# Escalation through Entanglement

## How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War

*James M. Acton*

The 2018 U.S. Nuclear Posture Review contains a highly consequential threat that has been largely overlooked in the wave of commentary surrounding the document's release: the United States warns potential adversaries that it would consider using nuclear weapons in the event of "significant nonnuclear strategic attacks . . . on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[1] This threat was motivated by the growing vulnerability of these assets—in particular, the United States' nuclear command, control, communication, and intelligence (C3I or enabling) capabilities—to advanced nonnuclear weapons, and is presumably intended to deter attacks on them.[2] In issuing this threat, the Nuclear Posture Review illustrates that nonnuclear attacks on nuclear forces and C3I capabilities could be highly escalatory, even to the point of directly sparking a nuclear war.

A key challenge in managing these escalation risks is that attacks on an opponent's nuclear forces or their C3I capabilities (whether they belong to the United States or another state) might not be deliberate. Since the late 2000s, scholars have warned about the possibility of escalation in a U.S.-China conflict resulting from so-called crisis instability generated by actual or threatened U.S. nonnuclear operations that were intended to suppress China's conventional forces but inadvertently degraded its nuclear forces or associated C3I assets located in the theater of operations, thus leading Beijing to fear it was

*James M. Acton is co-director of the Nuclear Policy Program and holds the Jessica T. Matthews Chair at the Carnegie Endowment for International Peace.*

For insightful comments on previous drafts of this article, the author thanks Alexey Arbatov, Toby Dalton, Catherine Dill, Geoffrey Forden, Michael Gerson, Charles Glaser, Ariel Levite, Jeffrey Lewis, Li Bin, Austin Long, Tim Maurer, James Miller, George Perkovich, Pavel Podvig, Joshua Pollack, Brad Roberts, Scott Sagan, Petr Topychkanov, Tong Zhao, and the anonymous reviewers, as well as interviewees and participants at seminars where he presented this research. He is also grateful to Jessica Margolis, William Ossoff, Thu-An Pham, Kathryn Taylor, Elizabeth Whitfield, and Lauryn Williams for research assistance. This work received generous financial support from the Carnegie Corporation of New York. The contents of this article are exclusively the author's responsibility.

1. U.S. Department of Defense, "Nuclear Posture Review" (Washington, D.C.: U.S. Department of Defense, February 21, 2018), p. 21, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.
2. Ibid., p. 56.

*International Security*, Vol. 43, No. 1 (Summer 2018), pp. 56–99, doi:10.1162/ISEC_a_00320
© 2018 by the President and Fellows of Harvard College and the Massachusetts Institute of Technology. Published under a Creative Commons Attribution 4.0 Unported (CC BY 4.0) license.



Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

being disarmed.[3] Similar, if more infrequent, scholarly warnings have been voiced about a U.S.-Russia conflict.[4] Such escalation would be inadvertent because it was the result of military operations or threats that were not intended to be escalatory.[5]

This article's thesis is that the risks of inadvertent escalation are even more serious than these warnings suggest and are likely to increase significantly in the future. Driving these risks is the possibility that Chinese, Russian, or U.S. C3I assets located outside—potentially far outside—theaters of operation could be attacked over the course of a conventional conflict. These assets include satellites used for early warning, communication, and intelligence, surveillance, and reconnaissance (ISR); ground-based radars and transmitters; and communication aircraft.[6] Such assets constitute key nodes in states' nu-

