O'Brien in not just disaggregating the state, but also disaggregating society. He shows how both state and nonstate actors (in the plural) compete to manipulate public opinion through "discourse competition" (p. 16). He thus exposes both the internal fragmentation of the Party-state and the heterogeneity of netizen groups (p. 175).

Empirically, Han contributes to our understanding of Chinese politics and society today through his detailed interrogation of the micro-dynamics of online discourse competition. Following Guobin Yang, Han engages in "guerilla ethnography," the long-term observation of selected websites and chatrooms (p. 23). This produces a rich picture of discourse competition in Chinese cyberspace. For instance, in Chapter 7 the reader learns about several techniques of online combat, such as "labeling wars," "face-slapping," "crosstalk," and "fishing." Examples of "labeling wars" include when nationalists label their enemies as the "U.S. cents party" (美分党), the "dog food party" (狗粮党), or the "road-leading party" (带路党) who invite foreign invaders in (pp. 160–161). These details provide a nuanced view of the identity politics that drive online debates.

Han was raised in Mainland China and received his Bachelor's at Peking University before earning a PhD at Berkeley. As a non-Westerner, Han easily sidesteps the liberal binary of control versus resistance that so often impedes Western studies of Chinese politics and society. He does not insist on pitting a David society against a Goliath state. Instead, Han clearly sees and describes the heterogeneity among the various state and social actors (in the plural) in Chinese cyberspace. A great strength of *Contesting Cyberspace in China* is its ability to deconstruct online society into many subgroups. In his Preface, Han shares that as a freshman at Peking University he was a "BBS addict" (p. x) on online bulletin boards, and his lengthy immersion in Chinese cyberspace gives his book a richness that few can match.

Being socialized in post-Tiananmen China may also shape Han's view of the nationalism that is so central to his story. Han argues convincingly that the Party-state is not directly in control of discourse competition online, and that the "voluntary fifty-cent army" and other cyber-nationalists play an immediate role in shouting down CCP critics as traitors. But what's largely missing from the book is the distal hand of the Party-state in constructing popular nationalism in the first place. We do not hear much about the post-Tiananmen "Patriotic Education Campaign" (爱国教育运动) that Sam Zhao first wrote about, or the CCP's more recent stoking of anti-Japanese sentiment though the financing and production of "War of Resistance Against Japan" (抗日战争) video games, movies, and serial TV dramas. Han also downplays the role that nationalism plays in legitimizing the Party-state today, highlighting instead legitimacy claims based on economic development and good governance (p. 177).

Han's very brief but anomalous treatment of Japan is noteworthy. "The Chinese," Han claims, "responded to the [2011] Japanese earthquake and tsunami with good intentions," but encountered "hostility from the Japanese" (p. 148). In a book marked by a laudably consistent deconstruction of the idea of a unitary Chinese public, "the Chinese" and "the Japanese" in the singular are striking. Given that many (not all!) Chinese netizens apparently actually responded to the 2011 disaster in Japan with schadenfreude, gleefully declaring "just deserts!" (活该!) online (see Ying Yang, Xiao-xiao Liu, Yang Fang, and Ying-yi Hong "Unresolved World War II Animosity Dampens Empathy Toward 2011 Japanese Earthquake and Tsunami," *Journal of Cross-Cultural Psychology*, 45(2), 2014), Han's essentializing depiction of the beneficent Chinese set against the ungrateful Japanese is particularly puzzling.

Contesting Cyberspace in China is a fantastic contribution to the literatures on authoritarianism, cyberpolitics, and Chinese politics. By deconstructing both state and society, Han shows that a key to authoritarian resilience/collapse lies in discourse competition among heterogeneous groups of Chinese netizens online. As long as a plurality of Chinese netizens have been socialized to believe that China needs a strong government to protect the "China Dream" (中国之梦) from internal and external "national enemies," and question democracy as a means to national revival (p. 186), they are likely to continue to neutralize regime criticism online and sustain authoritarian rule.

Cyber Strategy: The Evolving Character of Power and Coercion. By Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness. New York: Oxford University Press, 2018. 320p. $34.95 cloth.
doi:10.1017/S1537592718002578

— Giampiero Giacomello, *University of Bologna*

Strategy, more precisely "grand strategy," is the way in which all instruments available to a state are integrated together to achieve the political goals set by the state's political leadership. This is the "enduring nature" of strategy, while its "changing character" is given by the emerging methods and technologies available to successive generations of political leaders. In *Cyber Strategy*, Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness examine one specific use of these "new" instruments of grand strategy, namely, digital means. More precisely, they investigate how effective such digital means, and the pertinent cyberoperations they are part of, actually are in coercing rivals.

