Book Reviews

America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare

By Joel Brenner

*Reviewed by Hartman Young**

> *[W]e have awakened to the fact that our national security depends heavily on privately owned critical infrastructure and our economic might -- assets that lie outside the defense-military-intelligence realm. Outside that realm the government isn't protecting us at all. If nonmilitary targets were attacked from abroad by land, sea, or air, the government would respond. But apparently this is not true when it comes to cyberattacks. This is a little noticed but momentous change in the oldest, most basic function of government, which is protecting the nation. Is this all bad? Maybe not. How could the government be responsible for protecting all our information systems unless we turned over control of all communications to the government? Perish the thought.*
>
> Joel Brenner, *America the Vulnerable*, p. 223.

America the Vulnerable, Joel Brenner's call to arms in our nation's ongoing cyber-crisis, is both a diagnosis and a potential cure. Brenner, who served as senior counsel at the National Security Agency as well as in other high-level government positions, knows first-hand the dire challenge facing our government when it comes to cybersecurity. Much of his book provides a detailed—and chilling—depiction of our nation's overall vulnerability to cyber-attack. Well-documented cases of attack—such as those involving the Chinese stealing twenty terabytes of information from the Department of Defense (an accomplishment they have surely surpassed by now) and the Chinese stealing the results of a $5 billion Navy program to develop a quiet electric drive for its submarines and ships (not to mention Chinese hackers stealing much of Google's source code), receive attention here. However, other causes for concern are also discussed in detail, such as the particular vulnerabilities exhibited by much of our electricity generation and banking infrastructure, and by our corporations in general. Brenner's "Primer on Cybercrime" chapter is particularly useful in explaining in detail some of the mechanisms by which data is stolen. Brenner's chapter "June 2017" demonstrates how attacks on our corporations and public utilities can have daunting strategic implications. The chapter provides a hypothetical scenario depicting a confrontation between the United States and China that demonstrates how an exploitable domestic electric generation grid could impact military decision-making. It also provides a discussion of the problems presented by counterfeit electronic parts and the perhaps even more opportunistic tactic of supply-chain attacks. However, Brenner points out that, at least when it comes to electronic sabotage operations, the United States is not without its own capabilities. But overall, Brenner paints a bleak portrait of the challenge that faces not only our military and intelligence services, but also corporations, public utilities, and private individuals.

The chapter "Thinking About Intelligence" is indeed the most thought-provoking, as Brenner raises profound questions concerning the nature of spycraft, intelligence, and governance. To illustrate the changes overtaking the intelligence trade, Brenner describes the 2010 assassination of Mahmoud al-Mabhouh, a Hamas military leader, in his hotel room at the Al Bustan Rotana Hotel in Dubai. On one hand the operation appeared to be a traditional (albeit lethal) intelligence operation. However, the only reason we know that is because of the unearthing of 648 hours of hotel surveillance video capturing many of the actions of the perpetrators (suspected of being Mossad agents), along with electronic passport, travel, and key-card entry records. The ubiquitous nature of these methods of surveillance could make "traditional" intelligence operations nearly impossible to accomplish surreptitiously in the future. In an age where camera and other types of surveillance are quickly becoming universal and constant, where newsgathering organizations (as well as individuals with smart phones) can send video across the globe almost instantaneously, and where open-source intelligence now often rivals the classified kind, governments must re-think their intelligence priorities, and indeed re-assess the role of intelligence agencies. A rational re-prioritization will likely cause the government to disinvest from certain traditional intelligence activities.

Despite the bleak outlook, Brenner has thought comprehensively about what to do about these problems, and prescribes concrete actions for both government and private industry. The proposals are practical and well-considered, although a number of them seem beyond the realm of current political possibility. In some ways, the prescriptions seem as current now as when they were proposed in 2011. In 2011, many thought that comprehensive cybersecurity legislation was on the horizon, and that in any event private businesses would organize and adopt standards of their own. Largely, however, only piecemeal changes have been adopted. There has been no comprehensive legislation, and our corporations continue to be raided at an alarming rate. Brenner's prescriptions are therefore still very current and should be taken seriously by policymakers.

Brenner divides his prescriptions into things that the government should do and things that the private sector should do. In the government arena, Brenner calls for several reforms. Perhaps the key prescription here is to use the government's enormous purchasing power to require higher security standards of its vendors. On one level, this makes sense. The government has made some limited progress in the government contracting realm since *America the Vulnerable* was published in 2011, but it falls well short of what is needed. For example, Section 941 of the National Defense Authorization Act for 2013 requires DoD to establish rapid reporting requirements for cleared government contractors (defined broadly as those handling classified information) to report cyber intrusions on their networks. As of this writing, these particular reporting

**Hartman Young is an Attorney Practicing in Washington, DC.*

requirements are still within the regulatory process. Also, it should be noted that although the reporting requirements will help DoD and industry share information once a breach has occurred and perhaps even prevent future breaches, it is subject to the criticism that it is largely an example of guarding the henhouse after the fox is far away. On the other hand, the procedures DoD will establish will provide DoD with access to equipment or information of a cleared defense contractor so as to conduct forensic analysis. This may have a salutary effect going forward. In addition, DoD has provided additional guidance to its Defense Industrial Base (DIB) participants in 2012. Under this voluntary framework, DIB participants are to report cyber breaches to the government, and the government in turn shares cyber threat information with DIB participants. Another rule provides standards regarding the safeguarding of unclassified controlled technical information and reporting the compromise of such information. This regulation was issued in final form in November 2013. Although measures such as these may help at the margins, they are piecemeal approaches and do not rise to the level of the more comprehensive approach for which Brenner is advocating.