3. Michael S. Chase, Andrew S. Erickson, and Christopher Yeaw, "Chinese Theater and Strategic Missile Force Modernization and Its Implications for the United States," *Journal of Strategic Studies*, Vol. 32, No. 1 (February 2009), pp. 101–106, doi:10.1080/01402390802407434; Jeffrey G. Lewis, "Chinese Nuclear Posture and Force Modernization," *Nonproliferation Review*, Vol. 16, No. 2 (July 2009), pp. 205–206, doi:10.1080/10736700902969661; Joshua Pollack, "Emerging Strategic Dilemmas in U.S.-Chinese Relations," *Bulletin of the Atomic Scientists*, Vol. 65, No. 4 (July/August 2009), pp. 53–63, doi:10.2968/065004006; Thomas J. Christensen, "The Meaning of the Nuclear Evolution: China's Strategic Modernization and U.S.-China Security Relations," *Journal of Strategic Studies*, Vol. 35, No. 4 (August 2012), pp. 467–471, doi:10.1080/01402390.2012.714710; Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Posture and U.S.-China Strategic Stability," *International Security*, Vol. 40, No. 2 (Fall 2015), pp. 40–45, doi:10.1162/ISEC_a_00215; Joshua H. Pollack, "Boost-Glide Weapons and U.S.-China Strategic Stability," *Nonproliferation Review*, Vol. 22, No. 2 (2015), pp. 157–161, doi:10.1080/10736700.2015.1119422; Wu Riqiang, "Sino-U.S. Inadvertent Escalation" (Atlanta: Program on Strategic Stability Evaluation, Georgia Institute of Technology, n.d.), https://www.yumpu.com/en/document/view/38495325/wu-sino-us-inadvertent-escalation-program-on-strategic-stability-; 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, doi:10.1162/ISEC_a_00274; and Tong Zhao and Li Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective," in James M. Acton, ed., "Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks" (Washington, D.C.: Carnegie Endowment for International Peace, 2017), pp. 47–75, http://carnegieendowment.org/files/Entanglement_interior_FNL.pdf. A much larger literature, with many contributions from foreign authors, analyzes nonnuclear threats to nuclear forces but does not connect them to inadvertent escalation.

4. James M. Acton, "Silver Bullet? Asking the Right Questions about Conventional Prompt Global Strike" (Washington, D.C.: Carnegie Endowment for International Peace, 2013), pp. 120–126, http://carnegieendowment.org/files/cpgs.pdf; and Alexey Arbatov, Vladimir Dvorkin, and Petr Topychkanov, "Entanglement as a New Security Threat: A Russian Perspective," in Acton, *Entanglement*, pp. 9–45.

5. Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, Calif.: RAND Corporation, 2008), pp. 23–25, http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf. This concept was first developed at length in Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, N.Y.: Cornell University Press, 1991), pp. 12–16.

6. Although threats to some of these assets have been discussed, their potential to spark inadvertent escalation has not.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

clear C3I systems, but they are also "entangled" with nonnuclear weapons in two ways.[7] First, they are typically dual use; that is, they enable both nuclear and nonnuclear operations. Second, they are increasingly vulnerable to nonnuclear attack—much more vulnerable, in fact, than most nuclear-weapon delivery systems.

Entanglement could lead to escalation because both sides in a U.S.-Chinese or U.S.-Russian conflict could have strong incentives to attack the adversary's dual-use C3I capabilities to undermine its nonnuclear operations.[8] As a result, over the course of a conventional war, the nuclear C3I systems of one or both of the belligerents could become severely degraded. It is, therefore, not just U.S. nonnuclear strikes against China or Russia that could prove escalatory; Chinese or Russian strikes against American C3I assets could also—a possibility that scholars have scarcely even considered since the end of the Cold War.[9]

Two escalation mechanisms that have not been previously discussed in the academic literature are largely responsible for the increasing risk. First, the target might interpret nonnuclear attacks against its dual-use C3I assets that were motivated by conventional warfighting goals as preparations for nuclear use. It might respond to such "misinterpreted warning," to coin a term, by trying to deter the nuclear strike it believed might be coming or to mitigate its potentially calamitous consequences. Such efforts, which might include provocative nonnuclear operations to protect remaining C3I assets (such as strikes against anti-satellite weapons deep within the adversary's territory) accompanied, perhaps, by nuclear threats, could prove highly escalatory. These escalation pressures could arise even if the recipient of misinterpreted warning were not concerned about the survivability of its nuclear forces—a key distinction from crisis instability.

