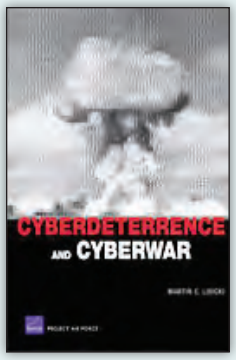
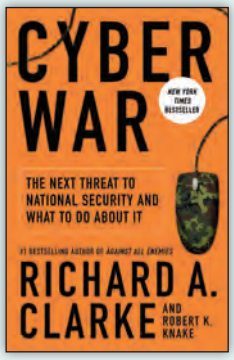
Francis P. Sempa is the author of *Geopolitics: From the Cold War to the 21st Century* and *America's Global Role: Essays and Reviews on National Security, Geopolitics and War.* He is an Assistant U.S. Attorney for the Middle District of Pennsylvania, an adjunct professor of political science at Wilkes University, and a contributing editor to *American Diplomacy.*





Cyberdeterrence and Cyberwar
By Martin C. Libicki
RAND, 2009
244 pp. $33
ISBN: 978–0–8330–4734–2

Cyber War
By Richard A. Clarke and Robert K. Knake
Ecco, 2010
304 pp. $25.99
ISBN: 978–0–06–196223–3

Review essay by
BRIAN R. SALMANS

The concept of war within the cyber domain is no longer an esoteric topic of interest to small groups of people with unique technical skills. It is not rare to hear public discussions on the efficacy of cyber war, a malicious software exploit (most recently the Stuxnet), whether U.S. critical infrastructure is adequately defended from computer network attack, or if the notion of cyber war is over-hyped. Unfortunately, as this warfighting domain evolves, the immaturity at the strategic level of thought is being revealed: contradictory initiatives in the U.S. Air Force (which added cyberspace to its mission statement in 2005 and planned to create a cyber major command, but then changed direction and established a Numbered Air Force instead); the length of time it took the Obama administration to fill its cyber czar position; the discussion of what level of involvement the Federal Government (U.S. Cyber Command and the Department of Homeland Security) should have in protecting civilian resources.

In their books, *Cyber War* and *Cyberdeterrence and Cyberwar*, Richard Clarke (with Robert Knake) and Martin Libicki offer significant contributions in filling this gap in theory and policy and bringing the discussion of cyber war to a more developed level of thought. The authors' achievements are most notable in the area of cyber deterrence, presumably with the intent to get leadership at the strategic level to listen to their warnings as organizations are formed, policies issued, and doctrine developed.

Libicki's portfolio contains a long list of cyber-oriented writings from his work at the RAND Corporation and the National Defense University. *Cyberdeterrence and Cyberwar* is the result of a RAND study to "help clarify and focus attention on the operational realities behind the phrase 'fly and fight in cyberspace'" (p. iii). The chapter on cyber deterrence is the most important of this book. In it, Libicki highlights such important and "wicked" problems of deterrence as attribution, proportionality, escalation, effects, and the role of third-party hackers. These challenges, specifically in attribution and damage assessment from initiating a cyber attack, are the reasons why cyber deterrence is so hard, since deterrence is about sending a signal. Moreover, the worrisome problem of escalation, where cyber activities cross the line to kinetic attacks leading to a physical confrontation, is a consideration that nuclear strategists did not need to address, since they did not have to worry about conflict escalation beyond nuclear exchange. Libicki next proceeds to his most unique contribution to the discussion about warfare within the cyber domain, an issue that is also inseparable from deterrence: the motivation of the originator of cyber attacks. Four categories of motivation are considered: error, coercion, force, and other (such as feelings of invulnerability on the part of the attacker, or the desire to create damage for its own sake). Libicki thoroughly discusses motivation, with thoughtful analyses of possible scenarios.

From these important considerations about deterrence, Libicki goes on the offensive, discussing various ways to respond within the cyber domain, both strategically and operationally. Here there is much room for disagreement as Libicki gets into less familiar territory, with assertions that are somewhat less convincing and do not hold up in practice. In considering conducting a computer network attack, Libicki maintains that several obstacles reduce the incentives of such attacks. An example is his belief that cyber attacks can tip off system administrators to further attacks, thus having the effect of strengthening their defense. Later, Libicki asserts there is a diminishing return from computer network attacks—that is, that more attacks reduce the available pool of vulnerabilities. However, he places too much confidence in system administrators (and in the effectiveness of intrusion detection system networks) learning from mistakes and computer attacks and responding correctly to further strengthen their systems. Frequent reports from the Department of Defense (DOD) and the Federal Government contend that at least 80 to 90 percent of cyber attacks are preventable or could have been avoided by proper configuration, monitoring, policies, or updating of patches. Moreover, in many instances the personnel most knowledgeable about computer network defense issues such as vulnerabilities and current threats are not the system administrators and, in many cases, do not talk with those administrators. Additionally, the belief that a finite number of vulnerabilities for information systems applications exists is hard to justify, considering the complexity of computer applications, the workload of system administrators, the ingenuity of hackers, the fact that updates or enhancements to applications can add their own vulnerabilities, and in observing vendor patch release trends. Anyone using the Internet Explorer browser can attest to the relentless cycles of vulnerabilities and patches.

