If you’re one of those people who thinks you’d be better off if you turned off your computer, unplugged it, took out the hard drive, chopped it into pieces, burned the pieces, and buried the ashes in someone’s yard twenty miles from your house, this book is for you.

Through its use of recent and not-so-recent history, it-could-happen-now scenarios, and just plain common sense, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare lays out a harrowing account of, well, digital espionage, crime and warfare. Author Joel Brenner spends nine chapters telling the reader all that has and could go wrong and then, thankfully, one chapter on “Managing the Mess.” Even that, though, tells us that the mess could be managed, not that it is being managed.

This interesting, well-written book is not pretty. But if you’re concerned about cybersecurity for your company, or agency, or government, or yourself, it is certainly enlightening.

Brenner, a member of the Virginia State Bar who practices law in Washington DC, knows what he’s talking about. He is a former senior counsel for the National Security Agency and served as the national counterintelligence executive in the Office of the Director of National Intelligence. At NSA he advised on legal and policy issues relating to network security. His legal practice focuses on privacy, data security, and related issues.

According to America the Vulnerable, network security is in sorry shape. The book opens with a question: “How did the Chinese manage to remotely download up to twenty terabytes of information from the Defense Department?” One would suspect that most of us didn’t even know the Chinese had done such a thing. Brenner knows, and he details the threats that this new type of espionage brings to our security.

We all know, or should, by now that anything we do on a computer can be found by anyone who is looking to find it. What Brenner so clearly demonstrates is that the same security issues that plague our laptops also afflict our government’s computers. The book is chock full of examples of cybersecurity failures.

With chapter titles like “Electronically Undressed,” “Bleeding Wealth,” “Degrading Defense,” and “Spies in a Glass House,” it is easy to come away from the book with a sense of foreboding. In one chapter, “June 2017,” Brenner lays out an imaginary scenario that starts with a conflict between China and Taiwan that ends with the Chinese electronically attacking U.S. power grids.

There is much here to contemplate. “America the Vulnerable” makes a strong case that the well-known WikiLeaks leaks were just the outer edge of what is a huge cyber soft spot. Killing our personal computers might give us a little more personal privacy, but it won’t make us any safer. We’re way beyond that.