

The NATIONAL STRATEGY FORUM REVIEW

An Online National Security Journal Published by the National Strategy Forum

America the Vulnerable

By Joel Brenner

Reviewed by Mark Frazzetto

Perhaps someone living a hermit's life in the Himalayas or Antarctica could claim not to be impacted or even care about digital technology's continuing transformation of the way of life in the 21st century. However, for those not living a hermit's life, Joel Brenner's new book, *America the Vulnerable* (New York: Penguin Press, 2011), is simply essential reading. In *America the Vulnerable*, Mr. Brenner describes how cyberspace, while providing great benefit, also contains a continuum of risk that spans the personal to the transnational. How the United States meets this challenge will go a long way towards determining the nation's fundamental security and prosperity.

America the Vulnerable begins by describing how electronic data has become "ambient." Nearly everything one does can be captured electronically. Individuals are watched by government and private security cameras, personal electronic devices signal our locations via global positioning satellites (GPS), and every time they click on a website, the activity is likely captured. Point of sale systems transmit what one buys at stores; this data is then aggregated, behavior patterns are identified, and the resulting information is used per the needs of whoever has the data, be it business or government. Ambient electronic data reduces marketing expenses, provides evidence for criminal investigations, allows public health officials to track disease, and generally makes life more convenient. While incredibly useful, technology has always been a two-edged sword. The cost of this convenience is a corresponding loss of privacy. For example, driver licenses, social security numbers, phone numbers, and almost every other personally identifying piece of datum are stored somewhere in cyberspace. This results in what Mr. Brenner calls "soft surveillance," and as Mr. Brenner points out, few of us are willing to give up the conveniences provided by ambient electronic data. Society demands this convenience, indeed finds it irresistible. Thus, everyone seems quite willing to be softly monitored.

Ambient electronic data is a virtual treasure trove, allowing merchants to tailor advertising to personal needs of individual customers and to stock merchandise according to what sells in specific geographic areas. Ambient electronic data allows banks and other financial institutions to consummate transactions with customers without having to pay human employees. Unfortunately, valuable things tend to attract the attention of criminals. According to Mr. Brenner, cyber criminals have hacked into the networks of big box retail chains, banks, and dot

coms. Cyber criminals put up 57,000 bogus websites onto which viruses and other malware are loaded in the hopes of infecting victims. Cyber criminals can be small time hoodlums or large scale, sophisticated international syndicates. Mr. Brenner also points out that, thanks largely to the anonymity that is built into the Internet, individuals usually have no idea who the cyber criminals truly are.

Mr. Brenner explains that the most vulnerable part of any network is the user. As one example, users download software designed to share large data files over the Internet. Unless configured properly, this file sharing software can open the gates of a computer network. Most computer users have no idea this can happen. Thus, Mr. Brenner points out, security does not work if it is left in the hands of the user. Further, a system is not secure unless the security is built into the system – i.e., a secure system would deny users the ability to download and install non-standard software in business and government networks.

In another section of the book, Mr. Brenner discusses national threats from cyber insecurity. He focuses on the activities of hackers who reside in China, although he makes clear there are many other players (such as hackers in Russia) as well. Mr. Brenner describes how Operation Aurora was launched from within China. Operation Aurora was a massive cyber attack launched against the intellectual property of thousands of companies in the West. Intellectual property is a primary target of Chinese economic espionage, much of which is conducted through cyber espionage. Hackers who engage in economic espionage, although ostensibly for private sector objectives, may (at times) be sponsored by government. The target of foreign economic espionage is often high technology that has applications in the private as well as the defense sectors. Thus, not only are defense and intelligence secrets pilfered but targets are also losing technology that represents that most important form of national wealth—innovation. The United States' economic security is threatened. As the downfall of the Soviet Union demonstrated, without economic strength, a large military, no matter how formidable, will not prevent the implosion of national power.

Mr. Brenner points out that China has been the world's dominant economic power for eighteen of the last twenty centuries, and seeks to reestablish its place in the international order – the “Middle Kingdom” whereby China is the regional power in East Asia. Direct military confrontation is unlikely given the strength of the U.S. military, but China and the U.S. are competing for power in other domains. As Mr. Brenner points out, cyberspace presents new opportunities for China to engage in this competition without resorting to overt military power. China can “prepare the battlefield” with the United States in a future conflict by planting malware in its various forms in key infrastructure and defense systems. Mastering cyber warfare techniques provides China with a competitive advantage over a powerful, albeit technologically dependent, U.S. military.

While *America the Vulnerable* discusses many different vulnerabilities in the American public and private sector networks, perhaps the most worrisome exposure lies within the nation's operational infrastructure systems. Operational systems are computerized control systems, as opposed to informational or transactional systems. Operational systems are used in areas such as industrial process control, robotic assembly, and most importantly, in infrastructure applications. Mr. Benner relates how a group of researchers, in a government sanctioned experiment, caused

an electricity generator to not only go offline but destroy itself. The researchers did this with computer, keyboard, and mouse. This experiment was done to show the vulnerability of the nation's electrical grid. For example, electricity utilities are connecting more and more of their operational systems to the Internet in order to increase efficiency. Unfortunately, these operational systems were intended to be isolated from contact with the world wide Internet. The result is that electrical power control systems have become highly exposed; in some cases, they can be accessed by a simple Bluetooth device. This situation is compounded by the fact that the type of power generator destroyed in the research experiment, and used throughout the electrical grid, is a type of heavy equipment that American businesses no longer make; they are only made in India and China.

America the Vulnerable is impressive in its scope. Mr. Brenner touches upon Wikileaks, how soft surveillance affects both intelligence agencies and private citizens, how technological convergence is leading to commercial information technology capabilities closer to those of military and intelligence information capabilities, and how citizens live in a post secrecy *and* a post privacy world. Through it all runs a common thread: information technology is changing the world at a breathtaking pace. Therefore, it is paramount to change how one thinks about protecting and managing information to better safeguard national security.

To this end, Mr. Brenner concludes with some thoughtful recommendations on how to improve cybersecurity in both the public and private sectors. Specifically, there are a set of recommendations for the United States government ranging from establishing regulatory standards on limiting electrical power systems' connectivity to the Internet to researching the possibility of redesigning the architecture of the Internet itself. Perhaps Mr. Brenner's most interesting recommendation is the creation of a civilian authority *above* the departmental (cabinet) level. Such authority would not be a coordinating "czar" but would rather be able to direct integration of the federal government's cybersecurity programs and policies. Mr. Brenner's recommendations for private enterprise focus on control, training and operations. They are the sort of nuts and bolts, common sense solutions that causes one to say, "Hey, why didn't I think of that?"

Mr. Brenner's book simultaneously provides a comprehensive review of and prescription for the American cyber strategy in the 21st century, and he does so in a clear, insightful way and with a refreshing sense of humor. *America the Vulnerable* is an important work. Those who are interested the strategies that underpin cyber security will find this book a valuable read.

Mark Frazzetto won the American Bar Association Law and National Security Writing Competition Award in 2010 for his paper titled [Protecting Against Economic Espionage: Trade Secrets, Standards, and Criminal Liability](#).