Strategic Substitution

China's Search for Coercive Leverage in the Information Age

Fiona S. Cunningham

After NATO accidentally bombed China's embassy in Belgrade on May 6, 1999, during the Kosovo War, Communist Party General Secretary Jiang Zemin vowed to protect the country's national interests by increasing its coercive leverage against the United States. "If Chairman Mao and Premier Zhou had not led us to produce nuclear bombs, hydrogen bombs, and man-made satellites, we would not be in this secure situation today," he declared, "I fear that we would have been attacked earlier on."[1] China's leaders viewed the embassy bombing as a signal of U.S. hostility, which would have serious implications if war were to break out across the Taiwan Strait. Taiwan was agitating for formal independence in the late 1990s, which the People's Republic of China threatened war to prevent. But if the United States intervened, China would not have been able to achieve a conventional military victory to prevent Taiwanese independence. Threats to escalate a Taiwan conflict were China's only hope of achieving that aim.[2]

How has China gained coercive leverage against a nuclear-armed adversary in a war over limited objectives without triggering an immensely destructive nuclear exchange? After the Belgrade crisis, Jiang Zemin did not abandon China's retaliatory posture for its nuclear weapons, which threatened nuclear use only after an adversary's nuclear attack. Instead, China turned to space, cyber, and precision conventional missile attacks to increase its coercive

Fiona S. Cunningham is Assistant Professor of Political Science at the University of Pennsylvania.

For helpful comments and suggestions, the author thanks James Acton, Ben Bahney, Ben Buchanan, Austin Carson, Toby Dalton, James Fearon, Taylor Fravel, Erik Gartzke, Francis Gavin, Charles Glaser, Avery Goldstein, Michael Horowitz, Alastair Iain Johnston, Tyler Jost, Herb Lin, Jon Lindsay, Vipin Narang, George Perkovich, Mark Pollack, Barry Posen, Brad Roberts, Scott Sagan, Caitlin Talmadge, Alex Weisiger, seminar participants at the University of California, Berkeley, Georgetown University, the U.S. Naval War College, the University of Pennsylvania, Princeton University, Temple University, Stanford University, the Stanton Nuclear Security Conference, the Nuclear Studies Research Initiative, and the anonymous reviewers. The research for this article was supported by a fellowship from the Smith Richardson Foundation.

1. Jiang Zemin, *Jiang Zemin wenxuan (er juan)* [Selected works of Jiang Zemin (volume 2)] (Beijing: Zhongyang wenxian chubanshe, 2006), p. 323.
2. Thomas J. Christensen, "Posing Problems without Catching Up: China's Rise and Challenges for U.S. Security Policy," *International Security*, Vol. 25, No. 4 (Spring 2001), pp. 5–40, https://doi.org/10.1162/01622880151091880.

International Security, Vol. 47, No. 1 (Summer 2022), pp. 46–92, https://doi.org/10.1162/isec_a_00438

leverage against the United States and Taiwan. This article refers to these capabilities collectively as information-age weapons. One year after the Belgrade embassy bombing, China's leaders decided to pursue offensive cyber capabilities that would enable it to attack an adversary's important information networks. In 2002, Jiang also hinted that China was pursuing counterspace weapons, and he instructed the People's Liberation Army (PLA) to build a "strategic deterrence system bringing together many means."[3]

China's threats to use these "many means" have manipulated risk to different degrees across capabilities and over time. In 2014, China's leaders brought the PLA's cyber capabilities under their direct control, out of the shadows, and focused them on controlling escalation from cyberattacks. These changes were an abrupt departure from China's initial approach, which tasked some of its decentralized and secretive cyber units with shocking an adversary into submission with large-scale attacks. Those attacks risked uncontrollable escalation to a full-scale war.

China's substitution of information-age weapons for threats of nuclear first use and war-winning conventional capabilities to gain leverage is puzzling. Nuclear strategists would expect China to behave like other countries that have adopted nuclear first-use postures to compensate for their inabilities to win wars with conventional forces.[4] The cyber conflict literature suggests that large-scale offensive cyber operations are not effective tools of coercion and are unlikely to escalate a conflict.[5] No theories specifically explain why or how states could use space weapons or conventional missiles for coercive leverage.[6] China's decisions could be explained by theories of military innovation

3. Jiang Zemin, *Jiang Zemin wenxuan (san juan)* [Selected works of Jiang Zemin (volume 3)] (Beijing: Zhongyang wenxian chubanshe, 2006), pp. 581–582, 585.
4. Bernard Brodie, *Escalation and Nuclear Option* (Princeton, N.J.: Princeton University Press, 1966); Morton H. Halperin, *Limited War in the Nuclear Age* (New York: John Wiley, 1963); and Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), pp. 118, 123, 184.
5. Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity*, Vol. 5, No. 1 (2019), p. 9, https://doi.org/10.1093/cybsec/tyz007; Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution*, Vol. 63, No. 2 (2019), pp. 317–347, https://doi.org/10.1177/0022002717737138; Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Jon R. Lindsay and Erik Gartzke, "Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains," *Journal of Strategic Studies*, published online June 1, 2020, pp. 22–24, http://doi.org/10.1080/01402390.2020.1768372; and Erica D. Lonergan and Shawn W. Lonergan, "Cyber Operations, Accommodative Signaling, and the De-escalation of International Crises," *Security Studies*, Vol. 31, No. 1 (2022), pp. 32–64, https://doi.org/10.1080/09636412.2022.2040584.
6. Stephen Biddle and Ivan Oelrich, "Future Warfare in the Western Pacific: Chinese Antiaccess/

and diffusion, but they raise questions for those theories as well.[7] China waited a surprisingly long time to adopt offensive cyber capabilities after the PLA wrote about the potential of U.S. "computer virus weapons" during the Gulf War. China's initial approach to cyber operations also gave PLA cyber operators a surprising degree of autonomy for a state with assertive civil-military relations.[8]

This paper develops an original theory of strategic substitution to explain why China's search for coercive leverage in the post–Cold War era led it to pursue information-age weapons. Counterspace weapons, cyberattacks, and precision conventional missiles stood out to China as promising sources of leverage because they can be used strategically to create a risk of escalation to nuclear war. To make credible threats of escalation, however, China had to configure its information-age weapons to create slippery slopes or ladders from conventional to nuclear war. I argue that China combines information-age strategic attacks with a retaliatory nuclear posture to compensate for its conventional military inferiority. This combination threatens to increase the intensity of a conventional war right up to the threshold of nuclear weapons use but places the burden of crossing that threshold on the adversary. But strategic substitution has been a gamble rather than a silver bullet for China.

The theory of strategic substitution explains why China pursued information-age weapons to address leverage deficits and how it configured them to gain

---

Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia," *International Security*, Vol. 41, No. 1 (Summer 2016), pp. 7–48, https://doi.org/10.1162/ISEC_a_00249; Ashton B. Carter, "Satellites and Anti-Satellites: The Limits of the Possible," *International Security*, Vol. 10, No. 4 (Spring 1986), pp. 46–98, https://doi.org/10.2307/2538950; and James Clay Moltz, *Crowded Orbits: Conflict and Cooperation in Space* (New York: Columbia University Press, 2014). For case-specific exceptions, see Joshua R. Itzkowitz Shifrinson and Miranda Priebe, "A Crude Threat: The Limits of an Iranian Missile Campaign against Saudi Arabian Oil," *International Security*, Vol. 36, No. 1 (Summer 2011), p. 199, https://doi.org/10.1162/ISEC_a_00048; and Benjamin W. Bahney, Jonathan Pearl, and Michael Markey, "Antisatellite Weapons and the Growing Instability of Deterrence," in Erik Gartzke and Jon R. Lindsay, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), p. 136.

7. Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, N.Y.: Cornell University Press, 1984); Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, N.Y.: Cornell University Press, 1991); Owen R. Cote Jr., "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles," Ph.D. dissertation, Massachusetts Institute of Technology, 1996; Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, N.J.: Princeton University Press, 2010); and João Resende-Santos, *Neorealism, States, and the Modern Mass Army* (Ithaca, N.Y.: Cornell University Press, 2007).

8. Peter D. Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, N.Y.: Cornell University Press, 1992), pp. 8–9; and Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton, N.J.: Princeton University Press, 2014), pp. 41–42.

coercive leverage. When China faced a leverage deficit because of a change in its threat environment, it searched for additional coercive leverage. A leverage deficit reflects a situation in which a state's capabilities are ill-suited for the type of war and adversary that it is most likely to fight, and it would likely fail to achieve its objectives if a war with that adversary were to occur. China's search for leverage became a search for substitutes, because its leaders harbored doubts about the credibility of nuclear threats, and they were unable to quickly redress a disadvantage in the conventional military balance of power. Information-age weapons were attractive substitutes because they promised quick and credible leverage in a limited war. In the absence of such a deficit, China did not change its policy for gaining leverage. To make credible threats to escalate a conflict using an information-age weapon, China had a choice between what I call "brinkmanship" or "calibrated escalation" force postures. These two postures reflect different approaches to manipulating the risk of uncontrolled escalation. China's choice of posture for its offensive cyber capabilities was shaped by its vulnerability to cyberattacks.

I demonstrate the plausibility of the theory of strategic substitution by examining three key Chinese decisions about why and how to use cyberattacks strategically to coerce the United States in a Taiwan conflict. The PLA characterizes a Taiwan conflict as a "local" war. Its decision to pursue a coercive cyber weapons capability at the end of 2000 was a response to the leverage deficit revealed by the NATO bombing of its embassy in Belgrade. China's low dependence on information networks around 2002 shaped its choice of a brinkmanship posture for large-scale offensive cyber operations. Chinese leaders switched to a calibrated escalation posture in 2014, following a dramatic increase in China's vulnerability to cyberattacks.

This paper makes three contributions to international relations scholarship. First, it updates theories of coercion among nuclear-armed states for the information age to reflect both technological change and cross-national variation in nuclear strategy. Existing theories focus on limited nuclear wars and do not explain how states with retaliatory nuclear postures (i.e., Israel, India, and China) might otherwise coerce their adversaries. Technological change also equips states with more coercive military capabilities today than in previous decades.[9] Some pioneering scholarship explores cross-domain deterrence dynamics,[10] but it does not explain how states have seized on the promise of

9. Caitlin Talmadge, "Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today," *Journal of Strategic Studies*, Vol. 42, No. 6 (2019), pp. 864–887, https://doi.org/10.1080/01402390.2019.1631811.
10. Jon R. Lindsay and Erik Gartzke, "Introduction: Cross-Domain Deterrence, from Practice to

information-age weapons to plug gaps in their existing nuclear and conventional military strategies.

Second, this paper fills important gaps in existing studies of how states use offensive cyber, counterspace, and precision conventional missile attacks for coercive leverage. The cyber conflict literature does not explain why states continue to pursue capabilities for large-scale cyberattacks and view them as valuable instruments of coercion, despite their questionable effectiveness.[11] Nor have Chinese views shaped theories of cyber conflict, given the scarcity of data on Chinese cyber decision-making.

Third, this paper exploits new sources to offer a novel and theoretically informed explanation of China's approach to strategic coercion in the post–Cold War era. It provides the most complete account of China's military cyber decision-making in the existing literature, relying on more than one hundred original Chinese-language written sources, supplemented by interviews with more than fifty Chinese experts conducted between August 2015 and January 2017.[12] Existing literature does not explain China's decisions about offensive cyber capabilities or recognize the extent of change in its military cyber posture since 2014.[13]

Theory," in Gartzke and Lindsay, eds., *Cross-Domain Deterrence*, pp. 1–23; and Jon R. Lindsay and Erik Gartzke, "Conclusion: The Analytic Potential of Cross-Domain Deterrence," in Gartzke and Lindsay, eds., *Cross-Domain Deterrence*, pp. 335–371.

11. One exception is Jon Lindsay, who argues that this disconnect in Chinese writings is a function of mistaken beliefs about cyber operations. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15), pp. 36–37, https://doi.org/10.1162/ISEC_a_00189.

12. Written sources include official government documents; the speeches, memoirs, writings, official biographies, and chronologies of top Chinese military and civilian decision-makers; and research and teaching texts from Chinese military and civilian research organizations. To preserve the anonymity of interviewees on this sensitive topic, identifiers are not provided.

13. One exception is Lyu Jinghua, who attributes a gradual change in China's military cyber posture to growing PLA dependence on information networks and learning about the limits of cyber effects. Lyu Jinghua, "A Chinese Perspective on the New Intelligence Framework to Understand National Competition in Cyberspace," in Robert Chesney and Max Smeets, eds., *Deter, Disrupt, or Deceive? Assessing Cyber Conflict as an Intelligence Contest* (Washington, D.C.: Georgetown University Press, forthcoming). Other studies describe recent changes to China's military cyber doctrine and organizations but do not explain why they occurred. See John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives No. 13 (Washington, D.C.: National Defense University Press, October 2018); and Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power," *Journal of Strategic Studies*, Vol. 44, No. 2 (2021), pp. 218–264, https://doi.org/10.1080/01402390.2020.1747444. See also Nigel Inkster, *China's Cyber Power* (London: International Institute for Strategic Studies, 2015); Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015); Joe McReynolds and James Mulvenon, "The Role of Informatization in the People's Liberation Army under Hu Jintao," in Roy Kamphausen, David Lai, and Travis Tanner, eds.,

This article proceeds as follows. First, it shows that some offensive cyber, space, and precision conventional missile capabilities can be used strategically to give states coercive leverage that is distinct from conventional and nuclear operations. It outlines two coercive force postures that states can adopt to use those weapons strategically. Second, it outlines the theory of strategic substitution to explain why China pursued these weapons and how it made credible threats to use them through its force posture choices. The remainder of the paper applies the theory of strategic substitution to China's cyber force posture. To conclude, it evaluates whether China's gamble on information-age weapons has delivered the coercive leverage that it promised and considers the implications of the theory for other nuclear-armed states and U.S.-China strategic stability.

Information-Age Weapons and Coercive Leverage

Among the information-age technologies with military applications, space weapons, cyberattacks, and precision missiles with conventional payloads have captured both the popular imagination and the attention of governments because of their potential to alter the course of a conflict. A space weapon disrupts or destroys another state's ability to use its satellites or other assets in outer space, including attacks that disrupt the relay of information between space and earth. Those weapons include jammers, lasers, microwaves, electromagnetic pulse weapons, and kinetic anti-satellite (ASAT) weapons that collide with an adversary's satellites. Cyberattacks disrupt or destroy the normal functions of an adversary's computer networks.[14] I define a precision conventional missile, the category of missiles discussed in this paper, as any cruise, ballistic, or hypersonic missile that relies on information networks to deliver a conventional payload within 50 meters of a target.

