, foremost among them China. Cybercrime is not deterred. Russia was likely deterred from a conventional attack against Estonia in 2007 by Estonia's membership in NATO, but it was not deterred from encouraging "patriotic hackers" to launch denial of service attacks against Estonian government websites and financial institutions.

Deterrence, in its archetypal form, is the possession of sufficient military power to credibly threaten to use force if vital interests are endangered, thus dissuading an opponent from taking action. Today, new opponents with different perceptions of risk and an inability to make credible threats mean that the ability to deter attacks against networks is so limited we can reasonably ask if deterrence makes sense as an organizing principle for strategy.

Efforts to resuscitate deterrence seek to redefine it as resiliency, compellence, anything other than using military threats to shape opponent decisions. U.S. capabilities for what can be called "general deterrence," remains high, and the U.S. can still effectively deter major military operations against America and its allies, but we can deter little else because the value of cyber 'attack" far outweighs the potential cost. Nuclear deterrence achieved success at a strategic level, but it did not deter Soviet espionage, use of proxies, or adventures at the strategic periphery, and we should not expect to deter similar challenges today.

One complication is that nuclear deterrence may not have actually worked as we think it did.[2] The U.S. had nuclear weapons and threatened to use them if there was, in Eisenhower's, words, "trustworthy evidence of a general attack against the West." Eisenhower hoped that nuclear deterrence would obviate the need for more expensive conventional forces. Later administrations moved away from this position to experiment with various response options and different mixes of conventional and strategic forces. The U.S. assembled a complex hierarchy of weapons, signals, and strategies, but despite a high degree of openness on nuclear strategy, by the U.S., the intent of this deterrent hierarchy was often not understood by the Soviets.

This is important because deterrence rests on assumptions about how potential opponents interpret and react to threats to use military force. The central assumption is that an opponent will correctly assess the risk of damaging consequences if they undertake certain courses of action, and that this will lead them to reject those actions as too risky or too expensive. Deterrence is most effective only in political environments that include sustained direct and indirect engagement with potential opponent. This environment no longer exists. Deterrence in the Cold War was the result of a long and tense set of exchanges over a period of years between the Soviets and the U.S. This has not been replicated with today's potential opponents.

Any reconsideration of deterrence must reassess Bernard Brodie's famous statement: "Thus far

[1] This is an abridged version of a longer essay published by the Stimson Center.
[2] A good account of this can be found in Payne, The Fallacies of Cold War Deterrence

the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose." There was little need to demonstrate the capability of nuclear weapons to win battles (noting that it would likely be a pyrrhic victory). The mere existence of a strategic nuclear force was enough to deter major conflict between the U.S. and Soviet Union. This is no longer the case. In peacetime, opponents will test the limits of provocation; in war, they will assume that attacking U.S. cyber assets is worth the cost. This chief purpose of strategy now is to speed the transition from deterrence to warfighting, asking how to win battles, how to fight through unavoidable attacks, rather than prevent them.

New Classes of Opponents

There has been a proliferation of opponents, from an adversary who would often mirror U.S. actions, to a diverse aggregation of different opponents, with different vulnerabilities, strategies, and attitudes towards risk. These new opponents include competitors like China and Russia, confrontational regional states like Iran and North Korea, and non-state actors. Each has different tolerances for risk and different abilities to accurately calculate risk that limits the ability to use threats to deter them.[3]

Some new opponents lack the experience, institutions, and skills to correctly calculate the risk of an attack. Other new opponents may be relatively impervious to threats. They have a different conceptual framework for conflict and lack the experience of the Cold War to guide their interpretation of American actions. Some overestimate their strength. For Iran, religious beliefs may lead it to devalue deterrent threats. This is not an issue of rational or irrational. Our opponents are rational in that they calculate risk and benefits, but their calculations are based on different assumptions and preferences.

Similar factors shape the reaction to deterrent threats by non-state actors, many of whom already accept a high degree of risk and who may not fear violence as much as State opponents. Non-state actors have no cities or population to threaten, and their tolerance for risk is much greater than most nation-states. These individuals have already accepted a high degree of risk in pursuit of their aims and they believe their populations are already under attack. They may accept death as a necessary sacrifice. Against jihadis and other insurgents, a threat to use force may not deter them from attacking. At best, a threat intended to deter will only shape their planning. Some non-state opponents may even welcome retaliation, expecting that the resultant collateral damage would provide justification and expand support for their cause.

