Nuclear Weapons and International Security: Collected Essays

The essays collected in Nuclear Weapons and International Security allow the reader to follow the thinking of nuclear and peace studies scholar Ramesh Thakur from the late Cold War years to the present day. In several of the essays, Thakur writes compelling and rigorous analyses of the Indian nuclear program, covering issues such as India’s regional security environment and “[t]he inconsequential gains and lasting insecurities of India’s nuclear weaponization.” He identifies as an Indian expatriate, but in an interesting footnote, he vigorously contests the notion that his name implies any bias in India’s favor. In another section, he examines nuclear-weapon-free zones, the state of the nuclear Nonproliferation Treaty (NPT), and potential solutions for “global governance disconnects” that hinder the growth of an effective global nuclear security regime. Thakur argues that the NPT’s central bargains are “under strain” and that the treaty suffers from “congenital defects, built-in flaws, ripening contradictions and increasing fragility.” He maintains that an emphasis on the humanitarian consequences of nuclear weapons use may be the best way “to generate political momentum for the nuclear disarmament cause.” Thakur concludes that progress on NPT Article VI disarmament obligations is essential and calls for a nuclear weapons convention that will achieve “verified destruction of all nuclear stockpiles within our lifetime.”—NATHANIEL SANS

Cyber War Versus Cyber Realities
Brandon Valerino and Ryan C. Maness, Oxford University Press, 2015, 266 pp.

Cyber War Versus Cyber Realities attempts to uncover “the realities and dynamics of state-to-state cyber conflict” through quantitative analysis. Authors Brandon Valerino and Ryan C. Maness, professors who study the issue of cyberconflicts, present evidence that suggests “restraint” is the current norm for state behavior in cyberspace and predict that this will continue to be the case well into the future. Valerino and Maness cast their evidence as a counterargument to the “cyber hype” that often makes headlines today, namely, that large-scale cyberconflicts capable of destroying a state’s critical infrastructure are inevitable. The authors point to “restraint mechanisms” such as the risk of potential harm to civilians, the possibility for a cyberattack to hit unintended targets, and the potential for technology behind cyberweapons, once used, to become widely available as the main reasons why states do not engage in high-stakes cyberconflict. International systems that further emphasize restraint in cyberspace will begin to emerge, Valerino and Maness say. They argue that to stop the worst-case scenarios from taking place in cyberspace, policymakers need to understand and frame the current state of cyberspace activities based on the realities of the actual threats. “Overstating the threat is dangerous because the response could then end up being the actual cause of more conflict,” the authors write. They maintain that if states believe “fear-based hype” and develop offensive cyberweapons in the belief that they will deter future attacks, “cyberspace is doomed.”—TIMOTHY FARNSWORTH

Source URL: https://www.armscontrol.org/ACT/2015_0708/Books-of-note