THIS BOOK ADDRESSES the problem of Chinese and Russian information warfare. I define the term “information warfare” as the use of social media by state agents to conduct foreign influence operations. The book proposes a new Alliance for Democracy so that democratic states can develop a coordinated, transnational approach to regulating social media to protect the integrity of their democratic political systems from the threat posed by Chinese and Russian information warfare.

I completed work on the initial manuscript for this project in November 2020. Then, on January 6, 2021, there was a riot at the Capitol in Washington, DC, unlike anything the United States had experienced since the Civil War. The insurrectionists were not Chinese or Russian agents; they were U.S. citizens. Most of them came to the Capitol because they believed the Big Lie: the claim that Democrats engaged in massive electoral fraud to steal the 2020 presidential election from the rightful winner, Donald Trump. Social media clearly played a role in disseminating the Big Lie, but so did several legacy media networks, such as Fox News, Newsmax TV, and One America News Network (OANN). Given available data, it is impossible to measure the relative influence of social media versus legacy media in spreading the Big Lie. Nevertheless, one thing seems clear: the people primarily responsible for spreading the Big Lie were U.S. citizens, not Chinese or Russian agents. There is some evidence that foreign agents helped amplify the main narrative, but their contribution appears to have been fairly minor.

In light of the insurrection at the Capitol on January 6, one might legitimately ask whether the book’s focus on Chinese and Russian information warfare...
warfare is misplaced. One could argue that the primary threat to American democracy comes not from foreign influence operations but from domestic disinformation campaigns. Indeed, after the events of January 6, if someone asked me to rank the significance of various threats to American democracy, I would rank domestic disinformation higher, and foreign interference correspondingly lower, than I would have before January 6. Even so, there are two primary reasons why a book focusing on Chinese and Russian information warfare is still timely and important.

First, Chinese and Russian information warfare poses a threat to democracies around the world, not just in the United States. The book’s central argument is framed in terms of the global threat to democracy. Chapter 1 demonstrates that, on a global basis, democracy has been declining and authoritarianism has been gaining momentum since about 2010. Moreover, chapter 3 notes that, since 2014, Russia has conducted foreign influence operations in at least twenty-one countries that are members of NATO, the European Union (EU), or both. Meanwhile, as documented in chapter 4, Chinese technology companies are helping to strengthen autocratic control in several countries by exporting “digital authoritarianism,” and China is exploiting social media to conduct foreign influence operations in Australia, Canada, the United Kingdom, and Taiwan, to name but a few states. Furthermore, as of this writing (in May 2021), there is no evidence that domestic sources of disinformation have been sufficiently influential to spark events comparable to the January 6 riots in other leading Western democracies. Thus, from the perspective of the global struggle between democracy and autocracy, Chinese and Russian information warfare remains a topic of vital concern.

Second, from a U.S. perspective, the First Amendment imposes significant limitations on the government’s power to regulate domestic sources of disinformation. Hence, the Constitution severely constrains the range of potential regulatory responses to the problem of domestic disinformation on social media. In contrast, Russian and Chinese agents who conduct information warfare activities on U.S. social media platforms—and who are physically located in Russia and China, respectively—are not entitled to any First Amendment protections. Granted, the First Amendment
imposes some limits on the government’s power to regulate speech on social media by Chinese and Russian agents, because the Constitution protects the right of U.S. listeners to receive that speech. Even so, the government has much greater leeway to regulate speech by foreign agents on U.S. social media platforms than it does to regulate speech by U.S. citizens on those same platforms. Part Two explains and defends a proposal for democratic states that are members of the proposed Alliance for Democracy to develop and implement a transnational regulatory system that would ban Chinese and Russian agents from U.S. social media platforms. (As explained in chapter 6, the proposed ban is subject to an exemption for benign state agents to protect the First Amendment rights of U.S. listeners to receive foreign speech.) Such a ban, if applied to domestic sources of disinformation in the United States, would clearly violate the First Amendment. However, as shown in chapter 8, the proposed ban is constitutionally defensible when applied to Chinese and Russian agents.

