Correspondence

Is Deterrence Possible in Cyberspace?

Richard J. Harknett
Joseph S. Nye Jr.

To the Editors (Richard J. Harknett writes):

In "Deterrence and Dissuasion in Cyberspace," Joseph Nye reveals the difficulties in applying deterrence to cyberspace by extending the concept from its hard core of retaliatory dynamics and threat of denial to include entanglement (interdependence by another name) and norms.[1] This extension of concept still leaves Nye apparently dissatisfied: he concludes that deterrence in the Cold War was not as good as scholars and policymakers think it was, so perhaps they are holding cyber deterrence to an illusionary standard. Essentially, Nye suggests that both scholars and policymakers should cut cyber deterrence a break.

The management of cyber aggression does indeed need a break: a sharp break away from deterrence-centric thinking. Nye's piece illustrates how we are facing a degenerative program moment or the friction one expects on the edge of a paradigm's need to shift.[2] The evidence from real-world security dynamics suggests that deterrence is the wrong framework for explaining cyber aggression and for formulating policy. Rather than contorting deterrence, we need a line of research outside the deterrence paradigm. In 1998, Nye and Sean Lynn-Jones urged security studies scholars to be open continuously to deep reflection if they are to make a difference.[3] The dominance of deterrence thinking is blocking such reflection and policy application.

Nye's article walks through the very real limitations of both retaliatory and denial-based deterrent threats against cyber aggression. Punishment is made more difficult by

Richard J. Harknett is Fulbright Scholar in cyber studies at the University of Oxford, a professor at the University of Cincinnati, and former scholar-in-residence at U.S. Cyber Command and the National Security Agency. The views expressed are those of the author and do not reflect the position of any U.S. Government agency.

Joseph S. Nye Jr. is University Distinguished Service Professor in the John F. Kennedy School of Government at Harvard University.

1. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi:10.1162/ISEC_a_00266. Subsequent references to this article appear parenthetically in the text.
2. Although Imre Lakatos and Alan Musgrave's notion of a paradigm shift differs from that of Thomas S. Kuhn, all three authors discuss historical moments in which such a shift did not occur. See Lakatos and Musgrave, eds., *Criticism and the Growth of Knowledge: Proceedings of the International Colloquium in the Philosophy of Science, London 1965*, Vol. 4 (Cambridge: Cambridge University Press, 1970); and Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962).
3. Joseph S. Nye Jr. and Sean M. Lynn-Jones, "International Security Studies: A Report on a Conference on the State of the Field," *International Security*, Vol. 12, No. 4 (Spring 1988), pp. 5–27, doi:10.2307/2538992.

International Security, Vol. 42, No. 2 (Fall 2017), pp. 196–199, doi:10.1162/ISEC_c_00290

the attribution problem, and denial is challenging because "cyber defenses are notoriously porous" and "offense dominates defense" (p. 56).

In short, if aggression sits below the threshold where serious military sanctions are credible but above the level where it can be deterred through "good cyber hygiene" (p. 57), the deterrence paradigm fails to address where recognizing security action is taking place.[4] But rather than recognizing these limitations as indicators that new concepts may be needed, Nye's response is to massage the retaliatory and denial problems and then suggest that interdependence and norms be reconceived as "means of deterrence and dissuasion." In doing so, he reduces their considerable potential as standalone approaches. For example, he notes that breaking norms can lead to "reputational costs," when denial fails (p. 60). But this is just the threat of punishment repackaged, which can succeed only if others impose costs through some behavioral change because of the aggressor's poor reputation. The actions of President Bashar al-Assad in Syria's brutal civil war may have damaged Assad's reputation, but unless states change their behavior toward Assad because of his reputation for violating norms (essentially exacting a cost from him), the norm against mass murder counts for little. The causal factor here for Nye that might lead to deterred behavior remains not norms but retaliation, which Nye has already said should not be the basis for deterrence in cyberspace.

What Nye actually wants is "to reduce and prevent adverse actions in cyberspace" (p. 54). This worthy goal does not, and need not, equate with deterrence. Retaliation and denial are tools different from defense, entanglement, and norms. They are also distinct from counter capability and operations offense, compellence, and other nondeterrence security approaches that can challenge, reduce, and manage but not necessarily deter adverse actions. Once one maps national security goals to the reality of cyber operations, deterrence theory becomes more of an impediment than a stimulus to thinking about strategy.

