# BOOK REVIEW

The Wires of War: Technology and Global Struggle for Power, Jacob Helberg,

(Avid Reader Press/Simon & Schuster, 2021) 384

2

## The Wires of War: Technology and Global Struggle for Power, Jacob Helberg,

## (Avid Reader Press/Simon & Schuster, 2021) 384

In the last thirty years, emerging technologies have transformed the character of war. Cyberspace has now become an additional battlefield. Cyberattacks to sabotage a state's critical infrastructure, cyber espionage to get sensitive information and Internet for fire-hosing or flooding for propaganda and misinformation have posed several new challenges to states' security. Moreover, the increasing threat of ransomware has become a major concern around the globe. Ransomware attacks on Colonial Gas Pipeline, JBS Meat, and software supply chains such as hacking SolarWinds aggravated cybersecurity concerns across the US. These attacks also led to the issuance of National Security Memorandum to improve cybersecurity for national security by President Biden.

In his book *The Wires of War: Technology and Global Struggle for Power*, Jacob Helberg discusses the use of technology driven instruments by states in their struggle for power. He terms Internet as the new theatre of geopolitical conflict. According to Helberg, the 21st century wireless war is being fought between autocracies and democracies. He regards China and Russia as major autocratic actors.

Helberg was appointed as Google's global lead for news policy in 2016. During this time, he fought against propaganda, disinformation, and foreign interference in US elections. The *Wires of War* is a detailed account of author's personal experiences and insight while serving in Silicon Valley. The book also provides an understanding of the nuanced issues about which only a few had knowledge. It discusses emerging technology in the context of “gray war” and how it is affecting the 21st century. The author argues that the algorithms that govern our online lives “may be one of the most powerful radicalizing instruments of the 21st century.” He recollects that some experts had predicted that the Internet’s buoyant freedom of expression would have an adverse impact on autocracies. However, that has not happened. Instead, the Internet has multiplied misinformation manifold. A single click now displays thousands of bizarre and fake ideas, assumptions, opinions, and stories. Ironically, these false stories spread six times faster than the actual news as research reveals.

The author defines flooding or fire-hosing as the process in which the Internet is flooded with misinformation due to which it becomes difficult to distinguish between authentic and fake information. Helberg points out how the culture of skimming through Google to verify a truth has widely spread in the digital age. The book also discusses how users’ overdependence on Internet, and their online behavior make their personal information accessible. The author refers to research conducted by Michael Kosinski who found that it takes only 68 Facebook likes to establish a person’s race, gender orientation, and political affiliation.

Helberg has also analyzed the so-called spread of “fake news” by Russia’s Internet Research Agency and explains how advancement in artificial intelligence, data gathering, and synthetic media such as deepfakes could accelerate propaganda and disinformation campaigns that will have graver consequences in the future. He is overly concerned about China’s technological advancements but completely ignores the use of propaganda and cyberattacks by the US.

Readers also get a recap of the debates about NATO’s mutual defense treaty and whether taking down Internet infrastructure constitutes an “attack” under Article 5 of its charter; the advancement in Chinese technological infrastructure from Huawei’s communications devices to Apple's iPhones made in China; and the threat of hackers shutting down power sectors of major cities.

Helberg is of the view that cyber aggression or ability to launch cyber war against any country would be contingent on that country's military strength or other elements of national power. Instead, he believes that the ownership of channels that spread information to billions of people, and data access will be significant factors for cyber warfare. He proceeds to trace how modern-day warfare could potentially undermine infrastructure, economies, privacy, innovation, cultures, and norms.

The author suggests that the US must rebuild its national strength to counter the perceived threats of cyberattacks, propaganda, disinformation, espionage, or foreign interference. He proposes appropriate investments in areas of innovation and technology to let government and private sector build new high-tech manufacturing centers while securing their back end and enhancing competitiveness. In a grey war, according to Helberg, the best offence boils down to a strong defense.

***Reviewed by Areesha Anwar, Research Officer at the Center for International Strategic Studies Sindh (CISSS), Karachi.***