Asymmetric Vulnerability Means Asymmetric Risk

Deterrence in the Cold War rested on a high degree of symmetry in targets and tactics; this symmetry helped to shape the Soviet's calculations of risk: it no longer exists. The benefits of attacking and disrupting computer networks will be readily apparent to new opponents. They will be tempted to use such attacks in the initial phases of conflict, particularly given the benefits of surprise, with the belief that cyber attack will provide them with asymmetric advantage. We

[3] Foreseen by Herman Kahn, who believed the ability to deter would decline as smaller, less reliable nuclear powers emerged.

can expect opponents to calculate that in conflict, the use of temporary and nondestructive attacks or the disruption of military computer networks adds relatively little additional risk of escalation or unacceptable damage for the attacker.

Americans tend to think about vulnerability from an apolitical and technological point of view. This involves assessing the chances that a weapon can reach its target and the damage it will cause. This may not be how opponents assess vulnerability. An opponent who discounts the use of force will discount vulnerability. Mao's famous statement (to Nehru in 1954) on how "the death of 10 or 20 million people [from an atomic bomb] is nothing to be afraid of" may have been bluster but it also reflected the views of a leader who was demonstrably willing to sacrifice millions of lives to achieve a goal. The massive losses in the Iran-Iraq War are also suggestive of a different attitude towards risk and loss. Overconfidence and underestimation of damage by opponents cannot be ruled out.

Implausible Cyber Threats and Vital Interests

New opponents with differing risk perceptions explain why conventional deterrence fails. Cyber deterrence, e.g. the threat of retaliatory cyber attack, is even less effective. The ability to make a credible threat against opponents' vital interests is the core of deterrence. To be effective, a threat would have to impose an "unacceptable loss." Initial estimates by the Department of Defense calculated that the "unacceptable loss" required to deter the Soviet Union included half of its industrial capacity, at least two thirds of their military forces and perhaps a quarter of their civilian population.[4] This is far beyond the capability of any cyber attack, and ridiculously disproportional as a response to the disruption of a computer network. A proportional response to a cyber attack that also would create the unacceptable loss needed to deter could lead to bizarre calculations (by both the U.S. and opponents. For threats against cyber assets, a proportional response will not produce a credible threat. To deter, a threat must entail existential risk for a state or a compelling and unavoidable threat to the state's territorial integrity or political independence. If there was a way to credibly threaten the use of nuclear weapons after a cyber attack, deterrence might be possible.

However, a threat to use nuclear weapons in response to cyber attacks would be dramatic but not credible. Nuclear weapons are sui generis. Unlike other weapons technologies, nuclear weapons pose an existential threat. Damage and casualties from their use would be massive. In contrast, cyber attacks do not reach the same level of destructiveness – they are certainly not existential threats. Cyber attacks lack the destructive force of a nuclear weapon and the threat to use them may not be compelling at all. We can dismiss calls for a nuclear response to cyber attacks as frivolous. Threats to respond by using conventional weapons in a proportional manner will not deter because they do not pose a risk of unacceptable damage.

The decision to use nuclear weapons is essentially binary; the choice was use or non-use. Many analysts criticized the idea that a nation could engage in graduated nuclear attacks or limited nuclear war without this escalating uncontrollably into exchanges that posed an existential threat.

[4] McNamara's 1967 "Mutual Deterrence" Speech, http://hawk.ethz.ch/serviceengine/Files/ISN/102970/ipriadoc_doc/d755811f-248e-48f1-bbe0-06c1cba0c559/en/1415_McNamara_MuturalDet.pdf

The theory, fortunately untested, was that once the nuclear threshold was crossed, once the nuclear taboo was broken, the deluge would inevitably follow (making nuclear warfighting something of a contradiction in terms). In contrast, cyber attacks can be limited in effect and the risk of escalation can be managed and controlled.

The limited destructive capacity of cyber weapons and the absence of existential or serious harm from their use mean they do not create a deterrent threat. Cyber attacks offer real military advantage, but are not likely to threaten the survival of the state or pose unacceptable damage. A keyboard versus keyboard cyber exchange would either be irrelevant (in terms of the harm inflicted) or likely escalate to conventional military conflict. Threatening someone with a cyber attack is not very frightening even if we exaggerate the consequences. Possessing a credible cyber offensive capability has little deterrent effect.

Anything less than an existential threat or a threat against truly vital interests will not have a deterrent effect– and these "existential" threats require either nuclear weapons or the massive use of military force. Determining a threat to vital interests is a political decision, but there are upper and lower bounds that we can identify. Drawing on the UN Charter, actions that threaten the territorial integrity or political independence of a nation would count as threat to vital national interests. Disruption of economic relations or of communications (subject to Pictet's tests of scope, duration, and intensity) [5] could qualify as serious harm to the national interest.

