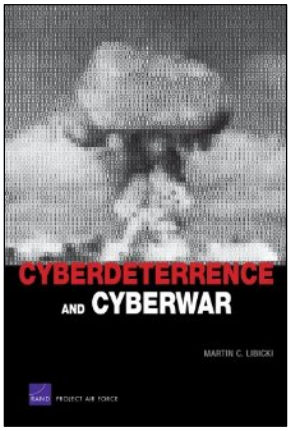
International Journal of Communication 4 (2010), Book Review 1144–1146 1932–8036/2010BKR1144

ijoMartin C. Libicki, **Cyberdeterrence and Cyberwar**, RAND Corporation, 2009, 244 pp., $30.46 (paperback).

Reviewed by
Negar Kahen
University of Southern California



Since modern societies rely on computer systems, enemies can, with little risk, use their mouses and keyboards to attack power stations, bank accounts, and military networks from afar. Today, a coherent strategy is needed to protect the United States from attacks launched by its enemies. The vast dump of government cables by Wikileaks in November 2010 is likely to raise government concern about the possibility of even more aggressive cyberattacks in the future. Martin C. Libicki, a senior scientist at RAND, analyzes the impacts of information technology on national security. His measured analysis will prove timely to panicky decision makers.

Libicki's *Cyberdeterance and Cyberwar* is meant to guide U.S. policy makers and Air Force leaders in crafting cyberwar and cyberdefense goals, strategies, policies, and operations. While highlighting the value of deterrence and vigilance, Libicki warns the U.S. Air Force leaders about the unpredictable nature of cybersecurity and aims to dissuade them from making cyberwar and cyberdeterrence a priority investment area. Libicki's approach is theoretical, rather than example-based.

Libicki defines cyberspace as "the agglomeration of computing devices that are networked to one another and to the outside world" (p. 6). Much like the domains of air and space, cyberspace is a medium of potential conflict—most notably, a cyberattack, which Libicki defines as "deliberate disruption or corruption by one state of a system of interest to another state" (p. 23). He distinguishes between an act of espionage and a cyberattack. In general, cyberattacks should not be retaliated against using deliberate provocations or escalations, lest they provoke a full scale cyberwar—a deliberate attack on a network with the aims of paralyzing it. Deterrence and war-fighting tenets established in other media may not translate into cyberspace, because cyberspace is different from other media, Libicki argues.

Libicki distinguishes a cyberwar from wars in other mediums by first stating that cyberwars are enabled by the exploitation of the enemy's vulnerabilities, not through the generation of force. Second, cyberwars are filled with uncertainty about who attacked and why they did so, what they achieved, and whether they can do so again. Third, cyberattacks that work today may not work tomorrow, as vulnerabilities can be plugged due to changes in technology and security practices. Finally, unlike a nuclear attack, in a cyber attack that creates a mutually respected safe zone is impossible, because the attacker is unspecified.

Libicki differentiates between two types of cyberwar. Strategic cyberwars—"cyberattacks launched by one entity against a state and its society primarily but not exclusively for the purpose of affecting the target states behavior"—are distinct from other, more conventional forms of strategic

coercion (p. 117). If a nation rolls thousands of tanks up to a border and announces its desire to accommodate the aggressor's interests, the nation facing the attack may consent. However, the same credibility calculus does not work in cyberspace, because the defending party may be unsure of what a cyberattack may do to its economy and society. Libicki argues that, in cyberspace, the attacker's capability and the attacked nation's vulnerability are unknown. Therefore, once a cyberwar starts, terminating it is more difficult than for other forms of coercion, because parties can cheat by moving from visible attack to more subtle corruption attacks. It also is possible that third parties will launch an attack masquerading as the other side. Such attacks could be denied if initial sallies fail. These differences, Libicki claims, make strategic cyberwar problematic and inferior to conventional forms of coercion. Therefore, U.S. government and Air Force leadership should not enshrine strategic cyberwar as a priority investment arena.

Operational cyberwar, on the other hand, is "the use of a computer network to support physical military operations" (p. 117). According to Libicki, operational cyberwar may offer a temporary, but potentially decisive, military advantage, because a surprise attack could make an adversary lose confidence in its own system capabilities and cripple its competence. Further, cyberwar is inexpensive to conduct, and hackers are not at personal risk. Yet, Libicki argues, cyberwar has limits. It cannot disarm or destroy the enemy, and cyberwar alone cannot lead to territorial conquest. Therefore, Libicki argues that operational cyberwar should only be used in a support function.

In cyberspace, it is important to use cyberdeterrence to create disincentives for starting or carrying out hostile actions. To be effective at cyberdeterrence, an analyst needs to discern the purpose of an attack. The attacker might have a specific objective in mind, or he could have "attacked" by mistake. Indeed, cyberdeterrence is symmetric, repeatable, and reduces the risk of cyberattacks to an acceptable level at an acceptable cost.

To demonstrate the problems of cyberdeterrence, Libicki provides a persuasive and provocative explanation of possible actions and potential reactions, detailing the complex strategic tradeoffs necessary. His analysis of whether a state should consider retaliation concludes that the state needs to consider what they might gain or lose by retaliating. States' actions could prevent further attacks or could push the attacker to escalate the war further. In addition, whoever must decide to retaliate needs to consider whether to attack publicly or privately. If the retaliator attacks publicly, there is a chance that the evidence presented to justify attack could reveal sensitive information about system security. The risk of a public attack is high because the attacker might not accept the attack passively and may strike back, leading to escalation. Alternatively, if the retaliator decides to strike back in private, the retaliation might be against the wrong target, because it is difficult to know who has initiated the attack. The attacker could be one or more individuals working on their own or at the direction of a state or a non-state actor. It may prove difficult to track down the source of the attack, or there might not be much to retaliate against. Libicki suggests that, because of the problematic nature of cyberdeterrence, United States should exhaust other options such as diplomatic, economic, and prosecutorial means before turning to cyberwar.

Libicki makes specific recommendations about how to react in an event of a cyberwar. Leaders hit by a cyberwar should initially try to convince the attacker that the damage was minimal and short-lived.

Simultaneously, leaders should repair the damage and redouble their defenses against future attacks. Leaders also might falsely portray their network contents to misdirect the attackers' focus. Libicki suggests simplifying systems and adding hardware that cannot be preprogrammed to reduce the risk of future attacks. An ideal system would cover damaged parts of the system and safeguard critical secrets.

Governments can also defend against a cyberwar through indirect means, such as sponsoring research and development in computer network defense and devoting more resources to cyberforensics, including adding traps to catch rogue codes for analysis and investing in threat intelligence.

Cyberdeterrence and Cyberwar is clearly written and well organized. Three appendices address what kind of cyberattack constitutes an act of war, when implicit deterrence policy is called for over the explicit policy and vice versa, and what the prospects are for cyber arms control. The author relies more on logic than on case studies to present his argument. *Cyberdeterrence and Cyberwar* provides a cautious but lucid discussion of factors that American policymakers should consider before resorting to cyberwar and cyberdeterrence.