STRATEGIC USES OF INFORMATION-AGE WEAPONS

States want coercive leverage in limited wars to achieve their political aims with threats of violence rather than continuing to bear the costs of fighting the

Assessing the People's Liberation Army in the Hu Jintao Era (Carlisle, Pa.: U.S. Army War College Press, 2014), pp. 207–256; and Joe McReynolds, "China's Military Strategy for Network Warfare," in McReynolds, ed., *China's Evolving Military Strategy* (Washington, D.C.: Brookings Institution Press, Jamestown Foundation, 2016), pp. 195–240.

14. Cyber intrusions for espionage are excluded from this definition but could be mistaken for preparations to attack. See Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford University Press, 2017).

war.[15] Conventional weapons give states coercive leverage, typically by threatening to achieve a military victory or deny an adversary's victory.[16] But some weapons are better suited to threatening to escalate a conflict to gain coercive leverage. By threatening to punish an adversary or deny it a military victory, or both, an escalatory attack affects an adversary's expectations about the future course of the conflict. The effects on military operations are less important than these strategic effects on the adversary's decision-making.[17]

Some space weapons, cyberattacks, and precision conventional missiles possess three characteristics that make them particularly well-suited to threats of escalation: their effects, ability to cross salient thresholds, and entanglement with nuclear arsenals. Because of these three characteristics, information-age weapons are promising for strategic uses, which are distinct from operational uses to engage an adversary's military capabilities.[18] They create additional pathways for a limited conventional conflict to become a nuclear war even when two states are locked in a nuclear stalemate. The credibility of a "threat that leaves something to chance"[19] of all-out nuclear war declines as two states enter deeper into a nuclear stalemate because both have secure second-strike capabilities.[20] Uncertainties about whether using information-age weapons would provoke a nuclear war revive the possibility of relying on a threat that leaves something to chance for bargaining leverage.

First, large-scale counterspace attacks, cyberattacks, and missile strikes can be used strategically to hold hostage an adversary's homeland, military, or allies using threats of significant damage. A large-scale cyberattack could disrupt a society's critical infrastructure as soon as the attacker activates malicious code. The disruption would, however, be difficult to sustain if the adversary eliminates the malicious code or cuts off the attacker's access to its networks. No state can be confident that its computer networks are completely defended against the cyberattacks of a persistent, well-resourced nation-state

15. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, N.Y.: Cornell University Press, 1996), pp. 13, 15.
16. John J. Mearsheimer, *Conventional Deterrence* (Ithaca, N.Y.: Cornell University Press, 1983). Conventional weapons can also be used to punish an adversary, for example, by using a naval blockade.
17. Richard Smoke, *War: Controlling Escalation* (Cambridge, Mass.: Harvard University Press, 1977), p. 274.
18. Carl von Clausewitz, *On War* (Princeton, N.J.: Princeton University Press, 1976), p. 128.
19. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960), pp. 187–203.
20. Robert Powell, "The Theoretical Foundations of Strategic Nuclear Deterrence," *Political Science Quarterly*, Vol. 100, No. 1 (Spring 1985), pp. 78–82, https://doi.org/10.2307/2150861.

adversary.[21] Using an ASAT weapon to destroy a few satellites could create enough space debris to make an orbit unusable. A debris cloud would permanently disrupt any state's use of that orbit to support communications, intelligence, weather, financial networks, and navigation for civilians and militaries alike. Satellites are fragile and have predictable trajectories, which makes them difficult to defend from ASAT attacks.[22] A missile attack could permanently destroy an adversary's military and civilian infrastructure. Unlike aerial strategic bombing, those missiles would not need to overcome an adversary's air defenses and could overwhelm missile defenses if equipped with countermeasures.[23] Information-age weapons that hold hostage assets that states value and are difficult to defend against create a situation of mutual vulnerability between similarly armed rivals.

Some scholars are skeptical that these attacks could effectively coerce a target. They argue that the direct effects of these attacks, while able to punish or deny an adversary's military victory, would not be as damaging as some conventional military operations, let alone nuclear attacks.[24] But their effects would signal a willingness to expand a limited, conventional war toward a nuclear war.[25] Of course, not all space, cyber, and missile strikes can be used to create these effects because some of them would have only localized, temporary, or small-scale effects, such as jamming an opponent's satellite receiver on the battlefield.

Second, some space, cyber, and conventional missile attacks would cross salient thresholds in limited wars, while leaving other thresholds intact. According to Thomas Schelling, salient thresholds are "obvious places to draw the line, for reasons more related to psychology or custom than to the mathematics

---

21. The cyber offense-defense balance, however, is contested. See Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 66–68, https://doi.org/10.1162/ISEC_a_00136; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND, 2009), pp. 32–33; and Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, https://doi.org/10.1162/ISEC_a_00267.
22. Bruce M. DeBlois et al., "Space Weapons: Crossing the U.S. Rubicon," *International Security*, Vol. 29, No. 2 (Fall 2004), pp. 62, 83, https://doi.org/10.1162/0162288042879922.
23. Steve Fetter, "Ballistic Missiles and Weapons of Mass Destruction: What Is the Threat? What Should Be Done?" *International Security*, Vol. 16, No. 1 (Summer 1991), p. 9, https://doi.org/10.2307/2539050.
24. Ibid.; Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), pp. 122–145, https://www.jstor.org/stable/26760131; and Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).
25. Smoke, *War*, p. 242.

of warfare."[26] Crossing those limits has strategic effects because it changes an adversary's expectations about a state's willingness to violate other salient thresholds in the future.[27] Currently, there is no evidence of an "ASAT taboo" or equivalent prohibitions against the use of conventional missiles or cyberattacks that constrain their use in a similar way to what Nina Tannenwald describes as the nuclear taboo.[28] But the use of space, cyber, or precision missile attacks with large-scale effects could violate limits on the geographical scope, parties, or intensity of a limited war that are salient thresholds for the belligerents.[29]

Third, information-age weapons could significantly increase the risk of nuclear war if an adversary believes that they might degrade its nuclear arsenal, whether the state intends to have that effect or not. Cyberattacks could disrupt the information networks that ensure the survivability and timely launch of nuclear weapons.[30] Precision conventional missiles could be mistaken for nuclear missiles or used to destroy nuclear weapons.[31] Counterspace weapons could damage nuclear early warning and communications satellites.[32] Even if a state does not intend to use its information-age weapons in this manner, an adversary would have difficulty verifying these intentions and, in addition, might worry that these weapons could inadvertently damage its nuclear arsenal once a war started.[33]

Posturing Information-Age Weapons for Coercive Leverage

To use an information-age weapon strategically, a state must pursue and configure that capability for coercive leverage against its adversary. A decision to pursue such weapons involves more than a decision to research, develop, or test an offensive capability. The state's leaders must recognize that the

26. Schelling, *Arms and Influence*, p. 135.
27. Smoke, *War*, p. 35.
28. Nina Tannenwald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security*, Vol. 29, No. 4 (Spring 2005), pp. 5–49, https://doi.org/10.1162/isec.2005.29.4.5.
29. Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965), pp. 4–6.
30. Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity*, Vol. 3, No. 1 (March 2017), pp. 37–48, https://doi.org/10.1093/cybsec/tyw017.
31. Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security*, Vol. 41, No. 4 (Spring 2017), pp. 50–92, https://doi.org/10.1162/ISEC_a_00274.
32. James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security*, Vol. 43, No. 1 (Summer 2018), pp. 56–99, https://doi.org/10.1162/isec_a_00320.
33. Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, N.Y.: Cornell University Press, 1991).

information-age weapon will be used to gain leverage, set a timeline for deployment, and configure the new capability so that it can be used to make credible threats to escalate a conflict. I outline two distinctive coercive force postures that states can adopt for information-age weapons: brinkmanship and calibrated escalation. I adopt Vipin Narang's definition of a force posture as a state's plans for using its weapons in a conflict, the capabilities it deploys, its command-and-control arrangements, and the signals it sends to adversaries about those plans.[34] A state can have different force postures for all three of its information-age weapons.

Both brinkmanship and calibrated escalation postures enable states to generate leverage by threatening large-scale space, cyber, or missile attacks, even if carrying out that attack could invite damaging retaliation.[35] Those large-scale attacks could trigger the use of other information-age weapons or even nuclear weapons. The two force postures differ in their approaches to the autonomous risk of escalation created by information-age weapons, which Schelling defines as a risk that neither the state nor its adversary can fully control.[36] Brinkmanship postures stoke autonomous risk, whereas calibrated escalation postures try to smother it.

BRINKMANSHIP POSTURES. A brinkmanship force posture threatens to use information-age weapons to generate a high risk of uncontrolled escalation to nuclear war, which enables a state to gain coercive leverage at a lower cost. It exploits an adversary's fear that a large-scale counterspace, cyber, or conventional missile attack could cause a conflict to spin out of control. Features of the state's force posture encourage the adversary to assume the worst—that the state has postured its capabilities to create a serious risk that both states could imminently slide down the slippery slope to large-scale attacks. For example, the state might have delegated authority to use information-age weapons on strategic targets down the chain of military command, or to civilian hackers or space companies. This risk increases the incentive for the adversary to take the "last clear chance" to avoid disaster, by acquiescing to the state's demands.[37] If the adversary does not acquiesce, the state would launch an at-

34. Narang, *Nuclear Strategy in the Modern Era*, pp. 18–19.
35. Schelling, *Arms and Influence*, p. 99. Retaliatory-only information-age weapons postures optimized to deter in-kind attacks with threats of retaliation would not generate coercive leverage in a conventional war.
36. Ibid., pp. 92–97.
37. Ibid., pp. 44–45. See also Powell, "The Theoretical Foundations of Strategic Nuclear Deterrence," pp. 76–78.

tack in a crisis or early in a conflict that could trigger uncontrolled escalation, such as disrupting the adversary's ability to communicate with its military forces, killing civilians in its cities, or damaging components of its nuclear arsenal.

To be credible, a brinkmanship posture requires a clear capability to carry out information-age strategic attacks. It does not, however, require transparency about any other aspects of force posture. Opacity enables the state to claim that it has tied its hands when making threats. It prevents the adversary from verifying how much autonomous risk the state's force posture actually creates. North Korea's cyber force posture is an example of a brinkmanship posture. Little is known about North Korea's plans for using cyberattacks in a conflict, but it has demonstrated its willingness to conduct peacetime cyber operations that cause collateral damage, such as its 2017 WannaCry ransomware attack that crippled the National Health Service in England and Scotland.

CALIBRATED ESCALATION POSTURES. A calibrated escalation force posture also threatens to use information-age weapons to generate a risk of nuclear war, but a lower risk than brinkmanship. This alternative posture requires the state to pay a higher cost for using its coercive leverage below the nuclear threshold. It threatens attacks of increasing intensity, starting with small-scale attacks, giving both sides plenty of clear chances to avoid disaster. The state envisions coercive bargaining as a process in which the parties ascend rungs on a ladder: at each step, they reveal how much damage they are willing to absorb to achieve their aims. To keep control of that bargaining process, the state attempts to minimize the risk of uncontrolled escalation from small- to large-scale attacks, although that risk cannot be entirely eliminated.[38] If the adversary refuses to acquiesce to its political demands, the state carries out a controlled and limited attack—such as using a laser to burn a small, permanent spot in the optical sensor of an imaging satellite—anticipating that the adversary will most likely retaliate with equivalent force, or capitulate.[39] If it

38. Small-scale space, cyber, or precision missile attacks could trigger a chain reaction to large-scale use, although scholars debate whether escalation from a cyberattack could be controlled. See DeBlois et al., "Space Weapons," p. 66; Jacquelyn G. Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict," Ph.D. dissertation, George Washington University, 2017; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3 (2017), pp. 477–478, https://doi.org/10.1080/09636412.2017.1306396; and Paul M. Nakasone and Michael L. Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, August 25, 2020.
39. Kahn, *On Escalation*, pp. 9–10.

Table 1. Indicators of Cyber Force Posture

Indicators of Brinkmanship Posture	Indicators of Calibrated Escalation Posture
• lack of attribution and testing capabilities • transparent about capabilities; ambiguity over other posture components	• doctrine states intent to control escalation • attribution and testing capabilities to help control escalation • only top leaders have authority to order strategic cyberattacks • transparent about steps to reduce the autonomous risk of escalation

NOTE: A lack of attribution capabilities suggests that the state intends to use its offensive cyber capabilities before its adversary, rather than in retaliation. Testing capabilities for cyber operations suggest that a state seeks to reduce the likelihood of its attacks causing unintended effects.

does not capitulate, the state calibrates the intensity of follow-on strikes to the adversary's counterattacks.[40]

A calibrated escalation posture for information-age weapons is technologically and organizationally more demanding than a brinkmanship posture. It requires capabilities to initiate coercive bargaining with small-scale information-age attacks. It also requires top leaders to maintain their strict authority to order the use of large-scale attacks, which in turn requires infrastructure and procedures to prevent accidental or unauthorized use. The state might also try to minimize an adversary's misperceptions that could spark uncontrolled escalation, for example by clearly communicating red lines that define rungs on the ladder.[41] This posture also requires the state to have the capability to identify the source of space attacks or cyberattacks. Without this attribution capability, the state might mistakenly target the adversary when a third party carries out an attack, or vice versa. France's military cyber posture is an example of calibrated escalation. It publicly states France's intent to manage escalation risks and minimize collateral damage, and it adopts centralized command-and-control arrangements.[42] The indicators that distinguish these two force postures, applied to offensive cyber operations, are summarized in table 1.

40. Powell, "The Theoretical Foundations of Strategic Nuclear Deterrence," pp. 79–83.
41. James D. Morrow, "International Law and the Common Knowledge Requirements of Cross-Domain Deterrence," in Gartzke and Lindsay, eds., *Cross-Domain Deterrence*, pp. 188–192.
42. Ministère des Armées, "Éléments publics de doctrine militaire de lutte informatique offensive" [Public elements of a military doctrine for offensive cyber warfare] (Paris: Ministère des Armées, République Française, 2019), pp. 6–9.

