superior to the chumps who fall for obvious cons. But the human capacity to believe and trust is vast, and let's face it: we all have fallen for something, whether it's the belief in a miracle cream or much worse—like losing your savings in a Ponzi scheme.

In Nate Hendley's *The Big Con: Great Hoaxes, Frauds, Grifts, and Swindles in American History*, this capacity for human credulity is on display. Hendley has compiled stories about common, bizarre, heartbreaking, and sometimes hilarious cons and con artists. This collection includes entertaining stories of man-bats on the moon (the original fake news), goat testicle transplants (meant to boost virility), the ubiquitous Nigerian prince e-mail (originally a Spanish prisoner letter), subliminal messages in Beatles songs ("turn me on, dead man" in "Revolution 9"), and more heartbreaking stories of baby-selling rings, scams that target the elderly, and fake investments that rob people of their savings.

Each of the eleven sections, focusing on topics like small cons, great pretenders, online scams, and para-abnormal fraud, contains detailed short entries and suggestions for further reading. The volume fills in the details of stories we've all heard of, like the hoax behind the book Go Ask Alice, and describes interesting scams like the Glim Dropper, which can only be performed by a con artist with one eye (certainly a niche market).

This book is immensely readable and a great resource for trivia nerds or those interested in human behavior. I would shelve it in nonfiction instead of reference, however, especially if your institution doesn't loan out reference materials: someone will want to check this book out and read every word. Recommended for libraries of all kinds.—*Tracy Carr, Library Services Director, Mississippi Library Commission, Jackson*

Encyclopedia of Cyber Warfare. Edited by Paul J. Springer. Santa Barbara, CA: ABC-CLIO, 2017. 379 p. $89.00 (ISBN 978-1-4408-4424-9). E-book available (978-1-4408-4425-6), call for pricing.

Great Britain was once the global power because it ruled the waves, but Germany ruled below the waves, and it almost won both world wars. Now the United States is the global power, but could the airwaves be our undoing?

The world remains innocent of an all-out cyber war, but cyber conflict has become routine. We read about cyber attacks on corporations, government agencies, and even the election system at home almost as often as reports of physical warfare abroad. Journalist Ted Koppel sent shivers through his readers with his book *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath* (Penguin Random House, 2015) when he conjured doomsday scenarios about the collapse of the American electric grid. This new work by Paul J. Springer, a professor of comparative military history at the Air Command and Staff College, is less sensational, but it still suggests ways America's economic and military superiority can be strangled by the Internet.

The single volume features a standard reference format of 223 entries by 59 authors arranged alphabetically by subject. The entries, which are largely focused on the experience of Western nations, include "see also" notes and suggested further readings. The front of the book has a guide to where specific topics can be found within broad subject areas. In the back, extra sections offer eight primary documents, a chronology, a bibliography, a list of contributors, and an index.

The entries will appeal mainly to academic or professional readers. They explain cyber conflict buzz terms—historical (Operation Shady Rat), technical (SQL Injection), bureaucratic (US Coast Guard Cyber Command), strategic (Cyber-Equivalence Doctrine), and biographical (Bradley—later Chelsea—Manning). There are also entries on certain pop culture topics, such as the 1983 movie *WarGames*.

Springer's encyclopedia follows his *Cyber Warfare* (ABC-CLIO, 2015). The older book is a more fundamental library resource. It contains full chapters on the history of cyber warfare and on the challenges and controversies facing those involved. It then provides perspective pieces by experts, profiles of key players and organizations, documents, resources, and a glossary. The newer work essentially expands on the profiles and glossary elements of the older one.

For readers ready to go beyond introductory material, an option is Paul Rosenzweig's *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (ABC-CLIO, 2013), which addresses key issues at more length. Perhaps even more than with most reference topics these days, however, a book about cyber warfare that is only four years old is already at risk of being out of date.

Fortunately, while not reference books, there are other more recent options. Among them are Fred Kaplan's *Dark Territory: The Secret History of Cyber War* (Simon and Schuster, 2016) and Brandon Valeriano and Ryan C. Maness's *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015).—*Evan Davis, Librarian, Allen County Public Library, Fort Wayne, Indiana*

Freedom of Speech: Documents Decoded. By David L. Hudson Jr. Documents Decoded. Santa Barbara, CA: ABC-CLIO, 2017. 207 p. $64.80 (ISBN 978-1-4408-4250-4). E-book available (978-1-4408-4251-1), call for pricing.

David L. Hudson's *Freedom of Speech: Documents Decoded* is another addition to the ABC-CLIO Documents Decoded series. Hudson, a prolific author of American legal issues, demonstrates his breadth of knowledge of the history of free speech in the United States in this volume. The Documents Decoded series volumes represent a new type of encyclopedia in which primary-source documents constitute the main texts. These primary-source documents are coupled with annotations by the authors that provide illuminating contextual information and situate the documents within broader events of the time. Hudson's *Freedom of Speech* follows this format and focuses largely on federal legal cases, but it also includes important speeches that either addressed