
Mark T. Peters II

USAF, Retired

Follow this and additional works at: https://digitalcommons.usf.edu/jss

pp. 122-125

**Recommended Citation**
DOI: https://doi.org/10.5038/1944-0472.16.2.2141
Available at: https://digitalcommons.usf.edu/jss/vol16/iss2/8

This Book Review is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

This book review is available in Journal of Strategic Security: https://digitalcommons.usf.edu/jss/vol16/iss2/8
Cybersecurity frequently becomes the bogeyman within modern political discussions focused on organizational change. Larry Clinton, as editor, gathered opinions in *Fixing American Cybersecurity* (2023) about federal and industry approaches to cybersecurity challenges. The book identifies current problems, proposes a solution, and then allows several Cybersecurity and Infrastructure Security Agency (CISA) defined critical infrastructure sectors to pontificate on unique problems. The different authors highlight the ongoing lack of strategy, structure, and resources to systemically combat criminal and national threats to US digital infrastructure. Proposed solutions include a recommendation of a central government agency to control and implement strategy through incentivizing users, modernizing policies, and economizing by implementing national digital protection laws. Overall, the book repeats previous government strategies of adding new regulations and agencies to an already complicated area.

The book’s thesis states the US government’s approach to cybersecurity is deeply broken and requires a new path to fix problems by creating a new agency. Starting with four chapters of explication, the text details China’s digital strategy, systemic cyber risk, and how the US government fell behind. The hypothesized solution creates yet another government cybersecurity agency, the White House Office of Digital Strategy and Security (ODSS). This agency would be separate from the current National Cyber Director (NCD) in that the NCD would lead federal policy and coordinate national response while the ODSS would proactively craft, assist implementation, and evaluate the overarching strategy’s success. This addresses competition with a Chinese, state-run, cyber offensive by adopting a common US strategy and consolidating currently disparate strategies. The biggest problem remains that creating a new agency would solve all the problems that previous agencies were created to solve did not.
Clinton divides the book into two sections but three would fit better with a statement of the problem, solution proposal, and the state of current CISA infrastructure sectors. The explanation starts with a generalized approach, examines how China solved internal problems, discusses systemic threats in the Solar Winds attack, and highlights US policy failures. The core incentive behind cyberattacks appears economic, an analysis tying with my own and other’s research. The Chinese approach, while labeled as unethical, blends economic and political power by partially nationalizing commercial firms while supporting their growth through intelligence activities and conducting cyber-piracy. In the United States, this corresponds to using the CIA and NSA to steal proprietary information from firms competing with US companies to increase national economic gains. The Solar Winds example, Russian malware on a federally contracted, US corporate system, highlights the inability and unwillingness of most corporations to systemically address cyber risk factors. Factors correlate in the last element, detailing current US regulation failures and referencing how highly regulated cybersecurity performance in finance and healthcare sectors are routinely worse than performance in automotive or manufacturing sectors (p. 60).

The next two chapters move from reinventing cybersecurity to implementing policy favored by authors. As mentioned above, the solution creates a new agency, the ODSS, to guide federal strategies. This agency advances from current solutions in the Information Sharing and Analysis Centers (ISAC) to a more modern partnership. The ODSS is intended to create a new social contract between federal and private organizations to combat multi-level cybersecurity threats. The proposed solution exhaustively describes the incentivize and modernize portions while only touching on “economize” proposals. Incentivization relies on establishing qualifiers to earn the incentive, ensure industry appropriateness, and be economically powerful enough to change behavior. “Modernize” hits on standard topics by improving legal standards, law enforcement responses, and community cyber education practices. “Economize” suggests streamlining regulatory structures and implementing national data protection similar to the EU’s General Data Protection Regulation. However, improving regulation while adding multiple new laws represents contrasting ideas.
The book’s last section invites seven different industry sector experts to comment on challenges and solutions within their specialty. Each section emphasized a slightly different approach. The health, finance, and retail sections dealt primarily with reducing criminal data theft. As an example, the health industry has lost 300 million patient records since 2015, but tele-health increased from 14,000/week pre-pandemic to over 1 million a week during its height, greatly accelerating cyber risks (p.124). This compares with an interesting retail chapter statistic that over 80% of individuals visiting e-commerce sites are hackers with stolen credentials (p.175) The defense sector focused on improving contractors through accelerated and detailed compliance scoring. The telecommunications and energy sectors’ greatest concern was the co-opting of their services by adversaries such as China. The section outlier was the Information Technology chapter which focused entirely on Communications Decency Act (CDA) Section 230 implications. CDA 230 establishes that communication platforms like Facebook and Twitter are not responsible for published content.

The book’s biggest fault was that the sectors were not held to a consistent outline. As mentioned, each sector approached a different goal, in a different manner. This reinforces one of the biggest problems in cybersecurity as every participant views challenges from a personal angle. The sectors reflect a self-serving bias, as they address personal experiences and ran counter to the book’s thesis supporting creating an over-arching federal strategy agency. A better fit here would have been to ask the sector representatives what the US government could do to incentivize, modernize, and economize sector cybersecurity approaches. That would have provided a common baseline for reader comparison.

Overall, Fixing American Cybersecurity (2023) becomes yet another exercise in suggesting a government solution to a complex problem. The book does mention that government solutions often take too long to implement and are outdated on arrival which is greatly exacerbated in cybersecurity. The cybersecurity topic needs answers, but technology’s fast pace means the US government will likely be significantly behind commercial industry solutions. One can examine regulation problems with cryptocurrency, data rights, and social media platforms as an example of current government failures to keep pace. The book offers a quick read, but not much as a new approach, unique solution, or even a
clear path forward. I would recommend this book for an airline trip if you have time, but most cybersecurity professionals or business experts can likely skip this one.

---