The Theory of Strategic Substitution

China searched for substitutes to nuclear first use and conventional victories to gain coercive leverage in limited conventional conflicts that would be fought under the shadow of nuclear war. Like other nuclear-armed states, China faced leverage deficits when its threat environment changed, and it discovered that its capabilities were ill-suited for the type of war and adversary it was most likely to fight. Like other nuclear-armed states, China searched for coercive leverage to address those leverage deficits. But unlike those states, China's search for coercive leverage was constrained by both its inability to build up war-winning conventional capabilities and doubts that threats to use nuclear weapons first would be credible. Information-age weapons were a promising substitute because they signal that "the war is getting out of hand but is not yet beyond the point of no return."[43] They could enable a state to strike a delicate balance between achieving a coercive victory and avoiding the use of nuclear weapons.

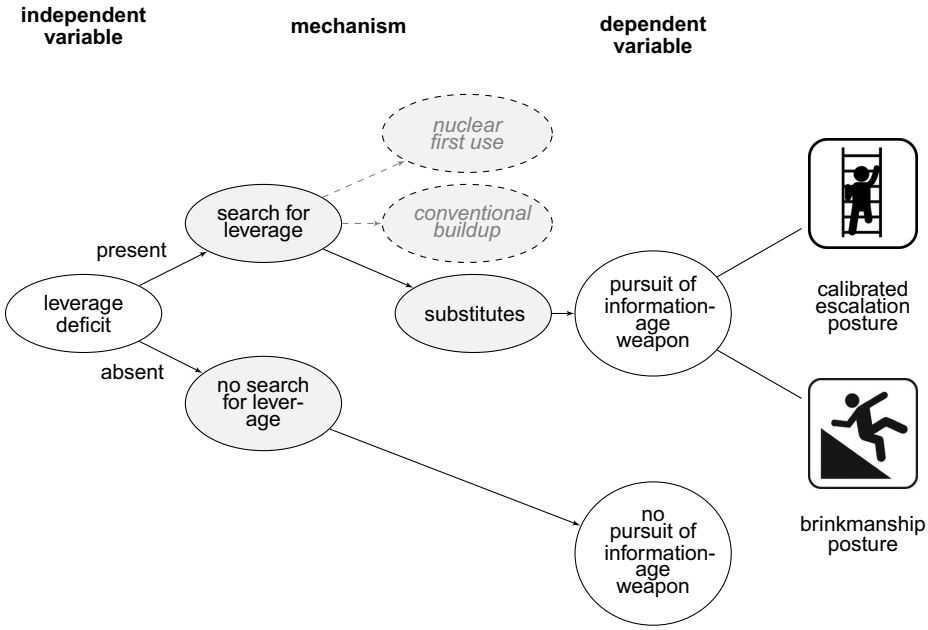
The theory of strategic substitution explains why China pursued information-age weapons in the post–Cold War era to gain coercive leverage against a nuclear-armed adversary. I argue that the existence of a leverage deficit (the independent variable) explains the decision to pursue a coercive counterspace, cyberattack, or precision conventional missile capability (the dependent variable) and the subsequent choice of force postures to configure the new capability to gain coercive leverage. In the absence of a leverage deficit, however, China had no incentive to pursue additional coercive capabilities because it had no reason to doubt whether the capabilities it was already developing would achieve its objectives in a limited war (see figure 1).

The theory assumes that China could have changed its nuclear posture but explains why that option could not address the strategic problem that it faced in the post–Cold War era. For the sake of parsimony, I assume that China is a unitary rational actor capable of accurately assessing both its own and its adversaries' strengths and weaknesses. Although the theory explains China's decision-making for all information-age weapons that it pursued to gain coercive leverage, this article focuses on China's decision-making for offensive cyber capabilities. I also examine an underappreciated but important influence on cyber force posture choices: a state's own vulnerability to cyberattacks.

---

43. Schelling, *Arms and Influence*, p. 113.

Figure 1. The Theory of Strategic Substitution



THE LIMITED WAR DILEMMA

States have three options to gain coercive leverage against a nuclear-armed adversary in a limited war, none of which fully resolve the dilemma of achieving war aims without risking nuclear catastrophe. The first option of threatening conventional victory has the advantage of being credible and enabling the state to impose its desired outcome on any noncompliant adversary, should coercive threats fail to achieve that outcome.[44] But conventional victories are costly and, especially for states facing conventionally stronger adversaries, deploying the required capabilities might not be feasible. Besides, nuclear-armed adversaries can always threaten nuclear first use to counter a conventional victory. The second option of threatening nuclear first use has the advantage of demonstrating a high level of resolve to an adversary. But nuclear threats are so destructive that they might not be credible. They might also threaten an adversary such that it overreacts in ways that worsen the state's security. A third

44. Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, N.J.: Princeton University Press, 1966), p. 9.

option is for the state to pursue the quicker and more credible alternative of coercive leverage that information-age weapons promise to provide.

Information-age weapons have both advantages and disadvantages when given a starring role in a state's answer to this limited war dilemma. Threatening to use these weapons could be more credible than nuclear threats and less costly than conventional victories, and these weapons use technology that many nuclear weapon states either already have or can easily acquire. But they are not a silver bullet. An adversary that remains undefeated conventionally can always continue to fight or threaten nuclear escalation.[45] Whether information-age weapons can effectively deliver on the promise that makes them so appealing—to coerce an adversary in a limited war while avoiding nuclear catastrophe—remains uncertain.

THE LEVERAGE DEFICIT

Changes in a state's threat environment can reveal a leverage deficit that encourages its leaders to search for additional coercive leverage. Those changes might include a crisis that increases the intensity of the threat posed by an existing adversary, the emergence of a new adversary, or the emergence of a new type of conflict that the state needs to prepare for.[46] A leverage deficit is present when a state's capabilities are ill-suited for the type of war and adversary that it is most likely to fight, and it would likely fail to achieve its objectives if a war with that adversary were to occur.

In response to a leverage deficit, a nuclear-armed state could build up its conventional military power, adopt a first-use nuclear posture, or search for substitutes. When a state cannot overcome its conventional inferiority and lacks confidence in the credibility of its threats to initiate the use of nuclear weapons, it faces incentives to search for alternative ways to increase its coercive leverage. In the absence of a leverage deficit, a state lacks the incentive to search for additional coercive leverage. China faced both of these constraints throughout the post–Cold War era. Once a leverage deficit was revealed, China's search for coercive leverage led it to recognize the advantages of relying on information-age weapons and the disadvantages of relying on a nuclear first-use posture or a conventional buildup. In the absence of a leverage deficit,

45. Mearsheimer, *Conventional Deterrence*, p. 56; and Bernard Brodie, *Strategy in the Missile Age* (Princeton, N.J.: Princeton University Press, 1965), pp. 334–335.
46. States might search for additional leverage because of an increase in wealth or foreign policy ambitions, but these changes do not create leverage deficits that require quick solutions.

China continued with its conventional military modernization plans and considered neither changing its nuclear posture nor pursuing substitutes.

CONVENTIONAL INFERIORITY. A state could pursue an information-age weapon because it has no conventional military option to increase its coercive leverage. States that are too weak to match an adversary's conventional military power often pursue asymmetric means of coercion to offset their military inferiority, such as sponsoring terrorist attacks or threatening to use nuclear weapons. They pursue information-age weapons for the same reasons. Some states have no hope of marshalling the resources to equal their adversary's conventional military power. But even for states that have the resources to catch up with an adversary's conventional military power in the long term, such a buildup would be slow and organizationally challenging. A conventionally weaker nuclear-armed state searching for leverage in the short term is likely to prioritize weapons that threaten escalation even if they do little to improve its prospects for fighting a limited war. Information-age weapons provide an attractive alternative for such a state to threaten escalation of a conflict against a nuclear-armed adversary while also signaling that it has not abandoned limits on its war aims—a key disadvantage of the readily available option of threatening nuclear escalation.[47] Information-age weapons are also a quicker fix for a leverage deficit because they use technology that nuclear weapon states either possess (missiles) or can easily acquire (cyberattack capabilities).[48]

NUCLEAR CREDIBILITY. A state that harbors doubts about the credibility of its threats to use nuclear weapons first in a limited conventional war is unlikely to judge that a first-use nuclear posture will address its leverage deficit. As Todd Sechser and Matthew Fuhrmann observe, "the combination of low stakes and high costs will render nuclear weapons impotent in most coercive [compellent] contexts, despite their unparalleled destructive power." If a state can survive without a segment of territory or defending a political principle, it will have a hard time convincing an adversary that it is willing to accept nuclear attacks

47. Threatening nuclear first use to compensate for conventional inferiority might be perceived as a signal of a state's aggressive and unlimited intentions. See Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security*, Vol. 37, No. 4 (Spring 2013), pp. 79–80, https://doi.org/10.1162/ISEC_a_00114; and Alex Weisiger, *Logics of War: Explanations for Limited and Unlimited Conflicts* (Ithaca, N.Y.: Cornell University Press, 2013), pp. 30–33.

48. Nuclear-armed states possess missile technology while the barriers to entry for rudimentary cyberattacks against an adversary's critical infrastructure are low. Lindsay and Gartzke, "Conclusion: The Analytic Potential of Cross-Domain Deterrence," p. 352.

on its homeland to deter an adversary from taking that territory or demolishing that principle.[49] In a limited war, the costs that nuclear use would generate for the state would far exceed the value of its political aims.[50]

By contrast, threats to use information-age weapons might be sufficiently damaging and risky to make an adversary change its calculations, but not so damaging or risky that the threat lacks credibility. Information-age weapons enable a state to increase the risk of all-out nuclear war without actually using nuclear weapons, which enhances the credibility of information-age weapons threats for two reasons. First, information-age weapons revive the significance of threats that leave something to chance, even in the presence of a robust nuclear stalemate. Limited nuclear attacks have difficulty creating threats that leave something to chance in those conditions because their use signals a willingness to endure and inflict destruction rather than to accept and manipulate the risk that both sides will lose control of the process of escalation.[51] Second, the burden of introducing nuclear weapons into the conflict after an information-age weapons attack falls on the adversary. Nuclear retaliation for an information-age weapons attack would likely be interpreted as disproportionate. Provided the adversary's retaliation for an information-age attack does not cross the nuclear threshold, it could be a price worth paying for a limited war aim.

Posture Choices

The search for coercive leverage does not end with a decision to pursue an information-age weapon: A state must adopt a force posture for that weapon to be able to use it strategically. Posture choices are likely to be influenced by a number of factors, such as China's strict civilian control over the PLA,[52] its pace of technological development, and adaptation as it gains experience with new military capabilities.[53] China's strict civilian control over the military favors a calibrated escalation posture that limits the autonomy of cyber operators, provided that the PLA is capable of meeting the posture's technological

49. Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York: Cambridge University Press, 2017), p. 57. See also pp. 50–51.
50. Clausewitz, *On War*, p. 92.
51. Powell, "The Theoretical Foundations of Strategic Nuclear Deterrence," pp. 75–96.
52. Phillip C. Saunders and Andrew Scobell, "Introduction: PLA Influence on China's National Security Policymaking," in Phillip C. Saunders and Andrew Scobell, eds., *PLA Influence on China's National Security Policymaking* (Palo Alto, Calif.: Stanford University Press, 2015), pp. 1–32.
53. Lyu, "A Chinese Perspective on the New Intelligence Framework."

and organizational requirements. But China's choices are also shaped by its vulnerability to cyberattacks.

Understanding how cyber vulnerability affects posture choices is theoretically important because it may be relevant to the choices that other nuclear-armed states might make about their cyber force postures. A state's vulnerability in outer space might similarly affect its choice of posture for counterspace weapons, another information-age capability. A state's vulnerability to cyberattacks is not tightly correlated with either its military cyberattack capabilities or its dependence on information networks to support conventional military operations. Information networks operated by civilians and the private sector also influence a state's vulnerability. A state has high vulnerability to cyberattacks if its society, government, and military provide many valuable assets that an adversary could target using offensive cyber operations. By contrast, a state has low vulnerability if it presents only a small set of low-value targets that could be damaged with a cyberattack, such as North Korea.[54] Cyber vulnerability influences a state's force posture choices because it affects the potential costs of retaliation that the state may face if it relies on threatening cyberattacks to gain coercive leverage.

A state that uses cyberattacks for coercive leverage must anticipate that its adversary will retaliate, either within or outside of cyberspace.[55] It cannot fully defend itself from a similarly armed adversary's cyberattacks. The more damaging the adversary's retaliation, the less credible the state's threats will be. As a result, the higher a state's cyber vulnerability is, the stronger its incentives to adopt a calibrated escalation force posture. The lower a state's vulnerability is, the more willing it might be to take a "high risk, high reward" brinkmanship approach to coercive bargaining in cyberspace. The prospect of in-kind retaliation for a state with high vulnerability to cyberattacks reduces the credibility of its threats to conduct the kind of risk-acceptant cyberattacks envisaged by a brinkmanship posture. A calibrated escalation posture ad-

54. Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, Calif.: RAND, 2008), p. 17; and Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security*, Vol. 44, No. 1 (Summer 2019), p. 76, https://doi.org/10.1162/isec_a_00351.

55. Lindsay and Gartzke, "Introduction: Cross-Domain Deterrence, from Practice to Theory," p. 4; Morrow, "International Law and the Common Knowledge Requirements of Cross-Domain Deterrence," pp. 188, 199; and Henry Farrell and Charles L. Glaser, "How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine," in Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, D.C.: Brookings Institution Press, 2019), pp. 45–80.

dresses this credibility problem. It reduces the likelihood of large-scale retaliatory cyberattacks by starting with small-scale attacks, which provides the adversary with an opportunity and an incentive to keep an exchange of cyberattacks limited.