Overly broad definitions of "vital interests" are both unhelpful and inaccurate. Defining the political independence and territorial integrity of Europe and Japan as vital American interests was compelling for both domestic and foreign audiences, particularly as it came after the tangible demonstration of commitment produced by a massive U.S. effort to liberate Europe and Asia in the Second World War, which included the use of nuclear weapons, followed by the creation of formal defensive alliances, the stationing of significant forces overseas, and clear, sustained high-level interest. A precise definition would identify vital interests as the territorial integrity and political independence of the nation. Under this definition, cyber attacks do not threaten vital interests.

To date, no cyber has threatened any nation's vital interests. Cyber attacks do not pose a threat to political independence or territory integrity. Our opponents suspect we will not start World War III over a non-destructive attack, and cyber incidents have generated little more than complaints. 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. We could excuse opponents if, in the face of these limitations, they did not find these threats to be much of a disincentive or deterrent.

International practice and law limits how force can be used. Nations have the right to use force in self defense against armed attacks or coercive acts which threaten their territorial or political integrity. The principle of proportionality embedded in internal law (and in U.S. doctrine) limits the use of excessive force in response to an attack and constrains the kinds of threats that can be

[5] Jean Pictet, 'The Geneva Conventions of 12 August 1949. Commentary Volume IV: Relative to the Protection of Civilian Persons in Time of War," http://www.loc.gov/rr/frd/Military_Law/Geneva_conventions-1949.html

made. How much force is excessive is of course a judgment to be made by political leaders, based on their concern for international opinion, their own values, and their assessment (with their military advisors) of the political and security consequences of the use of force.

Opponents will not find it credible that the U.S. will use its military against them in retaliation for actions which do not qualify as the use of force under international law (such as espionage or "denial of service" attacks). In international practice, espionage is not considered to be the use of force and a threat to use force in response to espionage is not credible. A military response to espionage would be unprecedented in international affairs and a precedent the United States, itself, might not wish to see created. Opponents will likely dismiss as bluster threats to respond militarily against an act that would not be considered as justifying the use of force in self defense under international law or practice.

While this may suggest that deterrence in cyberspace should not be domain limited and will require threats in other domains, such as saying that an attack on our networks will lead us to respond with kinetic attacks on terrestrial targets, this cross domain approach greatly increase the risk of miscalculation (either by us or our opponent) and carries the risk of escalation of conflict. The strategic calculations to decide what cross-domain action is proportional for a cyber attack would be complex. If the US responds to a cyber attack with a kinetic attack on a space launch facility, for example, this would be seen as disproportional and escalatory.

If we accept that only the threat of truly damaging retaliation has a deterrent effect, and if a truly damaging retaliatory threat can only be credibly made to in response to an attack that involves the use of force and poses an existential threat or threatens serious harm to national interests, we have set the threshold below which deterrence will not work. This means that cyber attacks that do not pose existential threats or immense harm to vital interests are not deterrable. This is also true for cyber espionage or cyber crime. They fall below the threshold that would justify a military response

Our opponents likely estimate that a cyber action that does not rise to the level of the use of force will not provoke or justify a military response by the U.S. An astute opponent would keep their malicious actions below this proportionality threshold. The Cold War showed that there were classes of actions that were not deterred by nuclear threats. The risk is that opponents with different cultural backgrounds, less experience in international relations, and with a higher tolerance for risk might miscalculate the threshold of action which would trigger a response. The likelihood of miscalculation is greater with the broad range of opponents the U.S. now faces and limits deterrence by affecting the credibility of any deterrent threat.

The chances of opponent miscalculation are increased by imprecision in public statements by the U.S. Imprecision erodes deterrence. Ambiguity in deterrent threats, often held up as strategically artful, may actually encourage miscalculation and risk taking. If opponents do not know which lines they should not cross, or if the lines are indistinct, they will underestimate risk. The U.S. believes imprecision retains its freedom of action, but opponents are either puzzled by or dismiss indistinct warnings, especially when they come embedded in a mass of lawyerly caveats. The remarks by then-Secretary Panetta on thresholds for cyber attack are a welcome antidote to generalities found in earlier U.S. strategies.[6]

Strategic Stability in Cyberspace

Nuclear deterrence was believed to produce strategic stability. Nuclear strategy assumed that there was a relationship between stability and vulnerability, where mutual and symmetric vulnerabilities created a stable international situation. The U.S. could "manage" strategic stability by ensuring a rough equivalence of strategic forces to produce symmetric vulnerability, so that the Soviets never perceived a moment when the benefits of attack outweighed the cost.