As the authors clarify (pp. 8–11), as an "art," strategy has various, multifaceted means to manifest itself (and war is but one of them). Indeed, creativity and lateral thinking

are at a premium in strategy. In the book, the authors focus on the *cyber* dimension of strategy, identifying it as a "modern variant of coercive diplomacy" (p. 9). More explicitly, the research question leading their undertaking is "How do states use cyber strategies to influence their rivals?"—which is a bit peculiar as a "research question." Indeed, Valeriano, Jensen, and Maness do investigate *how* states employ cyberstrategies (because it is relatively easy and it does achieve some results, especially when coupled with other tools), but they also try to explain *why* states do so, which is the more traditional format of a research question.

Truth be told, some readers who may expect from the book's title an in-depth discussion of cyberwarfare (or cybersecurity in general) may be disoriented, which is what happened at first to this reviewer as these issues only remain in the background. Fortunately, this was just a passing moment, and the fact that the book is *not* on cyberwarfare was indeed a positive discovery. Sharing Martin Libicki's skepticism ("Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly*, 8(1), 2014) about the value of writing a "cyber war classic," I was then encouragingly relieved that this work does not try to live up to such impossible expectations, but that its real value lies in many points elsewhere.

The first such valuable point is a concise but remarkable literature review (pp. 4–7) of cyberspace, which the authors divide into two broad camps, namely, "evolutionary" versus "revolutionary" theorists, and declare themselves as belonging to the former group. To be accurate, one should recognize that the evolutionary faction of cyberspace students (particularly among those with an international relations background) is larger than the revolutionary one. Most scholars (including this reviewer) were convinced in the beginning that cyberspace was indeed revolutionary, but slowly shifted toward a more evolutionary perspective. This change is probably the outcome of more and more governments slowly learning how to exercise more effective control on cyberspace than 20 years ago. Furthermore, cyberspace is so much a part of everybody's life today that the study of politics can no longer fail to take note of it.

The authors then proceed to identify coercion as a strategy that can be articulated in cyberspace through disruption, espionage, and degradation. They present three hypotheses: Cyberdegradation is more likely to produce concessions; cyberoperations are used as means of limited escalation; and unique combinations of cyberops and other tools are used to achieve concessions from rivals. These hypotheses are subsequently tested in the quite extensive quantitative portion of the book and the case studies.

The three case studies (pp. 110–201)—the United States, Russia, and China—are predictable, not only because they are the world's great powers but also because they are actively engaged in continuous cyberskirmishes. The picture presented is that of the United States desperately trying to protect itself from China's espionage and copyright theft (to close its technology gap) and from Russia's meddling in American and world affairs in a fashion consistent with its old Soviet past. Indeed, the close connections between the Russian government and organized crime are taken right from old KGB's manuals, so that anything that damages the West is acceptable, no matter who contributes to it. Besides, as Russia has a much weaker economy than its chief rivals, other retaliation options and thus deterrence capabilities are rather limited.

The case studies are well researched and contribute to the book's overall conclusions (pp. 201–214), which are also neatly summarized in a helpful policy appendix (p. 225): Cyberstrategies are functional to the political warfare of today, though unless accompanied by other means of coercion, they are unlikely to change the positions of rivals (a bit paradoxically, digital means are having a greater "tactical" impact on the battlefield).

These case studies do have a shortcoming, one weighty enough to be noted here: Europe, or more specifically the European Union, is nowhere to be seen in these pages. While this may be understandable in some ways, as the EU is not a sovereign state like the United States, Russia or China, and the complex functioning of the EU baffles most non-Europeans (and many Europeans as well), the EU nevertheless constitutes (along with the United States and Japan) the most advanced group of digital economies. And many EU member states are even more information technology (IT) dependent than the United States itself. This is to say nothing of the fact that the collapse of European infrastructures (transportation, commerce, undersea cables), let alone financial markets, would send more than a few ripples to the United States.

As a nonsovereign state, the EU cannot use digital means to coerce adversaries, but it is at the receiving end of those cyberoperations that are intended to intimidate the EU as a whole, as well as many of its member states. Consequently, as an integrated political entity, the EU is the world's biggest spender in *cyberdefense*. At least some of these elements should have been recognized and included by the authors. While the peculiarities of the EU illustrated here may explain the lack of interest and consideration of the EU, ignoring the work done by European scholars in the early phase of the study of cyberspace is much less understandable (e.g., Giampiero Giacomello, *National Governments and Control of the Internet: A Digital Challenge*, 2005).