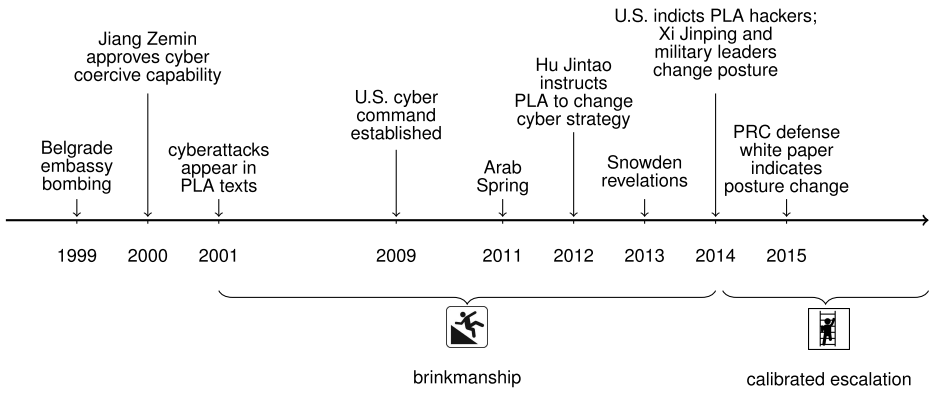
China's Cyber Force Posture

Offensive cyber capabilities are one of the three information-age weapons that China's leaders pursued in their search for coercive leverage in a Taiwan conflict scenario. China searched for substitutes for nuclear threats, which leaders did not think were credible, and war-winning conventional military capabilities, which China could not build in the immediate term. The bombing of the Chinese embassy in Belgrade in 1999 prompted the PLA to pursue a coercive cyberattack capability and adopt a brinkmanship cyber force posture in quick succession in the early 2000s. China's cyber vulnerability grew from low in 2000 to high by approximately 2010, as its dependence on information networks increased. In 2012, China's top leader, Hu Jintao, instructed the PLA to innovate its cyber force posture to take account of its growing vulnerability to cyberattacks. Hu's successor, Xi Jinping, approved China's change to a calibrated escalation cyber force posture in 2014. These decisions and other notable events outside China that concerned cyber capabilities are summarized in figure 2.

The case of China's cyber force posture decision-making offers an ideal opportunity to probe the plausibility of the theory of strategic substitution. Holding constant China's limited war aim to stop Taiwan from becoming a more independent country, I explain the effect that the presence or absence of leverage deficits over the past three decades has had on its cyber capabilities decision-making. I also show that China's cyber force posture had to change to stay credible because its vulnerability to cyberattacks increased. Compared with China's other information-age weapons capabilities, its cyber force posture decision-making is the most likely case for alternative explanations derived from the military innovation and diffusion literature. As a second-mover state, China could emulate the cyber force posture choices of first movers such as Russia and the United States. China's financial capacity to emulate those states also increased over the past three decades.

I use both congruence testing and process tracing to assess the explanatory power of the theory of strategic substitution compared with alternative explanations. To identify a decision to pursue a coercive cyberattack capability,

Figure 2. China's Cyber Force Posture Decisions



I examined annual speeches delivered by the Chinese Communist Party's top leader who serves as the chairman of the top military decision-making body, the Central Military Commission (CMC), at Commission meetings. I applied the indicators of calibrated escalation and brinkmanship cyber postures in table 1 to Chinese texts and secondary sources. To identify the periods when China faced a leverage deficit, I examined leaders' and PLA officers' assessments of the adequacy of China's leverage before and after crises with the United States. Debates among strategists about changing nuclear posture also demonstrate that nuclear first use was considered but ultimately regarded as a dead end in China's search for leverage.

THE DECISION TO PURSUE OFFENSIVE CYBER CAPABILITIES

In December 2000, General Secretary Jiang Zemin mentioned cyber warfare for the first time in a speech to the annual enlarged meeting of the CMC. He remarked that "information warfare has started to ascend into the arena of warfare, with electronic warfare and *computer network warfare* as its principal means" (emphasis added).[56] His speech implies that he was approving the PLA's pursuit of a cyberattack capability to gain coercive leverage. The other members of the CMC, China's top military leaders, likely drafted Jiang's speech for him, suggesting that the PLA strongly influenced the decision.

Before 2000, the PLA had dabbled in cyber capabilities but made no high-

56. Jiang, *Jiang Zemin wenxuan (san juan)*, p. 163.

level decision to focus on them as a means of warfighting or coercion. The PLA acknowledged that cyberattacks could be used strategically in 1992, when PLA publications reported that the U.S. military was researching "computer virus weapons," which would attack civilian and military targets to create chaos.[57] In 1995, they observed that cyberattacks "can be used to cause serious damage to C3I systems, informatized weapons and war potential."[58] "Informatized" weapons exploit information technology to increase their precision, lethality, and ability to network units to bring them under unified command.[59] Toward the end of the 1990s, the PLA researched and developed "computer virus warfare [*jisuanji bingdu zhan*]" capabilities and cyber defense capabilities for its newly automated command-and-control systems.[60] In January 1999, however, Vice-Chairman of the CMC Zhang Wannian mentioned that future conflicts would involve the space and electronic battlefields. He did not mention a cyber battlefield.[61]

The theory of strategic substitution would explain China's pursuit of a strategic offensive cyber capability as a response to a leverage deficit. In other words, a change in China's threat environment put its leaders on notice that they might not achieve their aims in a limited war with a nuclear-armed adversary. In the post–Cold War era, three crises with the United States confronted China's leaders with leverage deficits: the Taiwan Strait Crisis in 1995–1996, the Belgrade embassy bombing in 1999, and the collision between a U.S. EP-3 surveillance aircraft and a Chinese fighter jet in 2001. The theory would also expect decision-makers to justify their pursuit of information-age weapons for coercive leverage as a way to compensate for China's conventional inferiority with a more credible option than nuclear first use.

THE 1995–1996 TAIWAN STRAIT CRISIS LEVERAGE DEFICIT. After the 1995–1996 Taiwan Strait Crisis, China's leaders faced a leverage deficit against a nuclear-armed adversary in a limited war for the first time. China's search for leverage

57. Shao Pingfan, "Meijun zhongshi jisuanji bingdu de junshi yingyong yanjiu" [The U.S. military attaches importance to researching the military use of computer viruses], *Waiguo junshi xueshu* [Foreign Military Arts], No. 10 (1992), pp. 26–27.
58. Wang Baocun and Li Fei, "Manhua xinxi xhan" [An informal discussion of information warfare], *Jiefangjun bao* [People's Liberation Army Daily], June 13, 1995.
59. M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949* (Princeton, N.J.: Princeton University Press, 2019), p. 219.
60. Niu Li, ed., *Jundui Xinixihua Jianshe Zhanlue gailun* [Overview of the Military Informatization Development Strategy] (Beijing: Jiefangjun chubanshe, 2008), p. 51; and Tai Demin and Tong Zhongpu, "Junmin wangluo fenbu Datong Junfenqu wangluo fanghu jishu quebao xinxi anquan" [Datong Military Sub-Region cyber militia unit protects information security with cyber defense technology], *Jiefangjun bao* [People's Liberation Army Daily], July 21, 2003.
61. Guo Xiangjie, *Zhang Wannian zhuan (xia)* [The biography of Zhang Wannian] (Beijing: Jiefangjun chubanshe, 2011), p. 169.

began in earnest after that crisis, which confirmed that China's adversary in a future war would be the United States, a nuclear-armed state. China's starting point in that search was shaped by the twin legacies of its Cold War capabilities: a retaliatory nuclear posture, and a military incapable of seizing Taiwan with conventional forces (although it had the resources to modernize its military in the long term).[62] In the midst of that crisis, in December 1995, Zhang Wannian warned that "in a situation in which there is a disparity in our weapons equipment quality, the quantitative superiority of our military cannot substitute for the inferiority of our weapons quality."[63]

China's decision-makers did not think that they could credibly threaten to use nuclear weapons first against either Taiwan or a nuclear-armed opponent such as the United States. Before the crisis, they rejected a proposal put forward by some strategists that China adopt a limited nuclear deterrence posture to gain coercive leverage in local wars.[64] Local wars were the focus of PLA planning from 1988 onward. Debate about that proposal likely ended in 1992, when Jiang Zemin reaffirmed China's retaliatory nuclear posture.[65] That year, the PLA leadership reduced the military grade of those nuclear missile bases that had too few personnel or shorter-range nuclear missiles, which reduced their level of authority in the chain of command.[66] The Second Artillery, China's nuclear missile force, had to pay for range improvements to the first intercontinental nuclear ballistic missile, the DF-5, from its own budget after its requests for funding were denied.[67] Defense industry leader Qian Xuesen remarked in 1992 that "We absolutely do not wish to take them [nuclear weapons] to go scare and intimidate people."[68] A missile base commander in the early 1990s, Ge Dongsheng, also indicated that China could not threaten nu-

62. Eric Heginbotham et al., "The U.S.-China Military Scorecard" (Santa Monica, Calif.: RAND, 2015).
63. Guo, *Zhang Wannian zhuan (xia)*, p. 164.
64. Alastair Iain Johnston, "China's New 'Old Thinking': The Concept of Limited Deterrence," *International Security*, Vol. 20, No. 3 (Winter 1995/96), pp. 5–42, https://doi.org/10.2307/2539138.
65. Deng Lizhong, "Xinxi tiaojian xia Di'er Paobing he daodan zuozhan yunyong lilun yanjiu" [Research on the combat role of Second Artillery nuclear missile forces under informatized conditions], M.A. thesis, National Defense University, Beijing, 2004, p. 28.
66. Ge Dongsheng, *Nanwang lijian suiyue* [Memorable years sharpening the sword] (Beijing: Junshi kexueyuan chubanshe, 2016), pp. 150–151. PLA organizations are assigned a grade equal to that of its commander and political commissar. Grades are more important than ranks in the PLA, and they reflect the authority and responsibility assigned to an individual or organization. Kenneth W. Allen and John F. Corbett Jr., "Predicting PLA Leader Promotions," in Andrew Scobell and Larry Wortzel, eds., *Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College Press, 2004), pp. 257–277.
67. Ge, *Nanwang lijian suiyue*, p. 174.
68. Gu Jihuan, Li Ming, and Tu Yuanji, eds., *Qian Xuesen wenji* [Collected works of Qian Xuesen], Vol. 6 (Beijing: Guofang gongye chubanshe, 2012), p. 262.

clear use in a Taiwan conflict. Not only did China have a no-first-use policy, but "against our compatriots [*tongbao*] it is even more impossible to use nuclear weapons!"[69]

The 1995–1996 Taiwan Strait Crisis did not alter these credibility concerns about nuclear first use. Influential defense industry leader Zhu Guangya described the problems with threatening nuclear use shortly after the crisis in 1996. "The extreme increase in lethality" of war and weapons, culminating in the nuclear revolution, "has given rise to many political problems and has limited their use."[70] Zhu Guangya also indicated that using force more precisely and discriminately, including through the use of information warfare weapons, would achieve strategic aims with more flexibility, fewer lives lost, and lower resource demands.[71] In the midst of the 1995–1996 Taiwan Strait Crisis at the end of 1995, China also decided to sign the Comprehensive Nuclear Test Ban Treaty, which would prevent it from testing low-yield warheads that would have made a first-use posture more credible if it entered into force.[72]

Instead, China pursued more accurate conventional missiles—information-age weapons that could eventually threaten precision strikes—to gain coercive leverage. The capability to escalate a conflict using precision conventional missiles was also a substitute for the war-winning conventional capabilities that the PLA did not expect to realize for decades into the future. In the wake of the 1995–1996 Taiwan Strait Crisis, China's leaders decided to improve the accuracy, expand the size, and extend the range of the PLA's nascent conventional missile force.[73] In the late 1980s, the Second Artillery had responded to the PLA's shift to preparing for local wars by advocating for conventional missile units, which would ensure the relevance of the missile force in a future local war that was unlikely to go nuclear.[74] Conventional missiles, which became more accurate over time, were therefore a ready-made option to address China's leverage deficit prompted by the 1995–1996 Taiwan Strait Crisis.

China's leaders did not alter the policy settings that they had put in place after the 1995–1996 Taiwan Strait Crisis to gain coercive leverage from 1997 to

69. Ge, *Nanwang lijian suiyue*, p. 136.
70. Du Xiangwan, *Zhanlue kexuejia Zhu Guangya* [Strategist and scientist Zhu Guangya] (Mianyang, China: Yuanzineng chubanshe, 2009), p. 347.
71. Ibid., p. 347.
72. Alastair Iain Johnston, *Social States: China in International Institutions, 1980–2000* (Princeton, N.J.: Princeton University Press, 2007), pp. 100–101, 108–109. China would also need to ratify the treaty to be bound by its prohibition of nuclear testing.
73. Wang Xuedong, *Fu Quanyou zhuan (xia)* [Biography of Fu Quanyou] (Beijing: Jiefangjun chubanshe, 2015), p. 156; and Guo, *Zhang Wannian zhuan (xia)*, pp. 164–165.
74. Ge, *Nanwang lijian suiyue*, pp. 135–137.

1999 because they did not face a leverage deficit in this period. In addition to implementing their plans to develop a precision conventional missile force, leaders focused on the long, difficult process that they faced to close the gap with the world's most advanced militaries. In December 1997, Jiang Zemin laid out a development strategy for military modernization to be completed by 2050, assuming a favorable pace of economic development.[75] A few months before the Belgrade crisis, Jiang acknowledged that the military budget was "not yet sufficient" and China would need to take a "relatively low investment, relatively high efficiency" pathway to military modernization.[76]

THE BELGRADE LEVERAGE DEFICIT. China's decision to pursue a coercive cyberattack capability followed the NATO bombing of the Chinese embassy in Belgrade on May 8, 1999, during the Kosovo War. As the theory of strategic substitution would expect, the incident confronted China's leaders with a leverage deficit, which they ordered the PLA to address. During an emergency Politburo meeting after the bombing, Jiang Zemin exclaimed, "I'm shocked and indignant. This event is not a trivial matter, it is absolutely critical."[77] His remarks suggest that he viewed the bombing as intentional and causing a sharp deterioration in China's threat environment rather than accidental, as the United States claimed. He declared that "the Chinese people cannot be bullied!"[78] and instructed the CMC to strengthen the military to prevent future attacks on China.[79] The bombing was a wake-up call for China's leaders that the United States might act with similar hostility toward China to enable Taiwan's formal independence using military force. The General Staff Department (GSD) Chief of General Staff, Fu Quanyou, worried that "if the United States could engage in combat in the faraway lands of continental Europe, could it also one day in the future engage in armed interference in one of China's sensitive areas?"[80]

Jiang's instructions initiated a search for leverage that resulted in the pursuit of a coercive cyberattack capability by the end of 2000. Following the Politburo meeting, Zhang Wannian called an emergency CMC meeting, which brought together top military decision-makers to implement the Politburo's instruc-

75. Guo, *Zhang Wannian zhuan (xia)*, p. 19.
76. Jiang Zemin, *Lun Zhongguo xinxihua jishu chanye fazhan* [On the development of China's informatized technology industry] (Beijing: Zhongyang wenxian chubanshe, 2007), p. 128.
77. Jiang, *Jiang Zemin wenxuan (er juan)*, p. 321.
78. Ibid., p. 322.
79. Ibid., p. 323.
80. Wang, *Fu Quanyou zhuan (xia)*, pp. 206–207.

tions.[81] In response to the increased U.S. threat, Zhang implemented a PLA-wide initiative to change doctrine, operations, training, and equipment. He ordered the PLA to study the Kosovo War as a guide to both its own modernization and to identify U.S. weaknesses.[82]

Fu also organized meetings after the embassy bombing to formulate the PLA's response. He coordinated a nine-person "military technology small group [*junshi jishu xiaozu*]" to study the incident, which included representatives from the GSD, General Armaments Department, air force, Second Artillery, and space experts. The group's recommendations were submitted to the CMC later in May.[83] In October, on the CMC's instruction, the GSD, Academy of Military Science, and the CMC General Office formed a small group to research the Serbian militias' attacks on NATO forces. That group sent a report to the whole military encouraging the PLA to borrow from the Serbian example of attacking a stronger adversary.[84] Fu received CMC Vice-Chairman Zhang's approval to "strengthen information warfare [*xinxi zuozhan*] training and improve information confrontation [*xinxi duikang*] capabilities."[85] Both "information confrontation" and "information warfare" capabilities usually include cyberattacks, as well as other capabilities such as electronic warfare.

