February 2017

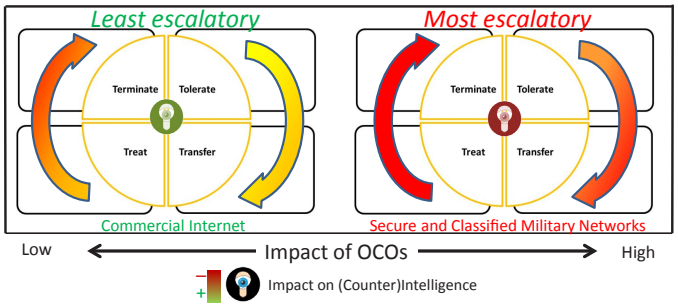
IDA | Research Insights

Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies*

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

The White House Strategy for Cyber Deterrence declares that the United States is creating cyber weapons to defend itself. Developing these capabilities – also known as offensive cyber operations (OCO) – is one challenge; another is determining how to best incorporate them into conventional deterrence strategies.

Communicating Resolve and Managing Escalation through Target Selection



OCOs can have unique attributes: the ability to cause damage that falls short of the generally accepted definitions of use of force and armed attack, the potential for reversible damage, manageable attribution, and the ability to moderate or amplify other capabilities' effects. This uniqueness suggests that integrating the use of OCOs can be informed by blending two strategic concepts: conventional deterrence, which uses the threat of force to convince an adversary not to do something, and coercive diplomacy, which uses military force to persuade an adversary either to stop short of achieving a goal or to undo a challenge once the intended goal is met. Incorporating OCOs into a conventional deterrence by cost imposition strategy allows for the imposition of costs without the use of force.

Issuing a credible threat of using OCOs relies on an adversary's assessment of capability and resolve. Both can be strategically demonstrated through a thoughtful calculus of how an OCO is employed. For example, employing a capability internal to a target is more intrusive, and thus communicates greater sophistication as well as resolve (due to the costs incurred in OCO development). Such employment requires detailed knowledge of an adversary's regime to determine which targets and effects would encourage resolution rather than escalation. Proportional response OCOs, which should discourage escalation, can be informed by IDA's tolerate, transfer, treat, or terminate risk matrix, which offers decision makers several choices for responding when assets are assessed as vulnerable to or experiencing cyber exploitation. This, in turn, requires intelligence support for mapping an adversary's network, exploiting available information on that network, and building a system baseline of the network to help the United States better understand an adversary's organization, plans, areas of interest, vulnerabilities, and system recovery mechanisms.

Communicating Resolve and Managing Escalation through Cyber Tactical Action Selection

Types of Damage: Physical, Functional, Human Psychological

Cyber Tactical Action Class	Target Intrusion	Capable of Influencing a Targeted Process	Command and Control
Specific Intrusion w/autonomous malware (e.g., STUXNET)	Yes	Yes	No – Autonomous
Specific Intrusion (e.g., Havex / SCADA & BlackEnergy) / energy engineering facilities, PDOS (phlashing))	Yes	Yes	No – Event Driven Yes – Duration, Intensity, Visibility
Generic Intrusion (e.g., ILOVEYOU worm)	Yes	No	No
Generic (e.g., DOS / DDOS)	No	No	Yes – Duration, Intensity, Visibility

Potential for Escalation: Highest, Lowest

Impact on (Counter)Intelligence

OCOs can and should be integrated with other military capabilities to either amplify or moderate deterrent effects. For example, using an OCO to disrupt an adversary's satellite-based intelligence, reconnaissance, and surveillance capabilities in conjunction with a force-projection capability would amplify a desired deterrent effect. Using an OCO to temporarily degrade an adversary's integrated air defense system while moving U.S. air forces out of effective range would moderate the intended deterrent effect.

NS D-8301

* Based on: IDA NS D-8213, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies," Michael P. Fischerkeller, October 2016.
Research sponsored by IDA Central Research Project C5175.

4850 Mark Center Drive
Alexandria, VA 22311-1882
www.ida.org