

Shaping the International Environment Using Cyber Operations, Actions, and Activities*

Michael P. Fischerkeller, Institute for Defense Analyses (mfischer@ida.org)

The international environment is dynamic. Significant actors are seeking, short of armed conflict, to shape it to support the realization or sustainment of their interests. Shaping operations, actions, and activities (OAs) manifest in a global posture that, in turn, generates residual strategic effects, including dissuasion (persuade a target not to consider a course of action (COA) that would threaten your interests), deterrence (persuade a target not to execute a COA that would threaten your interests), and reassurance (persuade a target to consider and/or execute a COA that would support your interests).

The cyberspace operational domain and cyber OAs introduce to the “shaping” competition uniquely dynamic characteristics that enable rapid, escalation-manageable, cross-domain, and potentially mutable changes to the international environment, as strategy or counter-strategy may demand. These characteristics include, but are not limited to, the malleability of the domain, one by and through which all other domains are enabled; the presence of persistent contact within the domain; and cyber OAs designed to allow for reversible damage, manageable attribution, and damage short of the use of force and armed attack.

The dynamic characteristics of cyberspace and cyber OAs are well suited to serving strategy more effectively than other domain-capabilities pairings. Similarly, given the persistent application of shaping OAs to mold that environment, the persistent-contact character of cyberspace and cyber OAs suggests that they would serve strategy most effectively as part of the shaping toolkit to generate the effects of dissuasion, deterrence, and reassurance.

A comprehensive strategy for cyberspace would address how cyberspace and cyber OAs can be integrated with all instruments of national power to shape the international environment in support of U.S. national interests.

The tables show potential examples of how cyberspace and cyber OAs could be integrated with national instruments of power to generate deterrence and dissuasion effects.

NS D-8312

Integrating Cyberspace and Cyber OAs with National Instruments of Power – Dissuasion

Diplomatic:	Use diplomatic power to argue for interpretations of existing international laws on <i>use of force</i> (with regard to cyber OAs) that support U.S. strategy for cyberspace; establish international norms for behavior in cyberspace when/while U.S. maintains capability advantage in cyberspace
Information:	Employ OAs against social or other media (targeting medium and/or message) to influence, disrupt, corrupt, or usurp media based operations of target audience
Military:	Force Composition: employ OAs to introduce system reliability issues in early development Force Structure: employ OAs against force structure, e.g., joint HQs, to reduce a challenger's confidence in its joint C2 abilities Force Employment: employ OAs to degrade fielded systems reliability
Economic:	Use economic power to develop/globally deploy physical/logical layers of cyberspace that facilitate OAs' employment; employ OAs for targeted financial sanctions or to complement (i.e., moderate or exacerbate) or enforce the intent of broader sanctions (i.e., limit effectiveness of circumvention efforts)

Integrating Cyberspace and Cyber OAs with National Instruments of Power – Deterrence

Diplomatic:	Employ OAs to complement (amplify or moderate) effects from diplomatic messaging, e.g., diplomatic protests coupled with degradation / disabling of non-military capabilities supporting the adversary's intended actions
Information:	Employ OAs against social or other media (targeting medium and/or message) to influence, disrupt, corrupt, or usurp media-based operations (e.g., recruiting) supporting the adversary's intended actions
Military:	Employ OAs to amplify or moderate the potential deterrent effects of other military capabilities
Economic:	Employ OAs to help ensure the intended effects of economic / financial sanctions are realized