Brenner advocates a much broader federal approach. This would include forbidding federal agencies from doing business with any Internet service provider (ISP) that is a hospitable host for botnets, and publicize the list of such companies. He would also require ISPs to notify customers whose machines have been infected by a botnet. Here Brenner argues that we can no longer allow ISPs to hide behind the mantle of "privacy" in not doing more to protect users from botnets. Brenner argues that ISPs should be permitted to block traffic from infected customers according to a subscriber's wishes, but also that government should *require* ISPs to flag all such traffic, so others can refuse to accept it. He also would have Congress direct the Department of Justice and the Federal Trade Commission to definitively remove the anti-trust concern when U.S.-based firms collaborate on researching, developing, or implementing security functions. Congress should also direct the Federal Energy Regulatory Commission (FERC) to require the North American Electric Reliability Commission (NERC) to establish standards that limit the ability of utilities to connect their industrial control systems directly or indirectly to a public network. Finally, Congress should change the Internal Revenue Code to incentivize corporate investment in cybersecurity.

In terms of securities regulation, Brenner argues for toughening public audit standards for cybersecurity. It should be noted that since the book's publication in 2011, some developments have occurred that have impacted corporations' public disclosure of cyber incidents. One example is the SEC Division of Corporate Finance's October 2011 guidance concerning disclosure obligations relating to cybersecurity risks and cyber incidents. Certain congressional leaders such as John D. Rockefeller IV, Chairman of the Senate Commerce Committee, have requested that the SEC make its guidance more formal by issuing it at the Commission level as opposed to the Division level.

Brenner also highlights a number of areas that need federal research dollars. First, research into better attribution techniques and identity standards is warranted. Here, Brenner calls for "a robust public-private research into better attribution techniques" so as to better solve what Brenner calls the "attribution problem"—simply knowing what machine launched the attack or the malware, who was at the keyboard, and, finally, what they were looking for. He also advocates research into verifiable software and firmware, and into the potential benefits of moving more security functions into hardware. Interestingly, Brenner believes more research into the feasibility of an alternative Internet architecture is necessary because insufficient progress (at least in terms of what has been publicly reported) has been made over the last few years. Brenner quotes Joe Markowitz, a former director of the CIA's Community Open Source Program Office, as advocating jettisoning "IP"—the current internet protocol—in favor of "a stratified network where we take the control channel out of the subscriber space." Although such a change would be "hugely expensive," Brenner's point is that we need to fund the critical research now in order to pave the way to harden at least some currently internet-dependent systems.

Rounding out his federal approach, Brenner argues that "[t]he United States should engage like-minded democratic governments in a multilateral effort to make Internet communications open and secure." Here too, real progress has proven elusive.

In the corporate realm, Brenner is pithy in his prescriptions, as he clearly believes that corporations could do a much better job—on their own—of protecting their networks. The prescriptions sound simple (each followed by a short narrative): "clean up your act," "control what's on your system," "control who's on your system," "protect what's valuable," "patch rigorously," "train everybody," "audit for operational effect," and "manage overseas travel behavior." The devil, however, is in the details. No doubt numerous corporations have stepped up their compliance and cyber-hygiene regimes, and have made the necessary investments to assure the integrity of their supply chains, but many have not, as the theft of our corporations' secrets continues apace.

America the Vulnerable is useful as a call to action to address our nation's cybersecurity problems. As such, it serves a role similar to Richard A. Clark's *Cyber War* and Stewart Baker's *Skating on Stilts.* At this point in 2014, what we all have at stake should be clear. What is to be done about the various cybersecurity problems is less certain. Given the worsening nature of the threat, one wonders if even Brenner's prescriptions would be adequate. However, as Brenner convincingly points out, a concerted effort by government, industry, and individuals is necessary.

The passage at the beginning of this review demonstrates Brenner's recognition of the uneasy tension between security and liberty that lies at the heart of the cyber problem. Brennan has proven prescient in recognizing the dangers inherent in granting the government too much control over private communications. Brenner could not have foreseen the disastrous handling of, and resulting uproar over, the recent revelations concerning various NSA surveillance programs. Brenner's book was published after Julien Assange and Wikileaks became an issue (therefore Brenner discusses each within a broader discussion of leaks and the changing nature of intelligence gathering), but before Edward Snowden, an NSA contractor employed by Booz Allen Hamilton, began leaking highly classified details of NSA surveillance programs to *The Guardian* newspaper. The briar patch to which Brenner alluded—stemming from increasingly comprehensive government access to far more private communications than anyone had previously imagined—is now front and center. Many recent books and articles regarding cybersecurity promote the idea that the government needs more tools to ward off the next wave of cyberattacks. This may well be true. Irrespective of the degree of support one might have for comprehensive cybersecurity legislation, the more general view that the government needs to do a better job in the cyber arena is well justified. However, it is also true that granting the government more access and control over communications comes at a significant cost, as dozens of the revelations concerning the NSA make clear. Indeed, as we move forward in addressing our nation's cybersecurity vulnerabilities, we need to be cognizant of the cyber risk presented from within our own government. It would be a tragic irony if, in an effort to fortify the United States against cyber-attack in order to protect her militarily, fiscally, and culturally, our nation instead came to resemble East Germany during the Cold War. For that reason, one hopes that future works addressing the cyber problem will address this often difficult to observe but nevertheless critical aspect of the problem.