As the theory of strategic substitution would expect, China's conventional military inferiority constrained those PLA decision-makers who were tasked with addressing China's leverage deficit. Zhang instructed the PLA to study the successes and failures of the Serbian attacks on the United States in the short term, as well as the lessons of the Kosovo War for the PLA's long-term goal of catching up with U.S. conventional military power.[86] In a GSD meeting on March 26, 1999, Fu warned that "now and for a relatively long period into the future, the situation of overall military power in which 'the enemy is strong and we are weak' will fundamentally not change."[87] Instead, he indicated that China would have to find U.S. weaknesses and attack them with its current capabilities to "win from a position of inferiority [*yilie shengyou*]."[88]

81. Guo, *Zhang Wannian zhuan (xia)*, p. 416.
82. Ibid., p. 417.
83. Wang, *Fu Quanyou zhuan (xia)*, p. 208.
84. Ibid., p. 209.
85. Ibid., p. 308. See also p. 309.
86. Guo, *Zhang Wannian zhuan (xia)*, pp. 418–419.
87. Wang, *Fu Quanyou zhuan (xia)*, p. 302.
88. Ibid.

Although some PLA strategists recommended changing China's nuclear posture to address its leverage deficit, leaders once again rejected that option. Second Artillery officers suggested that China could publicly threaten to "lower the nuclear threshold," or even use its nuclear weapons first if it was losing a conventional conflict over Taiwan.[89] But even one of those officers acknowledged that cyberattacks would be more credible in a limited war.[90] Other PLA researchers observed that "information deterrence has more real credibility in military affairs" compared with nuclear deterrence.[91] It is not clear whether civilian leaders who had the authority to change China's nuclear posture actually considered doing so. But they did order strategists to stop discussing changes to China's nuclear posture by 2006.[92] Instead, Jiang Zemin emphasized the diversity of means making up China's strategic deterrent system [*duozhong shouduan peihe de zhanlüe weishe tixi*].[93]

The PLA viewed large-scale cyberattacks as a promising capability that it could use to gain coercive leverage against an adversary with superior conventional military capabilities. PLA researchers paid particular attention to cyberattacks because conventionally inferior Serbian forces had used them against NATO websites and email servers for leverage during the Kosovo War. One PLA report observed that, "in a situation where our information warfare capabilities cannot reduce the gap with developed countries within the short term . . . using computer virus weapons to counter enemies possessing advanced information systems, is, after all, an extremely effective method."[94] The authors of the report indicated that cyberattacks would allow China to confront a strong adversary using inferior armaments and exploit U.S. cyber vulnerability more quickly than it could build up its overall conventional military power.[95]

---

89. Deng, "Xinxi tiaojian xia Di'er Paobing he daodan zuozhan yunyong lilun yanjiu," p. 41; and Yu Jixun, *Di'er Paobing zhanyi xue* [The science of Second Artillery campaigns] (Beijing: Jiefangjun chubanshe, 2004), p. 294.
90. Deng, "Xinxi tiaojian xia Di'er Paobing he daodan zuozhan yunyong lilun yanjiu," p. 27.
91. Wang Zhongchun and Wen Zhonghua, *Busan de he yinyun: He wuqi yu he zhanlue, cong zuotian dao mingtian* [The unfading nuclear cloud: nuclear weapons and nuclear strategy, from yesterday to tomorrow] (Beijing: Guofang daxue chubanshe, 2000), p. 295.
92. Evan S. Medeiros, "'Minding the Gap': Assessing the Trajectory of the PLA's Second Artillery," in Roy Kamphausen and Andrew Scobell, eds., *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military* (Carlisle, Pa.: U.S. Army War College Press, 2007), p. 156.
93. Jiang, *Jiang Zemin wenxuan (san juan)*, p. 585.
94. Bin Huang, ed., *Kesuowo Zhanzheng yanjiu* [Research on the Kosovo War] (Beijing: Jiefangjun chubanshe, 2000), p. 160.
95. Ibid., p. 162.

China's Early Cyber Force Posture

Once Chinese leaders decided to pursue a coercive cyberattack capability, they needed to decide how to posture those capabilities to gain coercive leverage. The PLA adopted a brinkmanship force posture in approximately 2001 and established its first cyber military units in approximately 2002–2003.[96] Until 2014, China provided no transparency about its cyber force posture beyond exercising its capabilities, nor did it seek capabilities to minimize the risk of escalation from the use of cyberattacks.

A brinkmanship cyber force posture. The PLA's cyber doctrine between 2001 and 2014 envisaged using cyberattacks to both achieve military objectives in a war and gain coercive leverage against its adversaries, principally the United States.[97] PLA texts outlined that China would use cyberattacks either in a crisis to deter an adversary from initiating a war, or early in a conflict. In a conflict, cyberattacks would be used alongside kinetic and electronic weapons in an "information warfare campaign" to carry out preemptive attacks against an adversary's military sensors.[98] A 2004 PLA text indicated that cyberattacks on an adversary's civilian and military command-and-control computer systems would allow China to "upset troop morale and the morale of the people . . . destroy their will to resist, and achieve the goal of winning without fighting."[99]

These targets and effects were repeated in texts published in 2013, once the PLA had more experience operating in cyberspace. The 2013 *Science of Military Strategy* claimed that "the deterrence capability of cyber war is no weaker than conventional destructive strategic weapons. Once cyber war succeeds, it can cause an adversary's economic collapse and combat system paralysis."[100] In true brinkmanship style, the book also described how uncertainty about escalation to large-scale, damaging cyber hostilities could have a deterrent effect: "because of the frightening consequences and uncertainty of avoiding an enemy cyberattack, all countries do not dare to lightly start a cyberwar."[101]

---

96. Xue Xinglin, *Zhanyi lilun xuexi zhinan* [Campaign theory study guide] (Beijing: Guofang daxue chubanshe, 2001), p. 53; and author's interview, Beijing 2015.
97. Xue, *Zhanyi lilun xuexi zhinan*, pp. 52–53; and Shou Xiaosong, ed., *Zhanlue xue* [The science of military strategy] (Beijing: Junshi kexueyuan chubanshe, 2013), pp. 192–194.
98. Zhang Yuliang, *Zhanyi xue* [The science of military campaigns] (Beijing: Guofang daxue chubanshe, 2006), pp. 151–154; and Xue, *Zhanyi lilun xuexi zhinan*, pp. 52, 636.
99. Yu, *Di'er Paobing zhanyi xue*, p. 352.
100. Shou, *Zhanlue xue*, p. 191.
101. Ibid., p. 196.

PLA teaching materials continued to list "important enemy civilian cyber systems" as targets.[102]

PLA writings indicate that China's initial offensive cyber capabilities were rudimentary. As one officer described in 2013, "technological means to breach security and encryption measures of enemy computer networks and enter its networks are not yet mature."[103] Nonetheless, China's cyber capabilities were sufficient to implement a brinkmanship posture. PLA reports of its military exercises and U.S. government reports indicate that China developed capabilities by 2013 to conduct offensive cyber operations against tactical military and U.S. critical infrastructure targets.[104] PLA writings between 2005 and 2013 list various cyber surveillance, offense, and defense capabilities.[105] Although those writings do not indicate whether China pursued the capabilities listed in them, they systematically omit attribution and testing, which are two capabilities that help to reduce escalation risks in cyberspace.

Until 2014, varied command-and-control arrangements for PLA cyber units would have created an autonomous risk of escalation in cyberspace in a U.S.-China conflict. The United States could not have been sure that China's leaders would have been able to prevent PLA operators from carrying out China's most damaging cyber operations in a crisis or conflict. Between 2002 and 2015, more than a dozen different PLA units subject to different command-and-control arrangements were capable of conducting cyber espionage or attacks.[106] The units that were most likely assigned the mission of carrying out

---

102. Zhou Xinsheng, ed., *Junzhong zhanlue jiaocheng* [Study guide to military service strategy] (Beijing: Junshi kexueyuan chubanshe, 2013), p. 126. See also Ye Zheng, ed., *Xinxi zuozhan xue jiaocheng* [Study guide to information warfare] (Beijing: Junshi kexueyuan chubanshe, 2013), p. 109.

103. Xu Guoxing, *Wo jun xinxi zuozhan liliang jianshe yanjiu* [Research on developing our military's information warfare capabilities] (Beijing: Junshi kexueyuan chubanshe, 2013), p. 113.

104. Wang Yi, ed., *Wangluo kongjian anquan zhanlue yanjiu: Zhongguo Junshi Kexue Xuehui Jundui Zhihui Fenhui 2012 nian youxiu wenxuan jibian* [Cyberspace security strategy research: China Association for Military Science Military Command Division 2012 selected best works] (Beijing: Guofang daxue chubanshe, 2013), p. 399; and Cybersecurity and Infrastructure Security Agency [CISA], "Alert (AA21-201A) Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," CISA, July 21, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-201a.

105. See Xinxi Zuozhan Lilun Yanjiushi [Information Warfare Theory Research Office], ed., *Xinxihua zuozhan lilun xuexi zhinan* [Guide to the study of informatized warfare] (Beijing: Junshi kexueyuan chubanshe, 2005), pp. 238–239; Ye Zheng, *Xinxihua zuozhan gailun* [Theory of information warfare] (Beijing: Junshi kexueyuan chubanshe, 2007), p. 393; and Shou, *Zhanlue xue*, p. 196.

106. Wang, *Wangluo kongjian anquan zhanlue yanjiu*; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, Pa.: Strategic

large-scale offensive cyber operations for strategic effects were in the GSD Fourth Department.[107] Together with cyber espionage units directly commanded by the GSD Third Department,[108] those units were under strict control of the CMC. A PLA textbook published in 2013 stated that strategic-level cyberattacks would be carried out "under the direct control of the highest supreme command [*tongshuai bu*]."[109]

In practice, however, the ability to authorize cyberattacks might have been delegated down the chain of command. Third Department units engaged in industrial espionage without the explicit approval of top leaders.[110] Therefore, top leaders lacked effective mechanisms to oversee at least some (if not all) PLA cyber operations, whether by accident or design. Although those units were tasked with espionage, China's adversaries would have to assume that they were also capable of carrying out offensive cyber operations because the methods of intruding into adversary networks for espionage and attack preparations are the same.[111]

China actively denied the existence of the PLA's cyberattack and espionage capabilities.[112] But cyber intrusions conducted by PLA units signaled the types of strategic targets that they might attack in a crisis or conflict. In 2014 testimony before a congressional committee, the commander of U.S. Cyber Command, Admiral Michael Rogers, did not refute claims that Chinese government hackers had penetrated U.S. critical infrastructure systems.[113] The U.S. government later confirmed that Chinese state-sponsored intrusions

---

Studies Institute, U.S. Army War College Press, 2009), p. 274; and Mark A. Stokes, "The Chinese People's Liberation Army and Computer Network Operations Infrastructure," in Lindsay, Cheung, and Reveron, eds., *China and Cybersecurity*, pp. 164–165.

107. Stokes, "The Chinese People's Liberation Army and Computer Network Operations Infrastructure," pp. 174–175.

108. Ibid., pp. 169–173.

109. Ye, *Xinxi zuozhan xue jiaocheng*, p. 109.

110. Author's interviews, Beijing, 2016 and Shanghai, 2016.

111. Shou, *Zhanlue xue*, p. 192; and Ye, *Xinxi zuozhan xue jiaocheng*, p. 70.

112. See, for example, "Former Defense Official Denies Chinese Hacking," *Xinhua News Agency*, March 3, 2013, http://www.china.org.cn/china/Off_the_Wire/2013-03/03/content_28115908.htm. Some Chinese experts also questioned the authoritativeness of PLA writings, such as the 2013 edition of the *Science of Military Strategy* published by the Academy of Military Science. Author's interviews, Beijing, 2015.

113. Hearing on "Cybersecurity Threats: The Way Forward," before the Select Comm. On Intelligence, 113th Cong., 2d sess., November 20, 2014 (transcript of Admiral Michael S. Rogers, Commander, U.S. Cyber Command), https://www.nsa.gov/Press-Room/Speeches-Testimony/Article-View/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/.