To conclude, the contribution of this book is undoubtedly original, well researched, and presented, but, in a sense, it confirms what international relations and strategy students already know and expect: Add another domain, and states will find ways to exploit it to their ends. When ruling the waves offered even more options

for states to achieve their objectives, sea power was born; subsequently it was the sky and then space, and today it is cyberspace. And tomorrow, who knows?

Nevertheless, what is really needed today, at least for cyberspace, is a greater number of original studies not on "states" but, rather, on the other relevant actors in cyberspace, namely, companies, organized criminal gangs, and certain technically savvy groups of individuals, as well as how these actors support, foster, or hamper states' cyberstrategies. This is the distinctiveness and (still) revolutionary field that sets cyberspace apart from other domains.

Censored: Distraction and Diversion Inside China's Great Firewall. By Margaret E. Roberts. Princeton: Princeton University Press, 2018. 288p. $29.95 cloth.
doi:10.1017/S1537592718002608

— Rongbin Han, *University of Georgia*

The coexistence of enduring authoritarianism and the Internet has drawn wide academic attention. Why are some authoritarian regimes, previously believed to be inherently incompatible with free information, surviving and even thriving despite the expansion of the Internet? In *Censored*, Margaret E. Roberts develops a novel theory of censorship to explain authoritarian resilience in the digital age. She argues that strong authoritarian governments such as China have the capacity to enforce censorship more forcefully, but choose not to do so; they instead embrace a strategy of porous censorship. Such a strategy combines fear, diversion, and distraction mechanisms, allowing autocrats to differentiate politically active citizens from the majority of the public and shape the latter's information-seeking behavior by altering the costs to accessing information. In this way, authoritarian governments manage to maintain sufficient control over information while avoiding the repercussions that are associated with heavy-handed repression. The book is an impressive display of theoretical originality, methodological sophistication, and empirical richness.

The book advances a theory of censorship explaining the strategic interplay between government control and citizens' production and consumption of information (Chapter 2). Roberts first describes the censorship incentives of the government, as well as how the media and citizens, respectively, interact with information, arguing that both the media and the public are sensitive to the costs of information production, distribution, and consumption. From there, she elucidates the three main mechanisms of censorship: fear, friction, and flooding. While fear works through deterrence, both friction and flooding reprioritize the production and consumption of information by affecting its relative price: Friction raises the absolute cost; flooding raises the relative cost (by lowering the costs of information from alternative sources). An example of friction is the "Great Firewall" of China, which is not impossible to circumvent, but prevents the majority of citizens from accessing banned sites by costing them more time, money, and energy. An example of flooding is "Twitter armies" amassed by governments to push for their views. Since the media and the public are cost sensitive, censorship is not just fear based but can work through friction and flooding tactics that do not stop information flow completely, but rather inconvenience users. Moreover, Roberts argues that in the Internet age, fear-based censorship has become more costly, while friction has become more impactful and flooding much cheaper.

After outlining the theoretical framework, Roberts tests her theory empirically using evidence primarily from China. In Chapter 3, she provides an overview of censorship in Chinese history as well as today. In Chapters 4 through 6, she discusses in detail how Chinese citizens react when they observe censorship, how their information-seeking behavior may be affected by even small and less observable frictions, as well as how flooding may shape information supply and demand. Roberts demonstrates that typical netizens in China are angered rather than intimidated after experiencing censorship, showing that fear-based censorship is ineffective; speed of censorship bears implications for the spread of information, while small impediments can generate an immediate impact on users' information-access behavior; and coordinated government propaganda can make certain types of information more likely to be shared in social media spheres.

It is in the empirical chapters that Roberts has fully demonstrated her mastery of rich data and sophisticated methods. She has truly done an admirable job testing her theory using experimental methods, national survey data, large-scale social media data sets, leaked propaganda archives, and data sets of newspapers. In a nutshell, she conducts mixed-method research long advocated in the field in an exemplary way, and her contributions are especially worth highlighting in two respects. First, the innovative approach and the data strategy are particularly inspiring for scholars working on sensitive topics in a constrained political environment. It is challenging to conduct research in a repressive authoritarian regime like China. Despite overall improvements in the reform era, there are still many obstacles, and the situation has only deteriorated in the past few years. What Roberts has done can serve as a road map for doing research in China and perhaps other authoritarian regimes in terms of a) how to conduct research without triggering repercussions for the researcher, the project, and most importantly our subjects; and b) how to make good use of available data. Second, while many of us still worry about data availability, we are at the same time in an age of data explosion. The Internet is providing so much more data