Reviews

Digital Influence Warfare in the Age of Social Media. By James J. F. Forest. Santa Barbara, CA: Praeger, 2021. Pp. vii+303. $77.00 (cloth). ISBN 978-1-4408-7009-5.

When it was discovered that Russia had interfered in the 2016 US presidential election through digital means—seeking to damage Hillary Clinton's campaign, increase Donald Trump's chances of election, and create political divisiveness—people became aware of just how powerful online tools and techniques could be in influencing personal thinking and decision-making. The report from the special counsel indicated that a Russian operation was in place from 2013 to 2017, and it involved creating a troll farm of thousands of fake social media accounts supposedly representing people with extreme political ideas. These accounts were used to spread false and provocative information through social media. Through this operation, other methods such as those involving hacking were used as well.

In his new book, James J. F. Forest refers to this kind of operation as a kind of "digital influence warfare." Forest addressed this topic to some extent in his 2009 book, *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in the War of Ideas* (Praeger). With the explosion of social media on a global scale, the situation is now more problematic and complex, with a much broader range of participants. Now people and groups beyond terrorists and governments are utilizing social media to influence the thoughts, beliefs, and actions of others.

Forest is a professor in the School of Criminology and Justice Studies at the University of Massachusetts Lowell, and he has written more than 20 books, including *Intersections of Crime and Terror* (Routledge, 2013); *The Making of a Terrorist: Recruitment, Training, and Root Causes* (Praeger, 2006); and *Countering Terrorism and Insurgency in the 21st Century* (Praeger Security International, 2007). In previous years, he served as the director of terrorism studies at the US Military Academy.

This new book is part of the Praeger Security International series, which examines some key security topics, such as terrorism, cyber warfare, and food security. The series is intended for professors, policy makers, and students and provides insights into issues related to these important subjects, considering them in the broad international context. In Forest's contribution to this series, he also wants to inform general readers.

The author notes that one reason he wrote this book was because of his encounters with intelligent acquaintances and friends who expressed thoughts and ideas that he knew were untrue and could not be supported by factual evidence. When he then provided factual evidence that their ideas clearly were untrue, they remained unconvinced and continued to affirm these ideas

The Library Quarterly: Information, Community, Policy, volume 92, number 4, October 2022.

and share them with others. Another reason he wrote the book was in response to new developments taking place, such as the Russian interference in the 2016 election and the efforts of radical right-wing groups using social media to spread falsehoods and dissention.

The association among information, social media, and warfare, as indicated in the book's title, might appear to be somewhat exaggerated. People generally know that much personal information can be found online and that advertisers use this information to target their ads effectively and persuasively. However, the situation is much more extreme than this. As Forest notes, "You, the potential target of the influence attempt, can be identified by a broad range of data, including your IP address, allowing data analytics to establish patterns of behavior and patterns of preference for and reactions to online information that can be captured, stored, and converted to decision-making algorithms" (162). Those making use of this information do not just seek to influence what products people purchase but also to shape and manipulate their beliefs, values, and personal commitments. They want to gain control over people.

Librarians and others find digital resources and information on the internet to be essential aspects of their work. Because they use this information in constructive and helpful ways, it is difficult to imagine that others weaponize information, using it in such destructive ways. Both governmental and nongovernmental agents (e.g., terrorists and extremists) use social media and other online sources to with great effectiveness, in substantial part by creating information silos. Using personal information of many kinds, along with other data, they create groups of people who share, for example, beliefs, values, and concerns. These agents then use tools of persuasion to shape and guide people's thinking and commitments, particularly in ideological ways. Those in these information silos are usually unaware of the extent to which they are being manipulated.

The book comprises seven chapters, with the first one introducing digital influence warfare—that is, any online method used to persuade other people to think or do something. It is warfare in the sense that there are attackers and targets and that specific operations are carried out. Forest identifies three kinds of digital influence warfare: psychological, informational, and political operations. Various kinds of attackers are involved in this type of warfare. Nations, terrorists, insurgents, and representatives of extremist movements all are actively at work, and they are increasingly disruptive to liberal democracies. Forest provides several examples of digital influence warfare, including several perpetrated by Russia. He also discussed efforts undertaken by China, such as those attempting to undermine the democracy movement in Hong Kong and to use disinformation to discredit leaders in Taiwan. He noted that this book is "about the intersection of human behavior, beliefs, technology, and power" (27).

