IDA | Research Insights

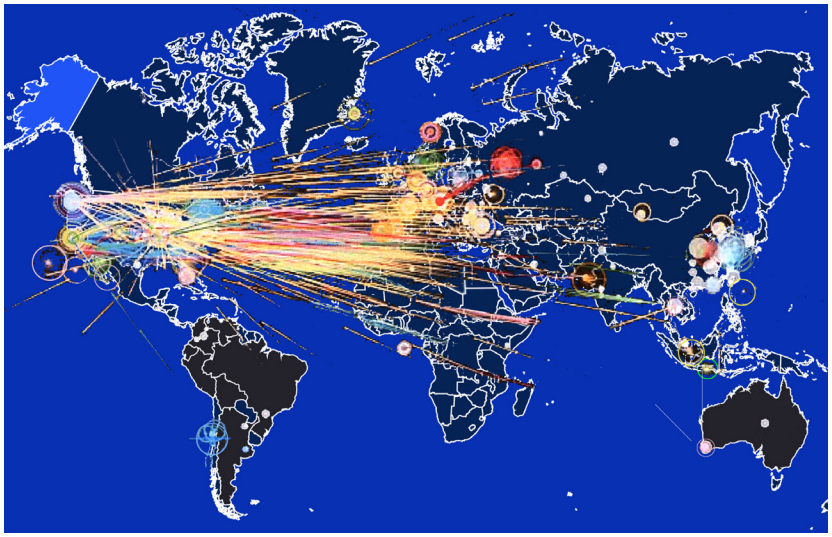
December 2017

Toward a Credible Strategy for Cyberspace

Michael P. Fischerkeller, mfischer@ida.org

In the operational domain of cyberspace, protection and advancement of U.S. national interests cannot credibly rest on deterrence as the dominant strategy. A strategy that takes advantage of the unique characteristics of cyberspace is needed.

Cyberspace is vastly different from land, air, maritime, and space operational domains. Relative to other operational domains, cyberspace has no physical boundaries and the scope and scale of its complex information technology infrastructures are shifting constantly. Both cyber infrastructures and infrastructure data are subject to rapid modification. In addition, whereas the segmentation concept of sovereignty encourages operational restraint in other domains, due to its non-segmented, interconnected nature cyberspace encourages operational persistence. Further, more operators, many able to manage operational attribution, are able to operate with consequence in, through, and from cyberspace than in other domains. Finally, cyberspace operators are able to inflict a broad range of strategic effects, employing cyber operations whose damage may or may not equate with the well-understood concepts of *use of force* and *armed attack*.



Strategies must align with strategic environments. In 2011, the United States adopted a strategy for cyberspace based on traditional principles of deterrence, including operational restraint. However, the cyberspace strategic environment (as described above) does not comprise characteristics that support well a strategy of deterrence. While the goal of deterrence is to avoid operational contact through the threat of use of force, for example, the innate connectivity of cyberspace makes persistent operational contact inevitable. Similarly, whereas a strategy of deterrence requires the source of the potential offending behavior be known, cyberspace allows sophisticated actors to mask their identities. Because these operators are able to conceal attribution more readily than operators in other domains, targets for punishment are not necessarily obvious. Time and again, unknown operators in cyberspace have gained strategic advantage through aggression rather than restraint. This helps account for why the United States and others relying on a strategy of deterrence are losing ground in this vital global space. A credible strategic framework must map to the realities of the cyberspace strategic environment.

The unique cyberspace operational domain calls for a strategy of cyber persistence. Through a dominant strategy characterized by active and persistent engagement in cyber operations, the United States could ensure, maintain, and enhance the strategic national security advantages afforded it by cyberspace. It could also begin to define what is and what is not responsible behavior in this domain. Such a strategy relies on persistent operational contact (as opposed to contact avoidance) through the use of cyber operations, activities, and actions (as opposed to the threat of use of force) to gain continuous tactical, operational, and strategic advantage in cyberspace.

Based on "Deterrence Is Not a Credible Strategy for Cyberspace," by M. P. Fischerkeller and R. J. Harknett, published in *Orbis*, May 18, 2017, https://doi.org/10.1016/j.orbis.2017.05.003.

NS D-8859