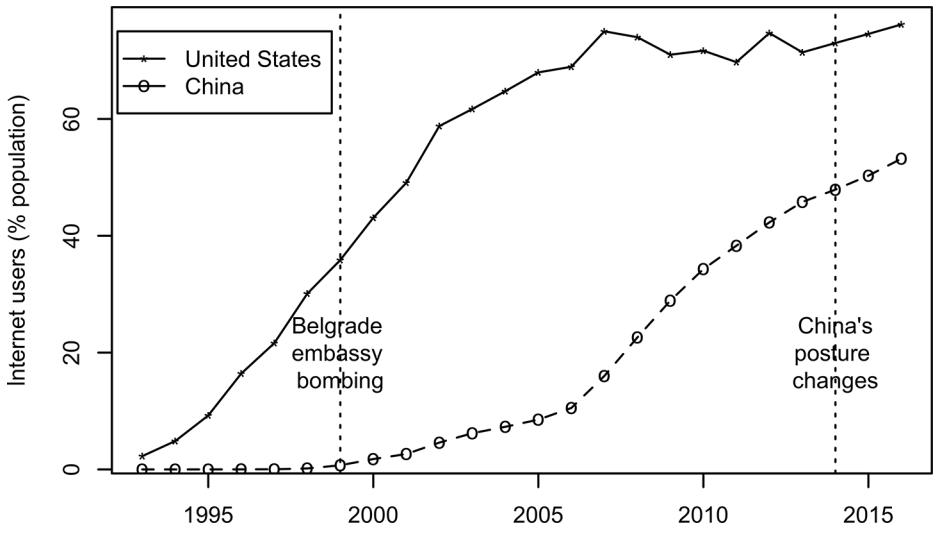
into oil and natural gas industrial control systems between 2011 and 2013 were conducted specifically for "the purpose of holding U.S. pipeline infrastructure at risk."[114]

LOW CYBER VULNERABILITY. China's low vulnerability to cyberattacks around 2000 enabled it to credibly threaten a brinkmanship posture. The 2000 *Science of Military Campaigns* acknowledged that cyberattacks were "one of the most effective means for militaries that are weak in their overall weapons equipment to confront strong militaries." The authors wrote that technologically advanced states face a dilemma: Advanced technology is key to maintaining military superiority but "on the other hand, the more developed their information technology, the closer their information links with the entire world, the weaker the protection of their information systems, and the greater the harm that logic [cyber] attacks can produce."[115] The *Science of Second Artillery Campaigns*, published a few years later, also acknowledged that high vulnerability to cyberattacks could be exploited by an adversary: "There are more targets to attack using information weapons in countries or militaries with strong technological, economic power."[116]

China had an opportunity to gain coercive leverage at a low cost by adopting a brinkmanship posture because of its low vulnerability to cyberattacks. As figure 3 shows, only 0.7 percent of China's population had Internet access in 1999 compared to over 40 percent in the United States. Chinese experts recognized that opportunity. He Dequan, an academician of the Chinese Academy of Engineering, wrote in 1997 that "poor adversaries can use low-cost strategic information warfare means to attack the United States, all types of the U.S. homeland's very large infrastructure are exposed to those attacks."[117] A 2000 PLA report on the lessons of the Kosovo War explained that China could take advantage of the U.S. military's vulnerability to cyberattacks because "the United States constructed the world's most developed and complex information network, but . . . its vulnerability is also the greatest."[118] But in 2001, PLA officers were already warning that China's society, economy, and

114. CISA, "Alert (AA21-201A) Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013."
115. Wang Houqing and Zhang Xingye, eds., *Zhanyi xue* [The science of military campaigns] (Beijing: Guofang daxue chubanshe, 2000), p. 174.
116. Yu, *Di'er Paobing zhanyi xue*, p. 341.
117. He Dequan, "Meiguo xinxi zhan zhanlue de tiaozheng" [Adjustments to U.S. strategic information warfare], *Waiguo junshi xueshu* [Foreign Military Arts], No. 2 (1997), p. 6.
118. Bin, ed., *Kesuowo Zhanzheng yanjiu*, p. 162.

Figure 3. Internet Penetration Rate in China and the United States



SOURCE: Data are from "World Development Indicators," World Bank, accessed October 1, 2020, https://datacatalog.worldbank.org/dataset/world-development-indicators.

military command networks were vulnerable and would become increasingly so in the future.[119]

CHANGING CYBER FORCE POSTURE

China's pursuit of offensive cyber capabilities to gain coercive leverage in the early 2000s was a gamble on a promising but uncertain new capability. While China's leaders remained committed to that gamble as the PLA learned more about offensive cyber capabilities, the credibility of its brinkmanship cyber threats diminished as China's cyber vulnerability grew. In 2014, General Secretary Xi Jinping and military leaders changed the PLA's brinkmanship cyber force posture to a calibrated escalation posture. The change signaled that China would still use cyberattacks strategically for coercive leverage. But it tried to smother the autonomous risk of escalation to avoid an exchange of damaging, large-scale cyberattacks with the United States that could trigger a

119. Zhang Tianping, *Zhanlue xinxi zhan yanjiu* [On strategic information operations] (Beijing: Guofang Daxue chubanshe, 2001), pp. 250–254.

nuclear war. The abrupt changes in key elements of China's cyber posture after 2014 suggests that those changes are not adequately explained by PLA adaptation to its maturing cyber capabilities.

A CALIBRATED ESCALATION CYBER FORCE POSTURE. Since 2015, China's cyber force posture has satisfied three of the four indicators of a calibrated escalation posture listed in table 1. First, PLA doctrinal writings state that China intends to control cyber escalation. Second, the PLA is developing attribution and cyberattack testing capabilities to minimize the autonomous risk of escalation from the use of offensive cyber operations. And third, China has taken steps to ensure that its top military and civilian leaders exercise strict control over the strategic use of cyberattacks. Although China has revealed more information about its cyber posture since 2014, its steps to reduce the autonomous risk of escalation (the fourth indicator) are not transparent enough to reassure an adversary.

Offensive cyber capabilities remain an important source of coercive leverage for the PLA despite China's high vulnerability to cyberattacks. To reconcile this tension, China officially stated that it intends to control the escalation of cyber conflict. A defense white paper published by the government in May 2015 outlined China's national security goals in cyberspace, which included "to stem [*e'zhi*] serious cyberspace crises."[120] It also officially recognized the existence of China's military cyber forces for the first time. By 2015, the head of the GSD Informatization Department, Senior Colonel Wang Kebin, assessed that China's increased reliance on cyberspace gave its "national security an unprecedented strategic weakness" because its economy, society, and critical infrastructure were vulnerable to strategic cyberattacks.[121] Major General Hao Yeli warned that cyberattacks could trigger a conventional conflict.[122] Nevertheless, the benefits of cyberattacks still vastly exceeded their risks.[123] The 2015 *Science of Military Strategy* claimed that cyberattacks could have "formidable

120. State Council Information Office, People's Republic of China, *Zhongguo de junshi zhanlue* [China's Military Strategy] (Beijing: Renmin chubanshe, 2015), p. 15.
121. Wang Kebin, "Jiangding buyi zou Zhongguo tese xinxi qiangjun zhilu" [Resolutely take the path of strengthening the military through informatization with Chinese characteristics], *Zhongguo junshi kexue* [China Military Science], No. 2 (2015), p. 2.
122. Hao Yeli, "Dui Meiguo jiakuai wangluo zhan fazhan de jidian sikao" [Some thoughts on the U.S. rapid development of cyber warfare], *Waiguo junshi xueshu* [Foreign Military Arts], No. 8 (2015), p. 5.
123. Li Zhaorui, ed., *Wangluo zhan jichu yu fazhan qushi* [The foundations and development trends of cyber war] (Beijing: Jiefangjun chubanshe, 2015), p. 19.

coercive power [*weishe li*] similar to a nuclear attack and even directly achieve war aims."[124]

It is not clear whether the PLA has amended its information warfare campaign to reflect China's goal of managing cyber escalation. In November 2020, the PLA updated its operational doctrine for the first time since 1999.[125] Although information about the content of that doctrine is not publicly available, it likely includes doctrine for offensive cyber operations. PLA exercises in 2017 involved joint information warfare formations, suggesting that PLA operational doctrine still includes an information warfare campaign.[126] China has likely raised the threshold for attacking an adversary's homeland critical infrastructure with cyber capabilities since 2014. In 2016, Chinese experts did not think that the PLA would use strategic cyberattacks against civilian targets in a crisis to deter the outbreak of war.[127] China demonstrated its ability to exploit critical infrastructure networks in preparation for offensive cyber operations during the Sino-Indian border conflict in 2020.[128]

The PLA is pursuing capabilities to better manage escalation during an exchange of cyberattacks. In a major speech on national cybersecurity policy in 2016, Xi Jinping instructed China's military, the government, and private industry to "strengthen its cyber defense and deterrence capabilities" by acquiring equivalent technology to its adversaries and balancing its own offensive and defensive capabilities.[129] To implement those instructions, the PLA took steps to improve the precision and effectiveness of its cyberattacks. A cyberattack testing capability would allow the PLA to better manage escalation risks since "cyberattacks can easily entangle innocent parties or cause rapid escalation [*tiaoyueshi shengji*], requiring precise control of the attack

124. Xiao Tianliang, ed., *Zhanlue xue* [The science of military strategy] (Beijing: Guofang daxue chubanshe, 2015), p. 211. This observation was repeated in the 2017 and 2020 revised editions of the same text. See Xiao Tianliang, ed., *Zhanlue xue*, rev. ed., (Beijing: Guofang daxue chubanshe, 2017), p. 228; and Xiao Tianliang, ed., *Zhanlue xue*, rev. ed., (Beijing: Guofang daxue chubanshe, 2020), p. 236.
125. "China's Guidelines on Joint Operations Aim for Future Warfare: Defense Spokesperson," *China Military Online*, November 27, 2020, http://english.scio.gov.cn/pressroom/2020-11/27/content_76954237.htm.
126. Dennis J. Blasko, Elsa B. Kania, and Stephen Armitage, "The PLA at 90: On the Road to Becoming a World-Class Military?" *China Brief*, Vol. 17, No. 11 (August 17, 2017).
127. Author's interviews, Beijing, 2016 and Shanghai, 2016.
128. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector/.
129. Xi Jinping, *Zai wangluo anquan he xinxihua gongzuo jiangtan hui shang de jiangzuo* [Speech at the cybersecurity and informatization discussion symposium] (Beijing: Renmin chubanshe, 2016), p. 18.

scope and strength, reducing 'collateral harm,' [and] achieving the ability to execute and stop an attack at will."[130] China has developed attribution capabilities as part of its investment in cyber situational awareness,[131] which enable it to correctly identify and retaliate against the actual perpetrator of a cyberattack. Xi acknowledged the PLA's progress toward these goals in a 2018 speech, indicating that China's "cybersecurity deterrence capability to strike back continues to grow" and that a "detection capability is a kind of deterrent capability."[132] He observed that China "continues to advance in the direction of balancing offensive and defensive cyber power."[133]

China began to reduce its reliance on computer network infrastructure, hardware, and software produced overseas in 2013 to reduce its vulnerability to cyberattacks. Chinese strategists feared that technology imports had compromised security features.[134] Xi acknowledged China's vulnerability given its dependence on foreign technology in 2013, remarking that "we are controlled by someone else [*shouzhi yuren*] in some critical [computer system and core 'informatization'] technologies and equipment."[135] Reducing reliance on foreign technology became a major policy goal in China's 13th Five Year Plan in 2015.[136]

Following sweeping military reforms at the end of 2015, China is likely to have strict command-and-control arrangements in place for strategic-level cyberattacks through the PLA's Strategic Support Force (SSF), although some uncertainty remains about the roles and authorities of cyber units outside of that force. PLA researchers recognize that cyberattacks "imply the escalation

130. Zhang Shibo, *Zhanzheng xin gaodi* [The new high ground of warfare] (Beijing: Guofang daxue chubanshe, 2016), pp. 91, 94. See also Xiao, *Zhanlue xue* (2015), pp. 387, 390–391.
131. Xi, *Zai wangluo anquan he xinxihua gongzuo jiangtan hui shang de jiangzuo*, p. 18; and State Council Information Office, *Zhongguo de junshi zhanlue*, p. 15. As of 2022 the Chinese government has not yet publicly attributed cyber operations to a foreign state.
132. Zhonggong Zhongyang Dangshi he Wenxian Yanjiuyuan [Central Party History and Documents Research Institute], ed., *Xi Jinping guanyu wangluo qiangguo lunshu zhaibian* [Extracts from Xi Jinping's expositions on a cyber superpower] (Beijing: Zhongyang wenxian chubanshe, 2021), pp. 9, 99.
133. Ibid, p. 44.
134. Zhang Yang, ed., *Jiakuai tuijin guofang he jundui xiandaihua* [Accelerating and advancing defense and military modernization] (Beijing: Dangjian duwu chubanshe, 2015), p. 22.
135. Zhonggong Zhongyang Wenxian Yanjiu Shi [Central Party Documents Research Office], *Xi Jinping guanyu keji chuangxin lunshu zhaibian* [Extracts from Xi Jinping's expositions on science and technology innovation] (Beijing: Zhongyang wenxian chubanshe, 2016), p. 45.
136. "'Shi San Wu' Guihua Gangyao: Shishi wangluo qiangguo zhanlue, jiakuai jianshe shuzihua Zhongguo" ["13th Five Year Plan" planning regulation: Implementing the strategy of a cyber superpower, accelerating the establishment of a digitized China], Cyberspace Administration of China, March 18, 2016, http://www.cac.gov.cn/2016-03/18/c_1118372649.htm.

of warfare and must be controlled from a high strategic level."[137] Establishing an "authoritative" and "unified" command structure would also help PLA cyber forces to fight more effectively.[138]

The SSF, established on December 31, 2015, consolidated cyber units previously scattered throughout the PLA into one organization, its Network Systems Department. SSF units were mostly drawn from the former GSD Third and Fourth Departments,[139] but also included some cyber espionage units formerly commanded by the services and Military Regions.[140] The SSF is believed to command both intelligence and strategic-level cyberattack units, both of which are under strict command and control.[141] These arrangements signal to an adversary that China's leaders directly control their most damaging offensive cyber capabilities. Nevertheless, the PLA's new Theater Commands, which replaced its Military Regions at the end of 2015, are likely to retain some cyber capabilities through regionally aligned SSF units. The command-and-control arrangements for those units, and the types of adversary networks that they would target, remain unclear.[142] The PLA has also established a Joint Staff Department Network-Electronic Bureau outside of the SSF, whose cyberattack authorities are similarly unclear.[143]

Although China has become more transparent about its military cyber posture since 2015, it is not transparent enough to reassure the United States that all possible steps have been taken to smother the autonomous risk of escalation from the PLA's use of offensive cyber operations. In December 2016, China released a National Cyberspace Security Strategy, which listed the kinds of networks that it designated as critical infrastructure and offered some insights into China's threshold for a cyberattack with strategic effects.[144]

---

137. Xiao, *Zhanlue xue* (2017), p. 229.
138. Zhang, *Zhanzheng xin gaodi*, p. 88.
139. Costello and McReynolds, *China's Strategic Support Force*, pp. 23–25.
140. John Costello, "The Strategic Support Force: China's Information Warfare Service," *China Brief*, Vol. 16, No. 3 (February 8, 2016).
141. Costello and McReynolds, *China's Strategic Support Force*, pp. 49–50.
142. An Weiping, "Zhuoyan wangluo qiangguo tuijin wangxin junmin shendu ronghe" [Advancing cyber and information civilian and military deep fusion from the perspective of a cyber superpower], *Junmin ronghe* [Civil-Military Fusion], Vol. 4 (2015), p. 61; and John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context* (Washington, D.C.: National Defense University Press, 2021), pp. 163–168.
143. Kania and Costello, "Seizing the Commanding Heights," p. 12; and Costello and McReynolds, *China's Strategic Support Force*, pp. 27, 33.
144. "Guojia Wangluo Kongjian Anquan Zhanlue" [National Cyberspace Security Strategy], *Xinhua News Agency*, December 27, 2016, http://news.xinhuanet.com/politics/2016-12/27/c_1120196479.htm.