The second chapter addresses different goals to be accomplished and strategies that are used. Forest lists several possible goals, such as strengthening political support, increasing conspiracy thinking, undermining governmental institutions and leaders, delegitimizing governmental

processes and voting results, fomenting societal and political discord, and creating suspicion toward media organizations. Taken together, the goals relate primarily to power. In developing strategies, attackers gather data on their targets—much of which can be obtained online—that indicate their values, commitments, and interests. With this information, they can focus their message (similar to the way that Google does) and use methods of influence related directly to these specific elements. Forest notes that while these goals and strategies might involve one nation targeting another, an important segment of it is nations focusing on groups or people domestically. He provides examples of this kind of action taking place in several countries, including Ethiopia, Guatemala, Vietnam, and the Philippines.

The third chapter shifts to specific digital tactics and tools used to influence others. These can be divided into three categories: those used (*a*) to deceive, (*b*) to provoke engagement, and (*c*) to attack targets directly. Some tactics used include spamming, spreading conspiracy theories, restricting available information, flooding with disinformation, falsely criticizing opponents, hacking and disseminating documents, manipulating algorithms, and using scare tactics. As social media becomes increasingly influential, these methods become more diverse and effective.

The fourth chapter focuses on the psychologies of persuasion that underlie the strategies, tactics, and tools discussed in the previous two chapters. Forest draws on research to provide insights into methods commonly and effectively used to persuade. The influencer seeks to get others to see himself or herself as trustworthy, legitimate, and authoritative. The influencer then learns about the targets and areas where they might be vulnerable. In general, people tend to conform to perceived authority, be uncomfortable with uncertainty, and use a limited amount of cognitive effort. Presenting a relevant message is also important, and three types relate to social relevance, personal relevance, and emotional relevance. Influencers use these kinds of elements and others in persuading people to think or act in particular ways.

The fifth chapter discusses the use of digital influence silos, also known as "filter bubbles." These are places where individuals are drawn together with like-minded people who want to have their beliefs confirmed and validated, which creates a kind of in-group that is separate from others. Influencers create and manipulate such groups through social media, gaining power of their perceptions and decision-making. Forest considers conservative influence silos, as represented by Rush Limbaugh and Fox News, as especially powerful and problematic. He sees them as a threat to democracy in the United States.

The sixth chapter addresses "information dominance" and "attention dominance," and Forest focuses on two primary groups: authoritarian countries and democratic ones. The former have more power in terms of controlling the thinking and attention of their citizens, with an ability to limit access to outside information, such as through filtering and limiting internet access. They also can suppress the media, imprison journalists, and present their message in

some ways as the only one. China and Russia are the most effective in doing these things. Nevertheless, democratic countries and leaders can do these same things to some extent, and he uses Trump as a key example.

The seventh chapter briefly provides a conclusion, in which the author presents some concerns about the future and even more effective digital influence warfare taking place. He also offers suggestions as to how people might increase their awareness of these techniques and resist them successfully.

Forest presents many important and concerning ideas, and he supports them with concrete examples and research data. His book is important for policy makers, professors, students, and the general public. One problem area involves his bias against conservative political groups and his embrace of more liberal ones, seeing the former as a true threat to liberal democracy. He seems to ignore the existence and influence of more progressive information silos—for example, Harvard students regularly protest against speakers coming to campus who would share political perspectives unlike their own, which is directly in contrast to the democratic vision of higher education, where diverse ideas are considered and debated. They are part of a liberal and narrow-minded information silo. On balance, however, Forest's book makes an important contribution to the academic literature and is successful in its goal of informing readers about serious problems related to the misuse of social media.

John Jaeger, *Johnson University*

A City Is Not a Computer: Other Urban Intelligences. By Shannon Mattern. Princeton, NJ: Princeton University Press, 2021. Pp. x+187. $19.95 (paper). ISBN 978-0-691-20805-3.

The datafication of urban life through the integration of surveillance technologies, data dashboards, and algorithmic decision-making in city planning and governance serves as the hallmark of "smart cities" initiatives, a tech-solutionist approach to urban planning and management that asks what the city of the future could be if it were built "from the internet up" (53). On paper, the smart city seems well enabled to address the challenges and inefficiencies of urban governance: up-to-the-second metrics, data-driven policy decisions, interconnectedness, and transparency for numerous branches of city government. However, Shannon Mattern's latest book, *A City Is Not a Computer: Other Urban Intelligences*, challenges us to consider the ethical, epistemological, and ontological implications of computational models of urbanism. As she notes in her introduction, "Filtering urban design and administration through algorithms and interfaces tends to bracket out those messy and disorderly concerns that simply 'do not compute.' We're left with the sense that everything knowable and worth knowing about a city can fit on a screen—which simply isn't true" (4).