Deterrence in the Cyber Age

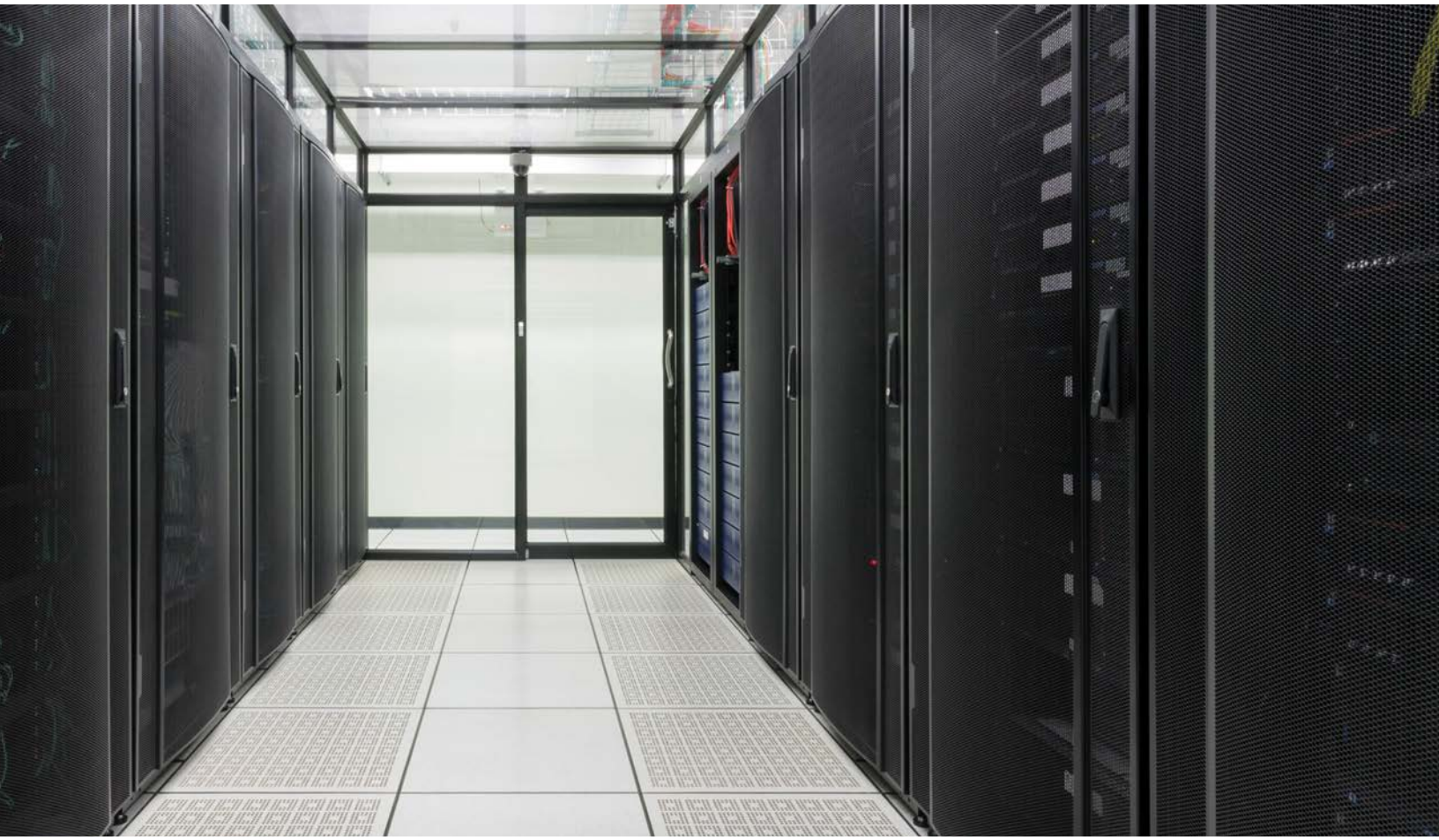
James A. Lewis

Deterrence is the threat to use military force to impose intolerable costs if an opponent takes an unacceptable action. The threat must be credible, which requires opponents to calculate whether it is serious and if potential gains outweigh the possible harm. The context for deterrence has changed markedly, from a single peer opponent to several different rivals, each with different capabilities and tolerance for risk.