---

7. To the best of the author's knowledge, the first use of the term "entangled" in this general sense occurs in John D. Steinbruner, *Principles of Global Security* (Washington, D.C.: Brookings Institution Press, 2000), p. 55.

8. 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. 67–68, doi:10.1162/ISEC_a_00114; and Stephen Biddle and Ivan Oelrich, "Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia," *International Security*, Vol. 41, No. 1 (Summer 2016), pp. 44–45, doi:10.1162/ISEC_a_00249.

9. There are passing references to this possibility in Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," p. 31; Zhao and Li, "The Underappreciated Risks of Entanglement," p. 51; and James N. Miller Jr. and Richard Fontaine, "A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict" (Cambridge, Mass. and Washington, D.C.: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, and Center for a New American Security, September 2017), p. 19, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-ProjectPathways-Finalb.pdf?mtime=20170918101504.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Second, a state with a damage-limitation doctrine would rely on sophisticated C3I capabilities to locate and destroy its opponent's nuclear forces and conduct missile defense operations. If these dual-use enabling capabilities were subject to attack in a conventional conflict—or even if their possessor feared they might be—the state could worry that its window of opportunity for conducting effective damage-limitation operations might have closed by the time the war turned nuclear. In this case, the state might take escalatory measures to protect its C3I system or even initiate counterforce operations preemptively. This escalation mechanism, which might be termed the "damage-limitation window," is distinct from crisis instability because it is driven by the state's desire to hold an opponent's nuclear forces at risk, not to protect its own. It is distinct from misinterpreted warning because it could operate even if the state did not believe that nuclear use by an adversary might be imminent; the state would only have to believe that such escalation was possible later on.

An additional implication of C3I entanglement is that the risks of crisis instability are more serious than portrayed in the academic literature. Scholarly warnings about crisis instability have focused on the potential for U.S. nonnuclear operations to degrade Chinese nuclear forces, but have also identified the risk of inadvertent threats to China's nuclear C3I capabilities located in the theater of operations.[10] These threats have received particular attention since the United States acknowledged, in 2013, that it seeks to defeat potential adversaries' antiaccess/area-denial capabilities by holding relevant C3I assets at risk as part of the concept formerly known as AirSea Battle (which was renamed, in 2015, as the Joint Concept for Access and Maneuver in the Global Commons and has since been further developed).[11] If overlap exists between the communication systems for China's land-based nuclear and nonnuclear missiles, as some analysts have suggested, China could mistake U.S. strikes designed to disable its nonnuclear missiles as an attack against its nuclear forces.[12]

---

10. Talmadge, "Would China Go Nuclear?" pp. 78–79, 83.
11. Air-Sea Battle Office, "Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges" (Washington, D.C.: U.S. Department of Defense, May 2013), p. 7, http://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf.
12. Christensen, "The Meaning of the Nuclear Evolution," p. 468. For a slightly dated description of Chinese command and control that implies an overlap, see John Wilson Lewis and Xue Litai, *Imagined Enemies: China Prepares for Uncertain War* (Stanford, Calif.: Stanford University Press, 2006), pp. 197–201. For opposing views, see Cunningham and Fravel, "Assuring Assured Retaliation," pp. 42–45; and Michael Glosny, Christopher Twomey, and Ryan Jacobs, "U.S.-China Strategic Dialogue, Phase VIII Report" (Monterey, Calif.: Center on Contemporary Conflict, Naval

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Entanglement, however, has created other potential triggers for crisis instability. The United States, for example, has—or could develop—incentives to launch nonnuclear kinetic attacks against existing and probable future dual-use Chinese or Russian early-warning capabilities, including over-the-horizon radars, ballistic missile early-warning radars (BMEWRs), and early-warning satellites, that are located outside the theater of operations.[13] (Kinetic weapons, which often use explosive warheads, aim to damage or destroy targets by transferring kinetic energy to them through physical contact; nonkinetic weapons include directed energy and cyber capabilities.) Moreover, Russian strikes on the United States could precipitate crisis instability if U.S. communication aircraft (currently, the United States' most survivable means to communicate with its nuclear forces) become vulnerable.