Cyberspace is not a stable environment. Building more weapons or pursuing equivalence in attack capabilities will not change this. We cannot build our way to stability in cyberspace. The nature of the cyber "weapon" encourages striking first, preemptively. Advance notice may render the attack useless. While truly destructive cyber attacks require skill and investment, less sophisticated cyber attacks are easier to carry out. A lack of agreed norms for cyber attack reduces stability. These factors reshape an attacker's perceptions of risk and work against stability.

The absence of an "arms race," where opponents acquire weapons to maintain a rough parity in capabilities, suggests that there is no link between cyber capabilities and to stability. An arms race is a kind of implicit bargaining between opponents, where one side's deployments or programs led to a countering effort by the other, creating an uneasy stability. Maintaining parity drove military investment and planning. Now, countries build weapons primarily for warfighting advantage. Taking Brodie's point on the utility of military force, the intent of building strategic arms was to deter. Neither we nor our opponents now build weapons with the intention not to use them.

From Deterrence to Warfighting

The United States cannot deter attacks on networks. In peacetime, opponents will stay below the threshold justifying the use of force in response, to avoid the risk of any U.S. retaliation (noting that for different classes of opponents, the level of acceptable risk will be different and in some cases, higher). During armed conflict, the U.S. will not be able to deter or prevent attacks on cyber assets, given different perceptions of risk by attackers that derive in part from the perception of asymmetric vulnerability. They stand to gain more than they expect to lose in any exchange. To paraphrase Michael Howard, there is widespread doubt that a posture of deterrence, however structured, will be enough to prevent an opponent that accepts war as an instrument of policy and has built up a formidable arsenal from not only initiating but fighting through a conflict in the expectation of victory, whether the United States wishes it or not.[7]

Deterrence should no longer be a goal for strategy. Wars can be fought without nuclear weapons; future conflict will include cyber attacks. Strategy should seek to deny cyber attacks

[6] In an October 19th speech in New York, Panetta said that the U.S. would take preemptive action against attacks that threatened U.S. lives or significant economic interests.

[7] Michael E. Howard, "On Fighting a Nuclear War," International Security, Spring, 1981, pp. 3-17 http://wiki.victorybriefs.com/downloads/0816/Howard_81_On_Fighting_a_Nuclear_War.pdf

success in achieving their larger objective of providing military advantage through disruption. The best way to do this is to maintain the ability to fight and win even if attacked. Planning and acquisitions must be based on the assumption that opponents will attack networks and that the U.S. must retain the ability to deliver the services these assets provide and limit any degradation in overall performance.

A second objective for strategy is to shape and constrain the use of cyber attack to influence opponent calculations during conflict. The development of agreed international norms could define constraints and escalatory thresholds and shape wartime use of cyber attacks by make it easier for opponents to calculate risk. Broad international acceptance of norms could lead opponents to choose targets or modes of attack that held less political risk.

If it was possible to "stigmatize" the use of certain attacks or attacks against certain classes of targets (beyond the constraints now found in international law), this would reduce the risk of cyber attacks. The Soviets were successful in changing public opinion to stigmatize the use of nuclear weapons as unacceptable (rather than just a larger and more destructive kind of bomb, as some early American planners saw them), although never to the point of seriously degrading the U.S. strategic deterrent. A similar stigmatization of some kinds of cyber attacks could reduce the risk of these attacks being launched. However, just as nuclear weapons are proportionally more destructive than cyber attacks, it is likely that the stigmatization of cyber attacks would be proportionally less effective in deterring their use (since the stigma for use will be lower). Stigmatization might be harder to create, as cyber attacks do not produce the moral repugnance that created the planned use of nuclear weapons.

Improving defensive capabilities, constructing a normative framework for the use of cyber attacks, and building in operational robustness that limited the benefit an attacker would gain, would all change opponent calculations in ways favorable to the U.S., although But none of these entail building offensive capabilities whose threatened use would deter. Nor will they create the stability and lower risk we assume deterrence brought in the Cold War.

The same strictures on deterrence likely apply to space and anti-satellite attacks. They are attractive targets that offer asymmetric advantage. We cannot make credible threats to deter non-destructive attacks, and in conflict, the value of anti-satellite attacks to an opponent may outweigh any risk unless we threaten a truly disproportional response. If an opponent interferes with an American satellite and the U.S. responds by interfering with one of theirs, we will run out of targets before they do. Risk and benefit are asymmetric and favor the attacker.

We must now ask if the strategies and concepts developed for nuclear deterrence can be usefully applied to other spheres of conflict. Nuclear weapons are uniquely destructive, and the bipolar global conflict was a unique political moment in international affairs. In this context, deterrence made sense, but these conditions no longer exist. Deterrence, like Mahan's decisive battle between fleets of battleships, may be an artifact of strategy from an earlier era that political and technological change has overtaken and made instructive, but not actionable.