Two very different aspects of my own professional background shaped my thinking about the proposed transnational regulatory system. First, during the Cold War—before I became a law professor—I spent almost a decade in the U.S. government, where I worked on East-West arms control negotiations. During that time period, I developed substantial expertise in designing arms control verification systems. The proposed system for defending Western democracies from Chinese and Russian information warfare draws on my expertise in arms control verification systems. Second, during my academic career, I have developed substantial expertise in U.S. constitutional law. Accordingly, I designed the proposed transnational regulatory system to be consistent (or arguably consistent) with constitutional limitations on the government’s power to regulate speech.

Critics may argue that the proposed transnational regulatory system is flawed because it does not solve the “useful idiot” problem. Russian strategists refer to foreigners who unwittingly help advance Russia’s foreign policy goals as “useful idiots.” Donald Trump is a classic example of a useful idiot. By spreading the message that the 2020 presidential election was tainted by fraud, Trump helped advance Russia’s goal of undermining the faith of U.S. citizens in the integrity of American democracy. There is
no credible evidence to support the fraud allegation. Nevertheless, a CBS News poll in December 2020 found that 82 percent of Trump’s supporters believed that Biden’s victory was illegitimate and tainted by fraud.\(^6\) That widespread belief clearly serves Russia’s foreign policy interests. However, neither Vladimir Putin nor his legions of cyber troops can claim primary credit for the successful disinformation campaign. To the contrary, Donald Trump, more than any other single individual, deserves the blame for persuading millions of Americans that the 2020 election was fraudulent.\(^7\)

The useful idiot problem is a serious problem that merits a thoughtful policy response. My proposed transnational regulatory system does not solve that problem. However, it bears emphasis that no regulatory proposal can solve every problem. This book focuses on information warfare conducted by foreign cyber troops, not domestic disinformation. The useful idiot problem—as illustrated by Donald Trump’s effort to promote the Big Lie—falls outside the scope of my proposal because it fits in the category of domestic disinformation, not information warfare.

Implementation of the proposed ban on Chinese and Russian agents is not cost-free. The primary cost is that—to make the ban effective—members of the Alliance for Democracy would need to implement a social media registration system requiring citizens and nationals of Alliance member states to register their social media accounts with their home governments if they want to engage in public communication on social media.\(^8\) Reasonable people may disagree as to whether the benefits of the proposed transnational regulatory system outweigh the costs. The January 6 insurrection clearly alters that cost-benefit calculus by strengthening the argument in favor of the view that domestic disinformation is a much bigger threat to American democracy than foreign interference. People who believe that domestic disinformation is a major threat to American democracy, and that foreign interference is a minor threat, might well conclude that the costs of the proposed transnational regulatory system outweigh the benefits, because the proposed ban and registration system would do very little to address the problem of domestic disinformation. (The proposed registration system may provide a useful building block for designing a regulatory system that could help alleviate the threat of
domestic disinformation, but the proposal developed in chapter 6 focuses primarily on the threat of information warfare.

Chapter 7 presents a detailed analysis of the costs and benefits of the proposed transnational regulatory system. The key point here is this: Given First Amendment constraints on regulating domestic sources of disinformation, and given that Chinese and Russian information warfare poses a threat to democracies around the world, it makes sense from a public policy perspective to think about Chinese and Russian information warfare as a problem that is distinct from the problem of domestic disinformation, and that warrants a different type of policy response. The fact that foreign agents often amplify narratives disseminated by domestic sources of disinformation does not alter the conclusion that domestic disinformation and foreign information warfare are analytically distinct problems that, although related, warrant separate treatment.

This book contributes to the scholarly and public policy debate by analyzing Chinese and Russian information warfare as a distinct threat to democratic governments, and by proposing and evaluating policy solutions tailored to that threat. Many readers will not be persuaded that my proposed policy solutions are the best possible solutions. Regardless, I hope that the book will help readers gain a better understanding of the threat posed by Chinese and Russian information warfare, and that it may prompt readers to develop their own ideas about how Western democracies can and should defend themselves against that threat.
This page intentionally left blank