The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age
Adam Segal (PublicAffairs, 2016), 320 pp., notes, index.

Reviewed by Jeffrey I.

The year between the June 2012 *New York Times* publication detailing an alleged Western cyber operation targeting Iran and the *Guardian*'s June 2013 publication of the Snowden leaks marked a significant shift in the international order. In these 12 months, the illusion of the internet as an ungovernable information utopia was shattered.

A less romantic vision took its place. Far from being an anarchic asylum guided by nationless hackers and idealistic entrepreneurs, the internet was revealed to be a place where security services and intelligence agencies had thoroughly penetrated, another arena for old international rivalries to play out. By the end of the summer of 2013, the world came to understand it was organs of state power—with mundane monikers like Tailored Access Operations and Unit 61398, not teenage super-hackers or technology adept activists—who were the most powerful actors in cyberspace.

Public denials and rebukes aside, undoubtedly many foreign governments knew the broad outlines (at least) of America's activities in cyberspace prior to the summer of 2012; however, the revelation of these activities to their constituents caused a swell in domestic pressure for leaders to address issues of privacy, sovereignty, and the role of information technology as an instrument of national power. What had been a niche national security or counterintelligence concern (or opportunity for intelligence sharing) was now a mainstream political issue and a matter of foreign policy. Cyberwarfare and computer aided espionage had left the shadows and become an overt tool of diplomacy and subject of public debate.

In his book *The Hacked World Order*, Council of Foreign Relations chair Adam Segal explicates the impact of these 12 months—what he refers to as "Year Zero"—on the international order, and the role computer network exploitation and cyber-operations have since played in foreign policy. Beginning with "Year Zero," Segal creates a well-thought-out strategic map of cyberspace, contrasting the different perspectives, motivations, and justifications of the various players. Throughout his book, Segal pegs his analysis to established foreign policy narratives: the rise of non-state actors, the decline of American power vis-à-vis China, and the shifting of economic and political centers of gravity to the Global South. These familiar narratives will serve to help orient readers new to cyberspace issues. They also suggest one of the central themes of the book: conflicts in cyberspace today are largely an extension of conflicts playing out in traditional foreign policy arenas. The role of cyber power has so far been limited in international conflicts, though its importance is rapidly increasing and will continue to be a source of significant strategic uncertainty.

Segal spends considerable time emphasizing the unpredictability of cyber weapons. They may fail to execute properly, spread to untargeted systems, or wreak significantly more havoc than intended. Furthermore, cyber weapons are difficult to use as a deterrent. As Segal puts it: "You cannot march cyber weapons in a parade or detonate them over a Pacific atoll." (108) Finally, many cyber weapons have a short shelf life as well as an erratic development schedule, compared to traditional munitions. "Exploits," the heart of most cyber weapons, can be patched at any time and there is no guarantee that a newly discovered exploit will have the same capability as one on the shelf.

The strategic advantage presented by new cyber weapons is often a "use-it-or-lose-it" proposition. All these factors make applying traditional theories of use of force difficult in cyberspace. They also make this a particularly dangerous time—as norms for use of cyber weapons continue to be established—for misunderstandings and unintended escalation. "Policymakers have lost a sense of strategic stability, predictability, and control," Segal explains. (265) From Segal's perspective, the ongoing lobbying by the American private sector for legal authority to retaliate against, or "hack-back," intellectual

property thieves, state-sponsored or otherwise, will only make this situation more precarious.

Because they pose significantly fewer risks for the attacker than cyber weapons, psychological warfare operations in cyberspace constitute a realm in which some actors feel much more comfortable aggressively operating. The author cites Russia as a particularly aggressive user of the internet as a medium for influence operations. According to Segal, however, the Russians don't believe they started the information war: "Russian politicians and military leaders see themselves as victims of information attacks from Western media, NGOs, and the internet itself." (81)

A weakened Russia, feeling threatened by NATO encroachment and increasingly reliant on what it feels is a Western-dominated internet may be fighting back the only way it can. Russia's well-publicized use of automated social-media posting ("bots") and paid commenters ("trolls") is designed not to present a counter-narrative, but to crowd out thoughtful conversation and spread confusion. Psychological warfare and influence operations have been used against a wide variety of Russian rivals. A coherent strategy on how to respond to these operations, which don't reach the threshold of armed conflict, has yet to be established. These operations are integral to Russia's war-fighting strategy and have been used in conjunction with cyber weapons in its military campaigns in the Ukraine and Georgia.

In addition to the military use of cyberspace, Segal covers the ongoing conflict over the future of internet governance. America's position, logically and physically, at the center of the internet has given it unique economic and military advantages. International rivals like China and Russia perceive that the motivating force behind America's efforts for a free and open internet is protecting those advantages. Our adversaries counter the American push to maintain an open internet with insistence that cyber-sovereignty be respected. While acknowledging the economic advantages of an open internet, China and others view domestic stability as the higher priority. What the United States sees as efforts to limit internet freedom and restrict the flow of information, others view as de-Americanizing it and claiming their cyber-sovereignty. Segal posits that some Europeans, who would have been sympathetic to US arguments, were dissuaded by the Snowden revelations, interpreting our calls for internet freedom—much like China and Russia—as the cynical defense of a hegemonic status quo.

Despite some shortcomings (a distracting, inconsistent style usage suggests the book could have used another pass by the editor, and the assessments of US capabilities seem to be largely taken from news media analysis of Greenwald-curated leaks), this is worthwhile read for any intelligence officer looking for a primer on strategic cyber issues. The information in this book will serve as a solid foundation for regional- or target-specific research and help put more focused information in perspective. Approaching cyber from a foreign policy perspective with a wide aperture makes this work accessible to a diverse audience; both the technically inclined intelligence officer and his better dressed colleague across the river will find something useful here.

❖ ❖ ❖

The reviewer: Jeffrey I. is a consultant supporting the National Security Agency. His work focuses on understanding emerging technologies.