Entanglement could catalyze escalation in any major U.S.-Chinese or U.S.-Russian conventional conflict, irrespective of its origins. That said, for the sake of concreteness, the kind of U.S.-Chinese conflict that forms the backdrop to this article would most likely begin with a Chinese attempt to reunify with Taiwan by force (either unprovoked or because the government of Taiwan had declared independence), followed by U.S. intervention on behalf of Taiwan. The most probable cause of a major U.S.-Russian conflict would be the invasion and occupation of one or more of the Baltic states by Russia, followed by a U.S.-led counterattack to liberate them. In both cases, fighting could spread from the theater in which it started.

There would, of course, be important differences between the escalation dynamics in a U.S.-Chinese and U.S.-Russian conflict. Nevertheless, there would also be important similarities that help illustrate the general nature of the risks stemming from entanglement. In particular, entanglement could not only precipitate the use of nuclear weapons directly, but could also frustrate efforts to manage nonnuclear escalation, thus raising the risk of nuclear use later on. Early in a conflict, for example, to emphasize its limited war aims, the United States might refrain from conducting nonnuclear strikes beyond a certain distance into an adversary's territory. Subsequently, if the United States became worried that key C3I satellites were at risk, it might believe that it had to

Postgraduate School, November 2014), p. 10, http://calhoun.nps.edu/bitstream/handle/10945/44733/2014%20008%20-%20US-China%20Phase%20VIII%20Report.pdf.

13. There are passing references to this possibility in Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat." Over-the-horizon radars are briefly mentioned in Christopher P. Twomey, "Asia's Complex Strategic Environment: Nuclear Multipolarity and Other Dangers," *Asia Policy*, January 2011, p. 64.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

attack Chinese or Russian anti-satellite (ASAT) weapons located further beyond the border.

This article begins by outlining the technological and doctrinal developments that are increasing entanglement. It then lays out three mechanisms—misinterpreted warning, the damage-limitation window, and crisis instability—by which entanglement might spark escalation and identifies the conditions under which escalation would be most likely. To provide a concrete demonstration of the severity of the escalation risks, the article then describes the likely effectiveness and effects of nonnuclear kinetic attacks against the U.S. early-warning system. It also considers the risks of cyber interference with dual-use Chinese, Russian, and U.S. early-warning assets, and in particular, the danger of the target's misinterpreting cyber espionage as an attempt to disable or destroy those assets.

With risk reduction likely to prove difficult, unilateral restraint and actions represent the most feasible policy responses for the short term. Although such steps would likely be only moderately effective in themselves, they could help pave the way for cooperative efforts in the future. Although difficult to orchestrate, cooperative risk-reduction would be desirable because, as this article emphasizes in the conclusion, the risks created by entanglement are likely to grow in the future, absent action to mitigate them.

## *The Technological and Doctrinal Drivers of Entanglement*

Entanglement describes interactions between the nuclear and nonnuclear domains. For current purposes, its most important manifestations are the dual-use nature of many C3I assets as well as nonnuclear threats (real or perceived) to nuclear forces or their C3I infrastructure. Other manifestations, mentioned only in passing here, are dual-use delivery systems; nuclear delivery systems that are superficially similar to nonnuclear ones; and the colocation of nuclear and nonnuclear delivery systems or C3I assets. Since the end of the Cold War, entanglement has increased significantly—and, indeed, is still increasing—as the result of four trends in military technology and doctrine.

