



Digital
IR

Book
Review

June 2021

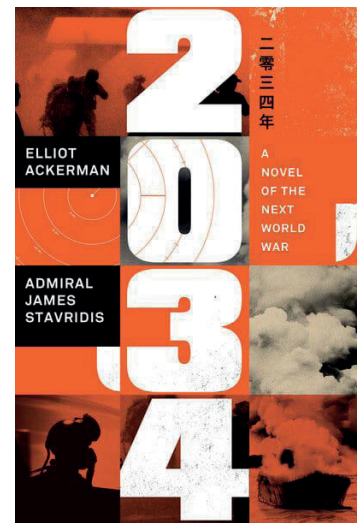
2034: A Novel of the Next World War

REVIEWED BY KENDRICK CHAN


In their recently released book *2034: A Novel of the Next World War*, Elliot Ackerman and James Stavridis sketch out in detail what great power military conflict in the near-future will look like. Yet beyond being a mere Tom Clancy-style thriller, the book sends a cautionary message to its readers: in today's digital age, there is a pressing need to find a way to avoid sleepwalking into war.

The book opens in the year 2034, with many of today's geopolitical disputes still largely unresolved—the South China Sea still remains a flashpoint, and so is the issue of Taiwan. It is therefore unsurprising that the initial clash between the United States and China takes place during one of the US Navy's Freedom of Navigation Operations (FONOPS) in the South China Sea. However, rather than describing the technicalities of how it is done, the authors do a good job of showcasing the significance of the digital domain and the vulnerable nature of command and control (or C4ISR, for the whole spectrum) systems through the eyes of the book's characters. The very same digital components that make future military systems so efficient and deadly now prove to be a lethal vulnerability. US Air Force pilot Major Chris "Wedge" Mitchell has his F-35 plane electronically hijacked and involuntarily landed in Iran on a routine flight in the Middle East, while US Navy Commodore Sarah Hunt loses her ability to communicate with the rest of her flotilla at the same moment the Chinese Navy engages them in combat. US Deputy National Security Advisor Sandeep Chowdhury fares no better, finding both his mobile phone and computer compromised in the midst of a crisis situation. Through a combination of cyber cloaking and satellite spoofing, the Chinese are able to deny the US military the precise coordinates needed for targeting the Chinese forces invading Taiwan. It is via this way that the Chinese military successfully launches a crossing of the Taiwan Straits and capture Taiwan.

Beyond the military examples, the authors also highlight how much of society relies on key digital infrastructures to function. The sabotage of a few undersea cables by the Russian Navy causes the United States to



'Beyond the military examples, the authors also highlight how much of society relies on key digital infrastructures to function.'



‘The importance of human connectivity in the conduct of international relations also appears occasionally alongside digital connectivity.’

suffer a ‘cyber Pearl Harbor’ as large-scale havoc is wrecked throughout the country. Beyond just losing internet connectivity, the entire United States also experiences a power outage, which in turn causes airport closures and panic on the stock market. This highlights the increasing vulnerability that states may very well find already themselves in. Interestingly, despite the sabotage being carried out by an opportunistic Russia, ongoing US-China tensions meant that the attack was perceived to be Chinese in origin, leading to a series of tactical nuclear exchanges between the United States and China. Social media and its mobilizing potency also get a mention in the book. The #FreeWedge hashtag trends on social media follows his capture, inflaming the emotions of the entire country and placing immense pressure on the American President to act.

The importance of human connectivity in the conduct of international relations also appears occasionally alongside digital connectivity. Chowdhury’s uncle serves as an admiral in the Indian Navy and their relationship enables Chowdhury to engage in some behind-the-scenes Track II diplomacy with the Iranians. Chinese admiral Lin Bao (a key character in the book) is of dual parentage (his mother is American) and fondly recalls his training at the US Naval College and Harvard Kennedy School as he reluctantly carries out a particularly dire military order, vowing to retire once it was followed.

Overall, the value of the book lies not with how it envisions a great-power war in 2034 might occur. Rather, its value lies in forcing its readers to grapple and rethink the relationship that countries and societies have with digital technology. This is pertinent, given that we are entering age where digital technology plays an increasingly important role in the conduct of international relations. Cyber capabilities, as displayed in the book, may very well be a two-edged sword. They might turn the tide of battle for a state in one scenario but cause it to suffer unacceptable losses in another. In the book, the same cyber and stealthing capabilities that the Chinese used to successfully invade Taiwan were also (unknowingly) possessed by India, who would utilize those capabilities to sink the flagship Chinese aircraft carrier Zheng He. How then should such game-changing capabilities be managed? In contrast to nuclear arms, “cyber” still remains a nebulous concept and without any reasonable metric to measure cyber weapons/capabilities, some form of “cyber arms control” will be extremely unlikely. The same can be said of the digital infrastructure powering the internet. While states whose societies enjoy high levels of internet access and connectivity can reap the economic and convenience benefits the internet has to offer, increased connectivity may mean increased risks if potential vulnerabilities are left unaddressed. It is with this in mind that credit must be given to authors Ackerman and Stavridis, for the book provides an excellent entry point for readers to think about the digital technology and its impact on great power competition in the world of the future. ■