ORION FORUM

Why the United States Must Raise the Cost of Attack to Increase Its Cyber Deterrence

AUGUST 11, 2026

Long before the invention of cyberspace, deterrence guarded the U.S. against attack by promising to retaliate in kind against any nation that struck American territory. The Cold War concept of mutually assured destruction may not have been sophisticated, but it was effective at discouraging nuclear conflict with the United States.

America's credible and survivable nuclear deterrent remains a key component of the country's security. Its powerful non-nuclear forces deter conventional attacks. The power of the American military has failed, however, to stop the thousands of state-sponsored cyberattacks that target American interests each year. The costs of these attacks are staggering. Among a long list of negative consequences, tens of billions of dollars of intellectual property are stolen annually while foreign actors manipulate American public opinion and threaten its critical infrastructure.

How and when the U.S. responds to cyberattacks is a closely held government secret. It's safe to assume that some retaliation is occurring, but the volume of attacks directed against the U.S. is a strong indication that adversaries don't take America's retaliatory capability seriously. This is either because the U.S. lacks the capability to counterstrike in cyberspace, which seems unlikely, or because it lacks the will to employ its capabilities. Either explanation represents a shortfall in America's ability to protect its citizens and national interests in cyberspace. This needs to be addressed.

Cyber espionage and other attacks are continuing, in part, because the nations conducting them assess the cost of getting caught is minimal compared to the potential gain. For the U.S.

to secure its cyberspace, this calculation must change. This doesn't mean action is always the right response and there are times when the right decision is to exercise restraint. The U.S. may want to preserve a cyber capability that loses its effectiveness once employed and its modus operandi becomes known to adversaries. It may also, for any number of reasons, want to avoid an escalatory cycle of attack and counterattack.

These are sound reasons to avoid deploying cyber weapons, but maintaining an offensive mindset is key to establishing deterrence. Adversaries must understand that cyberspace is no longer a permissive environment for offensive activities against the U.S. They must believe that America will retaliate following attacks on its networks, its corporations and its infrastructure.

The willingness to retaliate for state-sponsored attacks on U.S. corporations is critical. It makes little sense to leave private sector actors, even large corporations with significant resources, to fend for themselves against foreign governments. Many of these actors are essential to the American economy and important to the country's national security. If a foreign air force attacked the headquarters of an American company, that company wouldn't be expected to field an air force of its own for the purposes of deterrence and defense. The same should apply in cyberspace.

The U.S. can no longer accept large-scale theft of its intellectual property and the infiltration of its sensitive systems. America's technological lead is significantly reduced from the commanding position it once enjoyed, and allowing adversaries to close the remaining gap is a threat to the country's security. The best way to stop the cyber espionage that's undermining American power is through credible deterrence. Another way is through a digital border defended by America's military.

Digital borders, like China's Great Firewall, make it easier for a government to secure its cyberspace but stifles connectivity in a way that can negatively impact innovation. Maintaining a relatively open internet is usually in a country's best interest, but this is only true if deterrence persuades foreign actors not to exploit the openness and negate its benefits. It was the fear of nuclear escalation and the guarantee of American retaliation that limited the scope of Soviet offensive activities during the Cold War. Likewise, modern adversaries can be

deterred in cyberspace if they understand the U.S will apply a swift and significant cost. This doesn't mean, however, that the U.S. should escalate each time it's attacked in cyberspace.

Proportionality matters whenever democratic nations respond to aggression, and retaliation in cyberspace should be carefully calibrated. A cyberattack from a state or state sponsored actor that steals intellectual property from a U.S. company shouldn't, for instance, motivate the U.S. to destroy the electrical grid of the guilty country. The American response should, nonetheless, be sufficiently painful that the foreign actor reconsiders the value proposition of its offensive action. For deterrence to work, our response needs to be consistent, and foreign decision makers must know their actions in cyberspace will be met with a commensurate U.S. response. There's no room for ambiguity.

Beyond the ethical imperative, proportionality is also a control mechanism to ensure that a limited cyberattack doesn't initiate a cycle of escalation that leads to unintended destruction. Since the dawn of the nuclear age, the U.S. has been clear about the conditions under which it would employ its most powerful weapons. Under American doctrine from the 1960s onward, there was little chance that a limited conventional attack, for example, would cause the U.S. to respond with nuclear weapons. Responses were closely managed and thoughtfully considered because the results of uncontrolled escalation would lead to a nuclear exchange and be catastrophic for both sides. This same type of catastrophic risk exists in cyberspace where attacks against banks, infrastructure and government records could threaten the foundations of American society. This risk, however, can't be the reason America shies away from action.

The U.S is facing an onslaught of cyberattacks that it can't continue to tolerate if it hopes to maintain its competitive advantage. These attacks steal sensitive information, weaken social cohesion, threaten critical infrastructure and undermine the public's trust in the country's institutions. The attacks also force U.S. policy makers to wrestle with the possibility that foreign malware is present in our critical systems and might be activated as part of an adversary's response to American actions. This complicates American decision-making.

So far, the U.S. seems to have deterred adversaries from using their most destructive cyber capabilities, but for too long America has tolerated the lower-level attacks that do real harm. Each time America fails to respond to aggression in cyberspace, it undermines deterrence.

Even lower-level attacks provide adversaries the opportunity to load malware onto systems that can then lie in wait until activated at a moment of their choosing. What appears to be small scale probes and limited system penetrations may carry much greater risk than the small amount of damage they seem to cause. The U.S must realize that deterring smaller incursions is critical to guarding against more serious loss because each small attack emboldens adversaries and may be part of a larger campaign.

America possesses advanced offensive capabilities in cyberspace, but these are largely wasted if they're habitually held in reserve rather than employed. Artificial Intelligence is changing the cyber threat and may exponentially increase the capabilities of cyber attackers. If it does, deterring attacks will become increasingly important as adversaries find new ways to circumvent cyber defenses. Deterrence can work to safeguard American interests in cyberspace, but only if would-be attackers expect the U.S. to exact a cost each time they act against it in cyberspace.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.