### GROWING TECHNOLOGICAL THREATS

First, profound changes in weaponry have significantly magnified nonnuclear threats to states' C3I assets and, to a lesser extent, their nuclear forces. These changes include the deployment of two entirely new classes of weapons: cyberweapons (which could threaten both C3I capabilities and nuclear forces) and nonnuclear strategic ballistic missile defense systems (which could inter-

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

cept nuclear weapons after launch). The effectiveness of existing types of nonnuclear weapons has also improved dramatically. For example, although both the United States and the Soviet Union had some capability to target satellites without nuclear weapons by the end of the Cold War, nonnuclear ASAT weapons—both kinetic and non-kinetic—pose a much more potent threat today.[14] High-precision conventional weapons have also improved significantly, including with the introduction of satellite-guided munitions. Over the next couple of decades, further substantial improvements can be expected in all of these weapon types, and entirely new types of nonnuclear weapons, including long-range hypersonic weapons, may be deployed.[15]

### growing vulnerability of C3I capabilities

Second, changes in enabling technologies have exacerbated the growing vulnerability of the C3I assets involved in nuclear operations (whether these assets are dual use or not). Digital networks have become ubiquitous, for example, creating the possibility of cyber interference. Moreover, the United States, at least in an effort to reduce costs, has pursued greater commonality in the enabling systems, such as the receivers for satellite signals, associated with different nuclear-weapon delivery systems.[16] This development, however, could magnify cyber risks. If, for example, there was a design flaw in a common receiver that left it vulnerable to being disabled by a cyberattack, then all the nuclear-weapon delivery systems that used the receiver could be simultaneously compromised.

Another cause of this growing vulnerability—at least for the U.S. nuclear C3I system—is a reduction in redundancy (there is insufficient publicly available information to assess how the redundancy of the Chinese and Russian systems has changed).[17] In the late 1980s and early 1990s, for example, two largely independent satellite-based communication systems were in use for transmitting orders for the employment of U.S. nuclear weapons.[18] The

14. Laura Grego, "A History of Anti-Satellite Programs" (Cambridge, Mass.: Union of Concerned Scientists, January 2012), http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.
15. Acton, "Silver Bullet?"
16. Department of the Air Force, U.S. Department of Defense, "Department of Defense Fiscal Year (FY) 2017 President's Budget Submission: Other Procurement, Air Force" (Washington, D.C.: U.S. Department of Defense, February 2016), p. 267, line item 834210, http://www.saffm.hq.af.mil/Portals/84/documents/FY17/AFD-160208-049.pdf?ver=2016-08-24-102038-590.
17. For an overview of the late 1980s system, see Peter Vincent Pry, *The Strategic Nuclear Balance*, Vol. 2: *Nuclear Wars: Exchanges and Outcomes* (New York: Crane Russak, 1990), pp. 18–22.
18. Curtis Peebles, *High Frontier: The U.S. Air Force and the Military Space Program* (Washington, D.C.: Air Force History and Museums Program, 1997), pp. 44–54, http://www.dtic.mil/dtic/tr/

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Defense Satellite Communications System served intercontinental ballistic missiles (ICBMs). A separate system, the Air Force Satellite Communications System (AFSATCOM), served ICBMs, sea-launched ballistic missiles (SLBMs), and nuclear-armed aircraft, and consisted of special transponders hosted on tens of satellites mostly used for other purposes.[19] Today, the United States is in the process of deploying just four Advanced Extremely High Frequency (AEHF) satellites that will be the nation's sole space-based system for transmitting nuclear employment orders once legacy Milstar satellites have been retired. Similarly, at the end of the Cold War, the United States operated two independent networks of radio antennae to communicate with submarines.[20] One of these networks, which could provide global coverage using two extremely low-frequency antennae in the continental United States, has since been shut down.[21] Although modernization of the remaining assets would presumably enable them to function more effectively in the extraordinarily stressful conditions of a nuclear war, the overall loss of redundancy—a consequence of budgetary pressures—appears to have left the U.S. nuclear C3I system less resilient against nonnuclear attack.

### GROWING RELIANCE ON DUAL-USE C3I ASSETS

Third, the U.S. nuclear C3I system has always used some dual-use assets, and is becoming increasingly reliant on them, raising the likelihood of its being attacked in a nonnuclear conflict. The United States has, for example, never fielded communication satellites that were used exclusively for nuclear operations.[22] Today, Milstar and AEHF satellites represent the United States' most secure space-based means of communicating with both nuclear and "high-priority" nonnuclear users (users tasked with particularly important or time-critical missions).[23] In fact, the vast majority of data transmitted by these

---

fulltext/u2/a442844.pdf. The systems were not entirely independent, because some transponders belonging to the Air Force Satellite Communications System were hosted by Defense Satellite Communications System satellites.