Libicki returns to more solid ground as he wraps up his book by discussing cyber defense, which he states is "the Air Force's most important activity within cyberspace" (p. xx). Here he highlights the defensive goals of robustness, system integrity, and confidentiality. To paraphrase Sun Tzu, with computer network defense, to know oneself is essential to adequately defend one's network. The Federally

mandated initiative of enterprise architecture (EA) can be very effective in this regard. EA (which Libicki discussed in more detail in his 2007 work, *Conquest in Cyberspace*), can also contribute to the alignment of security efforts with the overall security goals derived from the cyber defense policy and risk analysis for any given entity of interest. Enterprise architecture can further address the trend of increasing complexity in information systems by facilitating the abstraction of this system complexity. EA—which, in many cases, is already being implemented in DOD organizations—may provide an organizing discipline in which to address cyber defense.

Another important addition to the discourse on cyber war and deterrence is Richard Clarke and Robert Knake's *Cyber War*. Clarke possesses an impressive national security résumé, having served in the Reagan, George H.W. Bush, Clinton, and George W. Bush administrations, where he served as the special advisor on cyber security. As with Libicki, Clarke's most important contribution to the discussion on cyber war concerns cyber deterrence. The authors of both books relate their substantial knowledge of nuclear deterrence to their consideration of cyber deterrence, but they make it clear that nuclear deterrence theory cannot simply be overlaid on the cyber domain. Interestingly, the difficulties of cyber deterrence and the lack of experience with and inability to determine secondary effects of cyber attacks (as well as the fact that the United States stands to lose the most in a cyber war) lead Clarke and Libicki to downplay the strategic value of offensive cyber war (as the value of a first strike or retaliatory nuclear capability was a crucial component of nuclear deterrence), and to advocate for better and more effective cyber defenses (whereas with nuclear deterrence, a defensive capability against a nuclear strike was not an important aspect). These are two very important points the authors derive from their experience and from deterrence theory. Both authors are best here, as they methodically arrive at this conclusion with examples from the world of nuclear deterrence as well as pointing out where nuclear deterrence theory falls short within the unique parameters of the cyber domain. In other words, the authors warn, the best defense is not offense; indeed, a strong defense is an enabler of computer network attack.

A stronger cyber defense would strengthen the viability of an offensive cyber strategy by making the United States more likely to withstand an ongoing and escalatory cyber war. Clarke speculates that the United States may be self-deterred because it has the most to lose in a cyber conflict. But he also makes an important observation. With the issue of strategic nuclear war, the military did not maintain complete and secretive control over the entire debate; the academic research community and media also put light on nuclear warfighting policies and plans, resulting in rational discourse on such matters and leading to rational controls and nuclear warfighting plans. Clarke likens our present state of cyber ignorance at the national policy level to that of the European nations just prior to the outbreak of World War I; the plans and operations of military cyber units may be laying the foundation for cyber war with little public scrutiny or oversight. Clarke stresses the need for public dialogue about cyber war—a most useful suggestion to avoid a cyber General Curtis Lemay or "Dr. Strangelove" from forcing the Nation's leadership into a cyber war for which we are not ready and where we do not fully develop the situation to consider all the ramifications and potential outcomes.

Belief in the importance of public discourse and oversight of governmental cyber war activities leads the authors of these two books to divergent views about the proper level of governmental involvement in cyber defense. Clarke is an advocate of large and aggressive Federal involvement in protecting the Nation's information systems; Libicki believes that the Federal Government can only play an indirect role in protecting private information systems and that a government deterrence policy could weaken the private sector's cyber defensive posture since it would transfer the responsibility for protecting systems from private owners to the government. As with Libicki's misguided confidence in system administrators, his argument is weak here as well. The Federal Government can and does have much influence over private sector communications infrastructure, and for there to be any reasonable level of protection of our Nation's critical infrastructure, the Federal Government must become heavily engaged and involved in securing it. There are many precedents for a more active Federal role in this context, such as the National Communications System and the Communications Assistance to Law Enforcement Act.

In the end, both *Cyber War* and *Cyberdeterrence and Cyberwar* cast light on important areas of cyber warfare that must be contemplated by researchers, military staff colleges, and policymakers at the national level. Neither Clarke nor Libicki is a cheerleader for offensive cyber capabilities, offering considered analyses on the difficulties inherent in their actual use. Instead, both demonstrate why the best offense may be a strong cyber defense, an important point when leadership considers resourcing decisions. Libicki and Clarke provide a great service in identifying important starting points and considerations for a discourse on cyber topics, and helping to nudge the discussion of the cyber domain to another level of maturity. But the question will remain: Is anyone listening? **JFQ**

Lieutenant Colonel Brian R. Salmans, USAF, Ph.D., is on the faculty at the USAF Air Command and Staff College. He is a cyberspace operations officer whose assignments have included computer network defense positions at the Defense Information Systems Agency's Department of Defense Computer Emergency Response Team and at U.S. Transportation Command.