By consenting to the 2014–2015 UN Group of Governmental Experts report, which it reaffirmed through UN processes in 2021, China tacitly approved a norm against targeting critical infrastructure networks with cyberattacks in peacetime.[145]

Nevertheless, the PLA has no declaratory policy outlining how it would use its offensive cyber capabilities in a crisis or conflict, nor does it provide any information about its organizations and doctrine for those capabilities. Around 2017, the Foreign Ministry reportedly opposed the use of the term "cyber deterrence" to describe China's cyber force posture in public statements because it implied the militarization of cyberspace and was inconsistent with China's diplomatic stance opposing the militarization of outer space.[146] Yet both Xi Jinping and the PLA have used the term "cyber deterrence [*wangluo weishe*]." This tension is reflected in China's International Strategy of Cooperation on Cyberspace, released in March 2017, which opposes "the tendency of militarization and deterrence buildup in cyberspace" without explicitly condemning "cyber deterrence."[147]

HIGH CYBER VULNERABILITY. The rapid increase in China's cyber vulnerability in the decade after 2001 reduced the credibility of the PLA's brinkmanship cyber force posture. The growth in Internet usage within Chinese society, the economy, the government, and the PLA increased the number, variety, and value of China's information networks that a foreign state could attack. As figure 3 shows, the percentage of China's population with Internet access reached 30 percent by 2009 and over 50 percent by 2016. PLA efforts to establish its own information networks also created valuable military cyber targets for an adversary to attack.[148]

From 2001 to 2010, other states' actions indicated to China's leaders that they faced an increasing diversity and severity of cyber threats. Protest movements such as the Color Revolutions in the early 2000s and the Arab Spring,

145. Author's interviews, Beijing, 2016; UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, July 22, 2015, https://digitallibrary.un.org/record/799853?ln=en#record-files-collapse-header; UN Secretary-General, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, July 14, 2021, https://digitallibrary.un.org/record/3934214?ln=en; and UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*, A/AC.290/2021/CRP.2, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
146. Author's interview, Shanghai, 2017.
147. "Full Text: International Strategy of Cooperation on Cyberspace," *Xinhua News Agency*, March 1, 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm.
148. Niu, *Jundui xinixihua jianshe zhanlue gailun*, p. 58.

beginning in late 2010, demonstrated the potential for the Internet to stoke social unrest.[149] Incidents such as Russian cyberattacks on Georgian infrastructure during the Russia-Georgia War in 2008 and the subsequent U.S.-Israeli cyberattacks on the Iranian nuclear program demonstrated the potential of cyber operations.[150] The revelations of Edward Snowden about the extent of U.S. surveillance programs in 2013 accentuated the risk to China's leaders of relying on foreign hardware, software, and Internet infrastructure.[151] The establishment of the U.S. Cyber Command in 2009 highlighted the increasing prominence of military cyber capabilities.[152] In May 2014, the United States indicted five PLA officers for cyber-enabled intellectual property theft and showcased U.S. cyber attribution capabilities. Chinese experts realized that online anonymity would not shield a hacker from U.S. retaliation.[153] These foreign demonstrations of cyber capability threatened China because of its increasing Internet dependence.

By 2012, China's top civilian leaders instructed the PLA to remedy the disjuncture between the country's growing vulnerability to cyberattacks and its brinkmanship posture. When General Secretary Hu Jintao took up chairmanship of the CMC in December 2004, he instructed the PLA to carry out a "New Historic Mission," which included defending China's expanding national interests in the electromagnetic and space domains.[154] In a work report to the 18th Party Congress as he left office in 2012, Hu reiterated the PLA's New Historic Mission but replaced the "electromagnetic domain" with the "cyber domain."[155] He instructed the PLA to further develop its cyber strategy.[156]

The PLA identified a multitude of cyber threats that had sprung up in the

149. Author's interviews, Beijing, 2016 and Shanghai, 2017; and Xiao, *Zhanlue xue* (2015), pp. 143–144.
150. Ye, *Xinxi zuozhan xue jiaocheng*, p. 55; and Xiao, *Zhanlue xue* (2015), p. 145.
151. Author's interview, Shanghai, 2017.
152. Author's interviews, Beijing, 2016, Shanghai, 2016, and Shanghai, 2017; Lü Jinghua, *Meiguo wangluo kongjian zhan sixiang yanjiu* [A study of U.S. thought on cyber warfare] (Beijing: Junshi kexueyuan chubanshe, 2014), pp. 232–239; and Lü Jinghua and Gou Huanlei, "Cong Meiguo fangbu xinpian 'Wangluo Kongjian Zhanlue' kan Meijun wangluo zuozhan fazhan qushi" [Trends in the U.S. military's development of cyber operations from its "Cyberspace Strategy"], *Waiguo junshi xueshu* [Foreign Military Arts], No. 7 (2015), pp. 39–43.
153. Author's interviews, Beijing, 2016.
154. Hu Jintao, *Hu Jintao wenxuan (di'er juan)* [Selected works of Hu Jintao (volume 2)] (Beijing: Zhongyang wenxian chubanshe, 2016), pp. 256–262.
155. "Hu Jintao qiangdiao gaodu guanzhu haiyang, taikong, wangluo kongjian anquan" [Hu Jintao emphasizes high level attention to maritime, space, and cyberspace security], *Haijun Wang* [Navy Online], November 8, 2012, http://mil.jschina.com.cn/system/2012/11/08/015164898.shtml.
156. Wang, *Wangluo kongjian anquan zhanlue yanjiu*, p. 1.

decade since it adopted a brinkmanship cyber posture. In December 2012, the PLA's China Association for Military Sciences convened a meeting to begin formulating a new cyber force posture that was appropriate for China's high cyber vulnerability.[157] The 2012 meeting highlighted four cyber threats: (1) "being controlled by others" because of foreign technology dependence; (2) China's weak position in international political, economic, and diplomatic competition over Internet governance; (3) everyday threats such as cyber crime; and (4) the "militarization" of cyberspace.[158] PLA researchers worried about cyber threats to China's critical infrastructure.[159] They also worried about the military's vulnerability to cyberattacks given its increased reliance on computer networks as part of a PLA-wide "informatization" effort to apply information technology to all aspects of military operations since the early 2000s. The military had neglected cyber defenses in that process.[160] National Defense University scholars described how "some [military] units fundamentally have not established who is responsible for cyber and information security, they immediately install one when they are inspected by superiors."[161]

PLA participants at the 2012 conference recognized that one of the biggest challenges they faced was to account for the vulnerability of China's civilian networks to cyberattacks in military cyber force posture. As one participant remarked, China's "state of affairs is clearly inappropriate for current world cyber and information security development trends, inappropriate for our country's expanding strategic interests, and inappropriate for the fundamental requirements of winning a local war under informatized conditions."[162] China's high cyber vulnerability made a brinkmanship cyber posture both inadequate and dangerous. The PLA needed to coordinate military cyber strategy with the rest of the government to adequately protect Chinese interests in cyberspace.

PLA officers singled out its delegated cyber command-and-control arrangements as one of the main problems with its brinkmanship posture. As an officer from the Jinan Military Region headquarters observed, if the management of cyber warfare operations is inappropriate, then "at the very least . . .

157. Ibid.
158. Ibid., p. 8.
159. Zhou Dewang, Fu Xiaodong, and Li Rui, "Lun wangkong duikang" [On cyberspace confrontation], *Zhongguo junshi kexue*, No. 4 (2014), p. 189.
160. Xu, *Wo jun xinxi zuozhan liliang jianshe yanjiu*, p. 114; and Lü, *Meiguo wangluo kongjian zhan sixiang yanjiu*, p. 242.
161. Wang, *Wangluo kongjian anquan zhanlue yanjiu*, p. 82.
162. Ibid., p. 9.

our operational intentions are revealed, at its most serious our overall national political and diplomatic situation is influenced."[163] Delegated command-and-control arrangements also hampered the PLA's ability to use its cyber capabilities in military operations. The same officer commented that "each cyber warfare force is fighting its own war [*gezi weizhan*]."[164] Although PLA officers called for a more centralized, comprehensive, regular cyber force with a stronger command-and-control structure, it took another three years to implement those changes. As some scholars of military innovation would expect,[165] the PLA's organizational inertia slowed its response to changes in China's cyber vulnerability. Hu Jintao, a civilian leader, had to intervene to catalyze change.

THE DECISION TO CHANGE POSTURE. One of the key reasons why China's leaders changed the country's cyber force posture in 2014 was to ensure that it could continue to credibly threaten large-scale cyberattacks. A calibrated escalation force posture was less damaging and more credible for a country with high vulnerability to cyberattacks. China's attribution capabilities and more visible cyber forces enabled it to better deter and defend against both in-kind retaliation (for using cyberattacks for coercive leverage) and unprovoked cyberattacks. A calibrated escalation posture also allowed the top civilian leadership to end the delegated command-and-control arrangements of its brinkmanship posture, which bred corruption and poor discipline. China's calibrated escalation cyber force posture is more in line with the strict control that the Communist Party of China exercises over the PLA's other information-age capabilities that could have strategic effects and its nuclear weapons. The initial choice of a brinkmanship cyber posture suggests that, when China's cyber vulnerability was low, its leaders might have judged offensive cyber capabilities to be less sensitive than its other information-age weapons, over which they have always asserted strict control.

Beginning in 2014, the Communist Party of China reformed both the PLA's cyber force posture and the civilian cyber governance structure to better manage China's growing vulnerability to cyberattacks. China reorganized its civilian agencies for cybersecurity policy by creating a new, domestically focused, high-level coordinating body, the Central Cybersecurity and Informatization Leading Small Group, which met for the first time in February 2014. The

163. Ibid, p. 87.
164. Ibid., p. 86.
165. Posen, *The Sources of Military Doctrine*.

PLA participated in that group, but also established its own All-Military Cybersecurity and Informatization Leading Small Group.[166] These two groups were established in close succession after the 18th Party Congress in November 2012 to provide centralized and unified leadership at the national and military strategic level to strengthen China's cyber and information system.[167]

Around 2013, China's top leaders also initiated a program of military-wide structural and doctrinal reform, which created an opportunity for the PLA to reorganize its cyber units and update its cyber doctrine. In a speech to the CMC in December 2013, Xi instructed the PLA to carry out "corrections to content in combat regulations and training outlines that do not fulfill the requirements of actual war,"[168] which accurately described its brinkmanship cyber posture. Xi called for innovation in military strategy in the cyber domain specifically, which he identified as one of the "new commanding heights of military competition."[169] In March 2014, a CMC Leading Small Group for Deepening Defense and Military Reform met for the first time to formulate a plan to reform the PLA.[170]

The statements of top leaders in late 2014 provide evidence that China was changing its brinkmanship cyber force posture, which had become dangerous given China's cyber vulnerability and problematic military discipline. The CMC issued an "Opinion on Strengthening Military Information Security Work" on October 7, 2014, which ordered a change in posture and articulated guiding principles for the PLA's future cyber force posture. The steps to implement the 2014 opinion included establishing a more comprehensive cyber defense and information protection system, developing PLA-wide rules for

166. Liang Pengfei and Zhang Yanzhong, "Quanjun Wangluo Anquan He Xinxihua Zhuanjia Zixun Weiyuan Hui zhaokai quanti huiyi" [All-Military Cybersecurity and Informatization Expert Advisory Committee convenes plenary meeting], *Zhongguo Junwang* [China Military Online], May 20, 2015, http://www.81.cn/jwgz/2015-05/20/content_6499978.htm.
167. Qiang Guo and Yaohui Zhao, "Niuzhu wangluo xinxi tixi jianshe zhuashou, women gai zhaozuo" [What we should do as a starting point to grasp cyber and information system building], *Jiefangjun bao* [People's Liberation Army Daily], November 20, 2018.
168. Renmin Jiefangjun Zong Zhengzhi Bu [People's Liberation Army General Political Department], *Xi Jinping guofang he jundui jianshe zhongyao lunshu xuanbian* [Selection of Xi Jinping's important expositions on national defense and army building] (Beijing: Jiefangjun chubanshe, 2014), p. 218.
169. Renmin Jiefangjun Zong Zhengzhi Bu, *Xi Zhuxi guofang he jundui jianshe zhongyao lunshu duben* [A Reader on Chairman Xi's important expositions on national defense and army building] (Beijing: Jiefangjun chubanshe, 2014), p. 56.
170. Zhonggong Zhongyang Wenxian Yanjiu Shi, *Xi Jinping guofang he jundui jianshe zhongyao lunshu xuanbian (san)* [A selection of Xi Jinping's important expositions on national defense and army building (3)] (Beijing: Zhongyang wenxian chubanshe, 2016), p. 49.

information security, adopting domestically produced information security systems and products, increasing information defense capabilities, and punishing illegal PLA activity online.[171] At an All-Military Political Work Conference (the New Gutian Conference) on November 4, 2014, Xi's remarks indicated that the force posture change would improve the PLA's ability to win local wars with a strong "informatized" force.[172] Xi criticized the PLA's existing posture for its lack of theoretical guidance, negative effects, and inappropriateness to the current state of the Internet.[173]