19. A 1981 estimate suggested that as many as thirty AFSATCOM transponders could be deployed by 1990. See Mark Hewish, "Satellites Show Their Warlike Face," *New Scientist*, October 1, 1981, p. 39.

20. U.S. Department of the Navy, "Submarine Communications Master Plan" (Washington, D.C.: U.S. Department of the Navy, December 1995), appendix B, http://fas.org/man/dod-101/navy/docs/scmp/part07.htm.

21. Robert Imrie, "Navy to Shut Down Sub Radio Transmitters," Associated Press, September 26, 2004, http://usatoday30.usatoday.com/tech/news/2004-09-26-sub-radio-offair_x.htm.

22. Peebles, *High Frontier*, pp. 44–52.

23. Air Force Space Command, "Advanced Extremely High Frequency System" (Washington, D.C.: U.S. Air Force, March 22, 2017), http://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

satellites is almost certainly associated with nonnuclear operations. Because it could be difficult for an adversary to disrupt the operation of these satellites in non-destructive ways (jamming, for example), they could become targets of direct attack in a conventional conflict.

Starting in the last decade of the Cold War, the United States has increased reliance on dual-use systems by assigning nonnuclear roles to C3I assets that used to be employed solely for nuclear operations. Until the mid-1980s, for example, U.S. early-warning satellites were used exclusively for detecting the launch of nuclear-armed missiles.[24] Today, they enable a variety of nonnuclear missions by, for example, providing cuing information for missile defenses involved in intercepting conventional ballistic missiles.[25]

In a parallel series of developments, the United States has dismantled various land-based nuclear-only communication capabilities. For example, the Emergency Rocket Communications System, which could transmit employment orders from modified ICBMs launched to overfly missile fields in the United States, was taken offline in the 1990s.[26] A decade or so later, the Survivable Low Frequency Communications System, which allowed ICBMs to receive launch orders from radio antennae, was also scrapped.[27]

The net effect of these developments is that, today, most assets in the U.S. nuclear C3I system "support both nuclear and conventional missions," according to the U.S. Government Accountability Office.[28] In fact, every C3I asset listed in the 2018 Nuclear Posture Review is known to be dual use, except for nuclear-weapon control capabilities directly associated with delivery systems (and perhaps also the United States' system for detecting nuclear

24. Their adoption for nonnuclear missions is discussed in Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare* (Annapolis: Naval Institute Press, 2000), pp. 242–245.
25. Committee on an Assessment of Concepts and Systems for U.S. Boost-Phase Missile Defense in Comparison to Other Alternatives and Division on Engineering and Physical Science of the National Research Council, *Making Sense of Ballistic Missile Defense: An Assessment of Concepts and Systems for U.S. Boost-Phase Missile Defense in Comparison to Other Alternatives* (Washington, D.C.: National Academies Press, 2012), p. 116, https://www.nap.edu/catalog/13189/making-sense-of-ballistic-missile-defense-an-assessment-of-concepts.
26. Federation of American Scientists, "Emergency Rocket Communications System (ERCS)" (Washington, D.C.: Federation of American Scientists, April 27, 1998), http://fas.org/nuke/guide/usa/c3i/ercs.htm.
27. Carla Williams, "Minot Completes Minuteman Emergency Communications Upgrade" (Washington, D.C.: U.S. Air Force, November 17, 2005), http://www.af.mil/News/ArticleDisplay/tabid/223/Article/132716/minot-completes-minuteman-emergency-communications-upgrade.aspx.
28. Christina Chaplain, "Nuclear Command, Control, and Communications: Update on DOD's Modernization," GAO-15-584R (Washington, D.C.: U.S. Government Accountability Office, June 15, 2015), p. 1, http://www.gao.gov/assets/680/670801.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

explosions—though some of its detectors are hosted by Global Positioning System satellites).[29]

