Summaries

"Rising nationalism" has been a major meme in commentary on the development of China's material power since the early 1990s. Analysts often claim that rising nationalism, especially among China's youth, is an important force compelling the Chinese leadership to take a tougher stand on a range of foreign policy issues, particularly maritime disputes in East Asia. The rising nationalism meme is one element in the "newly assertive China" narrative that generalizes from China's coercive diplomacy in these disputes to claim that a dissatisfied China is challenging a U.S.-dominated liberal international order writ large. But is this meme accurate? Generally, research on Chinese nationalism has lacked a baseline against which to measure changing levels of nationalism across time. The data from the Beijing Area Study survey of Beijing residents from 1998 to 2015 suggest that the rising popular nationalism meme is empirically inaccurate. This finding implies that there are other factors that may be more important in explaining China's coercive diplomacy on maritime issues, such as elite opinion, the personal preferences of top leaders, security dilemma dynamics, organizational interests, or some combination thereof.

PREVENTING AND RESPONDING TO CYBERATTACKS

Understanding deterrence and dissuasion in cyberspace is often difficult because our minds are captured by Cold War images of massive retaliation to a nuclear attack by nuclear means. The analogy to nuclear deterrence is misleading, however, because many aspects of cyber behavior are more like other behaviors, such as crime, that states try (imperfectly) to deter. Preventing harm in cyberspace involves four complex mechanisms: threats of punishment, denial, entanglement, and norms. Even when punishment is used, deterrent threats need not be limited to cyber responses, and they may address general behavior as well as specific acts. Cyber threats are plentiful, often ambiguous, and difficult to attribute. Problems of attribution are said to limit deterrence

and dissuasion in the cyber domain, but three of the major means—denial by defense, entanglement, and normative taboos—are not strongly hindered by the attribution problem. The effectiveness of different mechanisms depends on context, and the question of whether deterrence works in cyberspace depends on "who and what." Not all cyberattacks are of equal importance; not all can be deterred; and not all rise to the level of significant national security threats. The lesson for policymakers is to focus on the most important attacks and to understand the context in which such attacks may occur and the full range of mechanisms available to prevent them.

Most scholars and policymakers claim that cyberspace favors the offense; a minority of scholars disagree. Sweeping claims about the offense-defense balance in cyberspace are misguided because the balance can be assessed only with respect to specific organizational skills and technologies. The balance is defined in dyadic terms, that is, the value less the costs of offensive operations and the value less the costs of defensive operations. The costs of cyber operations are shaped primarily by the organizational skills needed to create and manage complex information technology efficiently. The current success of offense results primarily from poor defensive management and the relatively simpler goals of offense; it can be very costly to exert precise physical effects using cyberweapons. An empirical analysis shows that the Stuxnet cyberattacks on Iran's nuclear facilities very likely cost the offense much more than the defense. The perceived benefits of both the Stuxnet offense and defense, moreover, were likely two orders of magnitude greater than the perceived costs, making it unlikely that decisionmakers focused on costs.

How do states pursue nuclear weapons? Why do they select particular strategies to develop them, and how do these choices affect the international community's ability to prevent nuclear proliferation? The bulk of the proliferation literature focuses on why states want nuclear weapons. The question of how they pursue them, however, has largely been ignored. This question is impor-

tant because how states try to acquire nuclear weapons—their strategies of nuclear proliferation—affects their likelihood of success and thus the character of the nuclear landscape. Four strategies of proliferation are available to states: hedging, sprinting, hiding, and sheltered pursuit. Nuclear acquisition theory explains why a proliferator might select one strategy over the others at a given time. Empirical codings from the universe of nuclear pursuers, combined with a detailed plausibility probe of India's long march to acquiring nuclear weapons—including novel details—establish the analytical power of the theory. Different strategies of proliferation offer different opportunities and vulnerabilities for nuclear proliferation and nonproliferation, with significant implications for international security.

151–196

Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–16

Daniel Sobelman, Harvard University

What are the sources of deterrence stability and under what conditions can weak actors deter stronger adversaries? To deter a superior adversary, the weak actor must convince it that if conflict breaks out, the weak actor would be capable of rendering its opponent's strategic capabilities tactical and its own tactical capabilities strategic. The deterrence relationship that has evolved between Israel and the Lebanese Hezbollah in the decade since—and as a result of—the 2006 Lebanon War (a.k.a. the Second Lebanon War or the July War) confirms this observation. A comparison of these two actors' deterrence behavior in the years preceding the war and in its aftermath shows that one of the leading explanations for the ongoing stability along the Israeli-Lebanese border is that Israel and Hezbollah have learned to apply deterrence in a manner that meets the prerequisites of rational deterrence theory.

NOTE TO CONTRIBUTORS

International Security is a peer-reviewed journal that publishes articles on all aspects of security affairs. The articles published in the journal are first circulated for doubly blind external review. To facilitate review, authors should submit their manuscripts with a cover letter and an abstract of 150–200 words online via Editorial Manager at http://www.editorialmanager.com/isec. Authors should refrain from identifying themselves in their manuscripts. A length of 10,000–15,000 words is appropriate, but the journal will consider and publish longer manuscripts. Authors of manuscripts with more than 20,000 words should consult the journal's editors before submission. All artwork must be camera ready. For more details on preparing manuscripts for submission, see "How to Write for *International Security:* A Guide for Contributors" (Fall 1991).

For a fuller explanation of the review process, current contents, a cumulative index, the guide for contributors, and other useful information, please visit the journal's website at http://www.belfercenter.org/IS/. For information on subscriptions, permissions, and other details, visit the MIT Press *International Security* website at http://mitpress.mit.edu/ISEC. For more information on the Belfer Center for Science and International Affairs, the editorial headquarters of *International Security,* go to http://www.belfercenter.org.