



Strategic and Operational Issues in Cyberspace





Familiar concepts of strategy do not neatly fit into thinking about cyberspace as a military operational domain. The military domains of land, sea, air, and space encompass physical dimensions, whereas cyberspace is an information environment. As such, policy makers may need to tailor or abandon traditionally held ideas. Various IDA projects have tackled the challenges of developing strategic and operational concepts in this unique domain.

A strategic framework for cyberspace. U.S. cyber strategic and operational approaches have matured dramatically over the past several years. This is apparent, for example, in that *persistent engagement* has been the operational approach for U.S. Cyber Command since 2018. Persistent engagement is a new approach intended to inhibit adversaries' relentless efforts to realize strategic gains through the cumulative effects from cyber campaigns. Yet *deterrence* continues to crop up in discussions of cyber strategy. Two examples of this spillage are found in the notion of deterrence by denial and the tendency to equate a deterrence effect with security. In the past, the defense community has been prone to overlay strategic concepts developed for one environment atop another without carefully considering whether they are in strategic alignment. Policy makers need to be disciplined in their discussions and expectations of the [new cyber strategic framework](#).

Operational graphics that describe cyberspace actions. In the operational realm, IDA researchers have enhanced well-established [joint military symbology](#) to help cyber warriors easily express operational concepts in cyberspace. These graphics convey mission-relevant information to people unfamiliar with

the technical details of cyberspace. Using symbology already familiar in the military context will help joint commanders understand, plan, and fight cyber battles and ease decision-making.

Operational assessments of cyber defenses. IDA helps the Director of Operational Test and Evaluation plan, execute, and evaluate realistic cyber events during exercises for the congressionally mandated Cybersecurity Assessment Program. During these exercises, operational test agencies collect data on cybersecurity functional areas from the exercise operators and cyber defenders as well

Tactical Task	Operational Graphic	Traditional Operation	Cyber Operation
Attack by fire		Engage with enemy through direct and indirect fire	Disrupt origination point or interim relay point through overt action
Clear		Remove enemy forces and eliminate resistance in an area	Remove malware, adversary points of presence, and external connections
Secure		Prevent enemy from damaging or destroying a unit, facility, or location	Prevent adversary from changing data or functionality of a network device or domain
Neutralize		Render enemy personnel or materiel incapable of interfering with operation	Prevent another cyberspace unit from using offensive or defensive capabilities

End-to-end security is performed at the endpoints instead of in the network.

as the *red team* (players portraying the opposing force). IDA researchers on-site during the exercises collect data on attack details, defensive responses, and mission effects that combine to present an end-to-end picture of each exercise. IDA continually evolves its analytical methods for [this work](#) to adjust for increasingly sophisticated cyberattacks and defenses. Each exercise presents new questions and provides more insight into the state of cybersecurity across the U.S. military.

Analyzing reactive cyber-intrusion detection. The Department of Defense Information Network is under constant threat of being breached through phishing, hacking, and physical access to network infrastructure. [IDA analyzed](#) Combatant Command training exercises for fiscal years 2014 through 2016 using data on attack detection, defensive responses, and operational effects to develop an analytic framework for operational cybersecurity assessments. The resulting framework informed defensive strategy principles and suggested ways to improve detection of attacks. This article describes how IDA's framework for operational cybersecurity assessments of Combatant Command training exercises conducted between fiscal years 2014 through 2016 informed a defensive strategy. The data collected during these assessments provide insights on both the attacker and defender actions.

Lessons from data breaches. In July 2015, after data breaches of the Office of Personnel and Management affected 21 million Federal employees with security clearances, the DoD Deputy Chief Information Officer for Cybersecurity led efforts to develop a short-term response and a long-term solution. The short-term objective was to notify those affected by the breaches while protecting against additional compromise and exploitation. [IDA supported the DoD response](#) by identifying tasks, assessing progress, and helping bring a contractor onboard. Given the lessons from these efforts, the clear long-term solution to the problem of data breaches became a top-to-bottom, agility-driven transformation of the security clearance vetting ecosystem.



Margaret E. Myers (mmyers@ida.org) is Director of the Information Technology and Systems Division of IDA's Systems and Analyses Center. She leads a team of researchers who address cybersecurity and other challenges of national and global importance.