Nuclear weapons form the core of strategic deterrence, but their utility is increasingly constrained. "First strikes" are stigmatized, as is nuclear weapons use for anything other than to deter nuclear attack. The destructive effect of nuclear weapons is disproportional to the attacks we face, reducing the credibility of threats to use them. Nuclear weapons deter nuclear attack and (with general military forces) major conventional war, but there is little between these two extremes.

The likelihood that a country will carry out its deterrent threat depends on both material and political factors. Powerful militaries can inflict immense harm even without nuclear weapons, and no one doubts the capabilities of U.S. forces. Opponents use several techniques to manage and reduce the risk of retaliation, such as relying on proxy forces and irregulars. Opponents can limit their actions to those that do not qualify as the use of force (defined by the UN Charter as threatening a nation's territorial integrity or political independence) or that threaten American lives or major economic damage (the U.S. threshold for preemptive response to cyber attack) and diminish the likelihood of American retaliation.

This could be proof that deterrence works now much as it did during the Cold War and is effective at a "strategic" level. America's military rivals avoid actions that could



trigger a damaging U.S. military response. It also suggests the limits of deterrence. Opponents likely calculate that actions that do not affect America's vital national interests, as they perceive them, will not trigger a damaging response.

The United States could change these calculations if it convinced opponents that it had an expansive definition of vital national interests, such as defending the "global commons," but these broad definitions are unpersuasive. Other countries define vital national interests in a more limited fashion and it is through this narrower prism that they measure U.S. pronouncements. For extended deterrence, we can likely deter opponents from invasion or nuclear attacks on allies or friends, but not from supporting terror attacks by proxies or most kinds of cyber attack.

When it comes to a deterrent threat, nuclear weapons are too much; launching a few random cruise missiles is too little; perhaps threatening cyber attack can reshape opponent calculations? This idea is better in theory than in practice. If deterrence has to threaten unacceptable cost, cyber attacks cannot deliver. Their effect is tactical, and while they offer real military utility, they do not pose an existential threat or create intolerable costs. A stand-alone cyber attack like Stuxnet would create only temporary annoyance, and annoyance is not an astute strategy.

"Cross-domain" deterrence is another twist on traditional nuclear deterrence. The idea is to threaten that an attack by an opponent in one domain—for instance, on U.S. space or cyber assets—will result in damaging counterattacks in another domain—such as against sea or land targets. However, cross-domain deterrence turns out to be unworkable. How many ATMs must Iran hack to justify a cruise missile response? How much stolen intellectual property justifies a strike against a Chinese space launch facility? Cross-domain deterrence's complicated strategic calculus does not produce credible threats.

Some scholars argue that a lower threshold for the use of force in cyberspace could deter cyber attack. China's cyber espionage, they say, is "death by 1,000 cuts," and justifies retaliation as economic espionage imperceptibly saps vital industrial capabilities. There is no evidence that the Chinese follow this strategy, which sounds more like the plot of a cheap thriller. Nor have the 1,000 cuts done much harm—America continues to grow, and if growth has been slow in the last 15 years, it reflects bad policy choices more than nefarious foreign stratagems. In any case, after Snowden, it would be unwise for the United States to insist that cyber espionage is an act of war.

IF DETERRENCE HAS TO THREATEN UNACCEPTABLE COST, CYBER ATTACKS CANNOT DELIVER.

Deterrence worked best when linked to clear foreign policy goals and red lines, such as shielding Europe from invasion. Weak linkages between deterrent threats and vital American interests make red lines unpersuasive and encourage opponents to calculate how much they can get away with. The circumstances where the United States will inflict unacceptable harm on an opponent (and risk harm to itself) remain very few.

A vast range of coercive activities directed against the United States and its allies are not deterrable. Some of these actions have only symbolic effect, such as blocking a bank's website. Other actions advance regional agendas that may appear to opponents an peripheral to U.S. vital interests. Some actions, like cyber espionage, fall outside of the scope of what international law regards as justifying the use of retaliatory force. The United States can no more deter espionage or proxy conflict now than it could in the Cold War. Rather than ask what we can deter, it is better to ask how to clearly define vital interests and plan how to counter opponents who adjust their strategies to rely on techniques and technologies that avoid triggering a U.S. military response. ►