Nye quotes Jon Lindsay's finding that "deterrence works where it is needed most, yet it usually fails everywhere else" (p. 18), which implies that acts that might cross a clear traditional threshold are strategically relevant and "everywhere else" is not. In fact, "everywhere else" is fast becoming strategically relevant space. Cyberspace provides a new seam for traditional great power competition, the intensity of which will only increase as cyber actors leverage machine learning and artificial intelligence technology developments. If one examines the writings of Russian Gen. Valery Gerasimov and the Chinese People's Liberation Army's notions of informationized war,[5] it becomes clear that certain actors see cyberspace as a strategically salient vector for achieving their goals below the traditional deterrence/war threshold.

We must examine the dynamics of the cyber domain if we are to provide policies to secure it. Cyber deterrence thinking seems to block this effort. Every policy document on cyberspace begins with the notion that it is interconnected—and yet we declare it a military domain, rather than a domain in which the military must operate simulta-

4. In fact, the deterrence paradigm distorts policy: despite the actions of adversaries, the United States has pursued a "doctrine of restraint." See U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, April 2015), p. 6.

5. Charles K. Bartles, "Getting Gerasimov Right," *Military Review*, Vol. 96, No. 1 (January/February 2016), pp. 30–38; and Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare" (Carlisle, Pa.: Army War College Press, 2014).

neously with allies, adversaries, the business sector, and individuals. Interconnectedness means that national security actors are in constant contact with other players and, unlike in strategic environments in which deterrence might succeed, it suggests that strategy must assume that contact and action are never absent.

At the tactical level, the "terrain" of cyber engagement is constantly changing. This is human-created space, and every new software version, platform, user interface, and process shifts that terrain. It is perpetually under construction.

So what if the systemic structure of interconnectedness, the condition of constant contact, and the shifting nature of terrain combine to produce a distinct dynamic: offense persistence—a strategic environment characterized by actors with continuous willingness and capacity to produce security challenges? Security could then not be achieved in the absence of action. It would rest in challenging others' pursuit of cyber initiatives through a comprehensive operational approach encompassing resiliency, active defense, and offense. Security would be advanced when one anticipates the exploitation of one's own vulnerability, while anticipating the vulnerabilities of others. Deterrence does not explain how one organizes strategically relevant action in such a continuously active space.

The persistence of offense does not mean that security studies scholars and policymakers should despair; however, using a legacy construct of deterrence, whose measure of effectiveness is the absence of action, to explain an environment of constant action will not prevent adverse actions in cyberspace for many of the reasons that Nye himself outlines. Let us take the critique Nye offers us, not to resuscitate and stretch deterrence thinking, but to logically and creatively move beyond it.

—*Richard J. Harknett*
Cincinnati, Ohio

Joseph S. Nye Jr. Replies:

I am grateful to Richard Harknett for his thoughtful response to my article about deterrence and dissuasion in cyberspace.[1] We agree that classical Cold War deterrence theory is not a good approach to thinking about how to reduce and prevent adverse actions in cyberspace. As I say in the article, the aim in nuclear deterrence is total prevention, whereas many aspects of cyber behavior are more like other behaviors, such as crime, that we try imperfectly to deter. Moreover, attribution is generally less complex in nuclear events. Preventing harm in cyberspace involves four complex political mechanisms: threats of punishment, denial, entanglement, and norms.

I disagree, however, that there should be a "sharp break away from deterrence-centric thinking." Harknett praises my criticisms of "retaliatory and denial-based deterrent threats against cyber aggression." My view is that we should reformulate these aspects of deterrence, but not discard them. Instead we should realize that the complex political processes of dissuasion require us to add the dimensions of entanglement and norms because of the interconnectedness of cyberspace that he cites. He makes the

1. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi:10.1162/ISEC_a_00266.

good point that norms have independent causal effects besides threatened reputational costs, and I tried to indicate this with my example of how the nuclear taboo inhibited President Dwight Eisenhower from accepting the recommendations of the chairman of the Joint Chiefs of Staff in 1954 and 1955.

Our positions would be remarkably similar if Harknett would accept my amendment of his last sentence so that it would say "let us take the critique Nye offers us to resuscitate and stretch [classic] deterrence thinking, [and] to logically and creatively move beyond it." That is what I thought I was trying to do.

—*Joseph S. Nye Jr.*
Cambridge, Massachusetts