All the prospective threats identified in *Warnings* represent challenges not just for the United States, but for the entire international community. Yet, the book gives short shrift to the role of global governance and the potential need for the development of new norms to cover such matters as the use of artificial intelligence, the internet, and gene editing in warfare, peacetime, and the gray periods in-between. The present era requires more inclusive processes, not just among nation states but including representatives of the private sector and civil society, and enhanced cooperation.

The authors do not consider whether their emphasis on the sentinel role of human Cassandras will remain practicable. Technological advances are increasing our reliance on machines to assess impending catastrophes and to develop appropriate responses. Indeed, it is not science fiction to anticipate increased reliance on Cassandra machines, which issue credible and timely warnings regarding the location of failing infrastructure, the occurrence of natural disasters, and imminence of health emergencies, and that contribute to saving millions of lives. And yet, while we expect technological advances, including super-intelligent machines, to improve personal well-being, human dignity, and freedom, humans must continue to play a leading role in ensuring that values remain an essential part of the equation. PRISM

International Conflict and *Cyberspace Superiority*: Theory and Practice

By William D. Bryant.
Routledge, 2016
239 pp., $54.95
ISBN-13: 978-1-13889-319-1

Reviewed By: Diana Gill

Cyberspace Superiority is a compelling mix of advanced technological know-how and easy-to-understand writing. Bryant, a Lieutenant Colonel who is a career fighter pilot and earned his Ph.D. in military strategy, first examines whether cyberspace is a "global common"—i.e. a shared resource like the oceans, atmosphere, space, and Antarctica. The answer may well determine the future nature of cyber hostilities but, with the issue as yet unsettled, Bryant posits a far more pressing question—is superiority in cyberspace "a useful construct for thinking about and planning for nation-state conflict in cyberspace?"

Loosely defined, superiority in cyberspace is a combatant's freedom to achieve "friendly objectives, while preventing the enemy from achieving his objectives." For the United States, this means our ability to operate freely in that environment without significant interference from enemy combatants during a time of war. Bryant likens it to superiority inherent to other domains of warfare—land, air, sea, and space—such as efforts by the U.S. Air Force to control air space, or the U.S. Navy to control the sea. He distinguishes cyberspace from the other domains by its extremely plastic nature. "Every computer, router, or device attached, or removed,

Dr. Diana C. Gill is an independent scholar and author of *How We are Changed by War: A Study of Letters and Diaries from Colonial Conflicts to Operation Iraqi Freedom.*

from cyberspace changes the cyberspace domain as a whole. We can think of an individual computer coming online as another grain of sand on the beach."

The virtual territory is only one aspect of cyberspace because of the "the many interdependent networks of information technology infrastructures that are not part of the Internet." Superiority in cyberspace is ever-shifting and disturbingly non-visual. Generals cannot ruminate over aerial photos of proposed battlefields. Satellites cannot pick up troop movements and positions. Sonars cannot pick up sounds lurking beneath the waves. Cyberspace is the ultimate stealth environment, but one which knits together the other domains. Bryant explains:

> *If an enemy disrupted command and control systems in the middle of a major land offensive, the loss of the cyberspace systems could result in the reduction of coordinated close air support over the battle and lead to the loss of the battle in the land domain. All the domains have connections but cyberspace is the most interconnected as combatants have embedded cyberspace in all the other domains through modern information systems.*

In this hypothetical situation of disrupted command and control systems, can cyber superiority be maintained by a combatant or is it analogous to a drive-by shooting—i.e. deadly but temporary? Bryant suggests that assessing an enemy's superiority is dependent on attribution; however, "the difficulty of attribution in cyberspace makes it challenging for defenders to understand where an attack is coming from and makes defensive responses more difficult." The shared nature of cyberspace and low cost of entry further complicate attribution since virtually anyone on the planet with technical know-how and a computer is a suspect.

Bryant explores weaknesses that allow some measure of control in cyberspace and includes in his discussion, analysis of attacks that focus on physical damage and those that affect information. The former can be caused by anything from dropping an actual bomb on a server farm to rewriting protocols to cause the equipment to self-injure. The trick with such attacks is in seeing them for what they are, rather than carelessly assuming them to be normal equipment malfunctions or software glitches. Once the defense becomes aware of what is happening they can quickly learn how to counteract the attack. As Bryant astutely notes, "Cyberspace weapons are akin to glass swords: they can be very sharp and lethal, but they tend to break on the first swing."

Also, unlike in the other military domains, superiority in cyberspace is not intended to be absolute—domination of every computer across the world is unattainable—and is best achieved at the local level. Precision attacks are the goal. Straining for too much superiority invites detection and wastes the valuable resource of time, which is better spent exploiting a small but pivotal foothold in an enemy's computer system. But even on the local level, the persistence of superiority in cyberspace is fleeting—seven out of the eight case studies showcased in *Cyberspace Superiority* lasted less than fourteen days. In closing, Bryant is quick to assert that while cyberspace superiority is highly desirable, it will not win a war by itself. It is merely a "significant advantage to a combatant who achieves it." PRISM