The content of both Xi's remarks at the New Gutian Conference and the CMC 2014 opinion mirrored the PLA's concerns about China's brinkmanship posture. A commentary published together with a summary of the CMC 2014 opinion in the *PLA Daily* on October 11, 2014, indicated that the PLA's existing cyber force posture was harming the national interest. China was facing enormous pressure in cyberspace because of the "increasingly intense competition over the rights to development, leadership and control of cyberspace" among countries worldwide.[174] PLA cyber force posture needed to be coordinated with civilian cybersecurity policy to meet this threat.[175] Xi's remarks at the New Gutian Conference indicated that cyber conflict had become "the principal direction of attack" and one of the main arenas of military competition for the PLA.[176] He reportedly observed that, "currently some work is not at all suitable for the requirements of the cyber era, and it is already increasingly clear that ideas and concepts, and work methods are lacking in this age [*shidai cha*]."[177]

China's leaders also changed PLA cyber posture to eliminate military corruption and poor discipline that delegated cyber command-and-control arrangements had enabled. One of the new guiding principles outlined in the

171. "Jing Xi Jinping zhuxi pizhun Zhongyang Junwei yinfa 'guanyu jin yibu jiaqiang jundui xinxi anquan gongzuo yijian'" [Following Xi Jinping's approval, the CMC publishes an "opinion on accelerating the strengthening of military information security work"], *Renmin Wang* [People.cn], October 7, 2014, http://military.people.com.cn/n/2014/1007/c1011-25783981.html. CMC opinions are highly authoritative and may follow special work conferences dedicated to the topic.
172. "Jundui 'Hulian Wang Jia' shidai zhi quewen" [The military examines shortcomings in the "Internet Plus" era], *Jiefangjun bao* [People's Liberation Army Daily], January 15, 2015.
173. Cheng Jian, "Luoshi Gutian Zhenggong Hui jingshen de renshi yu sikao" [Understanding and reflecting on implementing the spirit of the Gutian Political Work Conference], *Zhongguo junshi kexue* [China Military Science], No. 6 (2015), pp. 104–110.
174. "Jing Xi Jinping zhuxi pizhun Zhongyang Junwei yinfa 'guanyu jin yibu jiaqiang jundui xinxi anquan gongzuo yijian,'" October 7, 2014.
175. Ibid.
176. Cheng, "Luoshi Gutian Zhenggong Hui jingshen de renshi yu sikao," p. 109.
177. Ibid.

2014 CMC opinion was to "sternly combat illegal, criminal acts on the Internet involving the military."[178] Cyber force posture most likely featured on the agenda of the New Gutian Conference, which focused on Party control over the PLA rather than military operations or strategy, because the online environment could undermine PLA loyalty to the Party.[179] Available sources about the New Gutian Conference and CMC opinion describe the strict command-and-control arrangements of China's new cyber force posture, but not its other elements that emerged after 2014.

ALTERNATIVE EXPLANATIONS

The theory of strategic substitution explains more of the variation in China's decision-making about offensive cyber capabilities than alternative explanations derived from the military innovation and diffusion literature. Those explanations include emulation of states that were the first to adopt cyber military capabilities and the influence of assertive or delegative civil-military relations on posture choices.[180] It also outperforms explanations of the 2014 posture change that emphasize the role of U.S. pressure on China's leaders to prevent the PLA from conducting cyber-enabled industrial espionage.

There is little evidence that China was emulating the United States, which was both China's adversary and a first-mover state that pursued an offensive cyber operations capability in the early 1990s. Nor is there evidence that China emulated Russia, the first state that the PLA credited with using cyberattacks for strategic effects in the 2008 Russia-Georgia conflict.[181] I argue that emulation does not adequately explain China's pursuit of offensive cyber capabilities for coercive leverage because these U.S. and Russian demonstrations of cyber capabilities occurred too long before or after China's decision to pursue coercive cyber capabilities around 2000. Moreover, neither Russia nor the United States gave strategic cyberattacks such a prominent role in their approaches to gaining coercive leverage. The PLA's reasons for recommending a coercive cyberattack capability to address China's leverage deficit also emphasized the need to offset rather than emulate the U.S. military. An emulation explanation

178. "Jing Xi Jinping zhuxi pizhun Zhongyang Junwei yinfa 'guanyu jin yibu jiaqiang jundui xinxi anquan gongzuo yijian,'" October 7, 2014.
179. Renmin Jiefangjun Zong Zhengzhi Bu, *Xi Jinping guofang he jundui jianshe zhongyao lunshu xuanbian (er) [A Selection of Xi Jinping's important expositions on national defense and army building (2)]* (Beijing: Jiefangjun chubanshe, 2015), p. 124.
180. Resende-Santos, *Neorealism, States, and the Modern Mass Army*; and Feaver, *Guarding the Guardians*.
181. Xiao, *Zhanlue xue* (2015), p. 145; and Ye, *Xinxi zuozhan xue jiaocheng*, p. 55.

might expect China to pursue a force posture similar to the United States, which revealed little about its offensive cyber capabilities until it established a Cyber Command in 2009. Although the PLA examined the force postures of other countries around 2012, it did not recommend that China adopt a similar command structure to the U.S. Cyber Command or the force posture of any other country.[182]

The theory of strategic substitution also helps to explain some of the questions that China's cyber choices raise for theories of military innovation and diffusion. A civil-military relations explanation would attribute China's choice of a calibrated escalation posture to civilian leaders' preferences for a posture that asserted their control over PLA cyber activity. But this explanation cannot account for China's brinkmanship posture. Leaders' sensitivity to China's high cyber vulnerability might explain the temporal variation in its force posture, despite continuity in the Communist Party's assertive control over the PLA. China's posture also changed more abruptly in 2014 than either an adaptation or capacity-based explanation would expect.[183] For example, though the 2013 *Science of Military Strategy* claimed that uncertainty about cyber escalation deterred the outbreak of cyberwar, only two years later the 2015 *Science of Military Strategy* claimed that stricter cyber command and control could prevent escalation.

Some experts have argued that the United States successfully pressured China's leaders to reign in the PLA's online behavior in 2014.[184] Before October 2014, cyber espionage units from the PLA's Third Department were conducting operations against a variety of Western enterprises and giving their commercial secrets to Chinese companies.[185] Western sources claimed that an agreement between Xi Jinping and President Barack Obama in September 2015 to refrain from state-sponsored industrial cyber espionage changed the behavior of PLA cyber units.[186] My empirical analysis puts this shift in PLA cyber ac-

182. Wang, *Wangluo kongjian anquan zhanlue yanjiu*, p. 28. U.S. Strategic Command served as an inspiration but not a model for the PLA's Strategic Support Force (SSF). Costello and McReynolds, *China's Strategic Support Force*, pp. 9, 49–50.
183. Horowitz, *The Diffusion of Military Power*; and Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies*, Vol. 29, No. 5 (2006), pp. 925–930, https://doi.org/10.1080/01402390600901067.
184. Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, Calif.: RAND, 2016).
185. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Reston, Va.: Mandiant Intelligence Center, February 18, 2013), https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.
186. Dustin Volz, "Chinese Economic Cyber-Espionage Is Diminishing, Says U.S. Official," Reuters, June 28, 2016, http://www.reuters.com/article/us-cyber-china-idUSKCN0ZE1S8.

tivity in a broader context. The activity of PLA units that conducted persistent espionage operations dropped dramatically in mid-October 2014 and mid-July 2015.[187] These decreases in activity are correlated with the CMC opinion in October 2014 and the Politburo's approval of the PLA reform plan in July 2015, respectively. The resurgence of Chinese cyber espionage activities since 2015 by units affiliated with the Ministry of State Security suggests that China reassigned some espionage tasks to non-PLA units,[188] which would be consistent with its calibrated escalation posture.

Conclusion

China's approach to gaining coercive leverage in limited wars with nuclear-armed adversaries differs from the choices of other nuclear-armed states. This article has explained China's puzzling reliance on information-age weapons to address the limited war dilemma. When its threat environment changed and China confronted a leverage deficit, its search for coercive leverage was constrained by doubts that nuclear threats would be credible and an inability to quickly build up war-winning conventional forces. Instead, China searched for substitutes and found information-age weapons, which it postured as slippery slopes or ladders between conventional and nuclear war. In the case of China's offensive cyber capabilities, its leaders embraced the strategic substitution of strategic cyber operations for nuclear and conventional options when they faced a leverage deficit. China's leaders postured their cyber capabilities to gain coercive leverage and later altered their force posture to account for an increase in China's cyber vulnerability.

The theory of strategic substitution explains why China pursued offensive cyber operations to gain coercive leverage and how it configures them to threaten escalation. Information-age weapons, including strategic cyberattack capabilities, promised to revive the threat that leaves something to chance of all-out nuclear conflict that would have otherwise diminished as the nuclear stalemate between the United States and China deepened. China pursued these new capabilities and developed a force posture to use them to strike a

187. "Red Line Drawn: China Recalculates Its Use of Cyber Espionage" (Milpitas, Calif.: Fireye, June 2016), p. 11.
188. Maria Korolov, "APT3 Hackers Linked to Chinese Intelligence," May 24, 2017, CSO Online, https://www.csoonline.com/article/3198105/apt3-hackers-linked-to-chinese-intelligence.html; and Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," Fireeye Cyber Defense Summit 2019, sess. 8, October 10, 2019, 3:30–4:20 p.m., https://summit.fireeye.com/learn/tracks.html.

delicate balance between threatening sufficient damage and running the risk of nuclear war.

The theory of strategic substitution makes two key theoretical claims about China's choices. First, China's search for coercive leverage in the post–Cold War era was a search for substitutes. Like other states, China experienced leverage deficits when changes to its threat environment revealed that its existing capabilities were inadequate for the war or adversary it was most likely to face. But China's search for leverage to address that deficit differed from those of other states because it was constrained by conventional military inferiority and doubts about nuclear first use. Those constraints shaped China's decisions to pursue information-age weapons. Second, the theory explains how information-age weapons can provide the most credible strategic leverage—when they are explicitly postured for coercion using a brinkmanship or calibrated escalation posture.

The explanatory power of these theoretical claims is demonstrated by the case of China's coercive cyber capabilities. China pursued coercive cyber capabilities around 2000 because, after NATO bombed China's embassy in Belgrade in 1999, it recognized that it would face a leverage deficit if there were a war with the United States over Taiwanese independence. Threatening cyberattacks against the United States would be more credible in that limited war than threatening to use nuclear weapons, and quicker than building up China's conventional military capabilities. Initially, the PLA adopted a brinkmanship posture, which was credible because of China's low vulnerability to cyberattacks. But as China became more vulnerable to cyberattacks in the decade that followed, its cyber force posture needed to change to remain credible. In 2012 civilian leaders ordered the PLA to address the mismatch between its brinkmanship posture and the country's growing vulnerability to cyberattacks. The theory of strategic substitution will require further testing on China's decision-making about its other information-age weapons to confirm its explanatory power, beyond this plausibility probe of the cyber case.

The theory has limited cross-national applications because no other nuclear-armed state has faced constraints as severe as China when confronted with a leverage deficit. Nevertheless, the theory offers three generalizable insights into the behavior of other nuclear-armed states. First, another state could face similar constraints to China if it wanted to pursue war aims that did not require the total defeat of a nuclear-armed adversary but lacked both the conventional capabilities and the confidence that its nuclear threats would be taken seriously. India might face those constraints in its long-standing border

dispute with China, given its nuclear no-first-use policy and conventional inferiority. Second, it suggests that all nuclear-armed states benefit from having information-age weapons to escalate a conflict when they want to coerce an adversary but do not want to threaten nuclear use, even if they acquired those capabilities for other reasons. Third, other nuclear-armed states might share China's sensitivity to cyber vulnerability in their cyber force posture choices. France's calibrated escalation-style cyber force posture and North Korea's brinkmanship-style posture conform with the theory's expectations about the implications of vulnerability to cyberattacks.

The findings of this article have three important implications for scholars and policymakers. First, it remains unclear whether China's gamble on information-age weapons for coercive leverage will endure in an era of intense U.S.-China rivalry. Indeed, it was not clear that offensive cyber capabilities would actually deliver the leverage that China's leaders pursued in 2001. Two decades later, significant uncertainty remains as to whether China's offensive cyber capabilities would provide it with coercive leverage in a rapidly escalating crisis or war, fail to cause enough damage to coerce an adversary, or catalyze a nuclear war despite its calibrated escalation posture. China's leaders continue to view cyberattacks as valuable for coercive leverage, regardless of this uncertainty. But the constraints that defined their earlier searches for leverage are loosening. The PLA is closing the conventional military gap with the United States. Meanwhile, the growth in China's nuclear arsenal size and sophistication since 2019 hints that current leaders might be open to embracing nuclear options whose credibility past leaders had doubted.

Second, the theory of strategic substitution helps to interpret the current qualitative and quantitative improvements in China's nuclear forces. China's incentives to adopt a first-use nuclear posture are weaker than they were at any point in the post–Cold War era, given its growing conventional military power and maturing capability to threaten information-age attacks for coercive leverage. In addition, China's approach to coercion in limited wars for the past three decades has aimed to exploit the reluctance of its adversaries to cross the nuclear threshold rather than to threaten to cross that threshold itself. If China's approach to gaining coercive leverage continues along these lines, its nuclear modernization is unlikely to reflect the pursuit of a nuclear first-use posture. But if China's leaders have concluded that information-age weapons cannot substitute for threats of nuclear first use after all, or that U.S. resolve to use nuclear weapons first in a war with China is stronger than they had assumed, China's nuclear modernization might suggest that it is no longer will-

ing to gamble on information-age weapons. Rather, China is turning to a more certain option for gaining coercive leverage: threatening nuclear first use.

Third, China's emphasis on information-age weapons in its approach to gaining coercive leverage suggests that U.S.-China efforts to reduce nuclear risks will encounter novel challenges. China is unlikely to embrace crisis stability measures that limit the coercive leverage it gains from threats to use space, cyber, and precision missile capabilities until it deploys war-winning conventional capabilities (or it adopts a first-use nuclear posture). Further, any future nuclear arms control agreements will need to also include nonnuclear capabilities. Those capabilities will increase the number of veto players and verification challenges in any negotiations. More optimistically, China's decision to substitute information-age weapons threats for nuclear threats increases the degree of mutual vulnerability in the U.S.-China relationship beyond what the nuclear balance might suggest. This overall strategic stalemate gives both countries a stronger shared interest in restraint during a crisis because of the uncertain dangers that information-age attacks portend.