The Russian nuclear C3I system probably also includes some dual-use assets. In a 2007 edition of the journal *Military Thought*, published by the Russian ministry of defense, one retired and one serving military officer describe how satellites then under development would be used for communicating with "strategic and nonstrategic nuclear forces," as well as nonnuclear forces and even "federal and regional government agencies."[30] Their description appears to refer to communication satellites that have since been deployed as part of Russia's Unified Satellite Communication System. Separately, according to state-controlled Russian media outlets, Moscow has recently acquired a number of airborne command posts capable of communicating with both nuclear and conventional forces.[31] Moreover, as discussed below, various types of Russian radars are already dual use, and Russia's new early-warning satellites could take on nonnuclear missions in the future.

The extent of the overlap between the communication systems for China's land-based nuclear and conventional missiles has been the subject of considerable debate among analysts.[32] Beijing's recent deployment of the DF-26 ballistic missile provides some additional evidence that this overlap is significant. The warhead (or warheads) on an individual missile body can, according to an apparently authoritative Chinese source, be rapidly switched between nuclear and conventional variants.[33] This capability suggests that the physical communication infrastructure associated with these missiles can be used to transmit nuclear and nonnuclear employment orders. This evidence is not definitive, however, because it is possible that missiles are transferred between nuclear and conventional missile brigades when the warhead type is changed (though this procedure would seem to obviate the whole purpose of the "change the

29. U.S. Department of Defense, "Nuclear Posture Review," pp. 56–57.
30. V.A. Grigoryev and I.A. Khvorov, "Military Satellite Communications Systems: Current State and Development Prospects," *Military Thought*, Vol. 16, Nos. 3–4 (July 1, 2007), p. 149; see also p. 150.
31. "Russian Next-Generation 'Doomsday Plane' Finally Ready for Action," Sputnik, July 28, 2016, http://sputniknews.com/russia/20160728/1043728673/russia-doomsday-plane-ready.html.
32. Christensen, "The Meaning of the Nuclear Evolution," p. 468; Lewis and Xue, *Imagined Enemies*, pp. 197–201; Cunningham and Fravel, "Assuring Assured Retaliation," pp. 42–45; and Glosny, Twomey, and Jacobs, "U.S.-China Strategic Dialogue, Phase VIII Report," p. 10.
33. Andrew S. Erickson, "Academy of Military Science Researchers: 'Why We Had to Develop the Dongfeng-26 Ballistic Missile'—Bilingual Text, Analysis, and Related Links," andrewerickson.com, December 5, 2015, http://www.andrewerickson.com/2015/12/academy-of-military-science-researchers-why-we-had-to-develop-the-dongfeng-26-ballistic-missile-bilingual-text-analysis-links/.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

warhead, not the missile" capability).[34] Additionally, as discussed below, various Chinese early-warning capabilities are already, or may become, dual use.

### GROWING DOCTRINAL THREATS

Fourth, the military doctrines of China, Russia, and the United States appear to envision attacks on space- and land-based C3I assets, including dual-use ones, to further conventional warfighting goals. In the case of the United States, this tactic was explicitly articulated in the AirSea Battle concept. Meanwhile, Washington has openly expressed concern that both China and Russia seek to hold U.S. C3I satellites at risk to support potential efforts to undermine U.S. conventional operations.[35] The U.S. intelligence community has highlighted the threat from both states to U.S. early-warning satellites, in particular.[36] A consistent picture is painted by Chinese and Russian sources. For example, the *Science of Second Artillery Campaigns*, a classified but leaked textbook from 2004 believed to contain an authoritative description of China's strategic doctrine, appears to endorse attacks against U.S. early-warning radars as a way of suppressing missile defenses in a conventional conflict.[37] Moreover, Chinese experts have openly advocated for the ability to attack U.S. early-warning satellites.[38] In a similar vein, Russian experts have stated that, in a conventional conflict, Moscow would consider attacking U.S. C3I assets, including ground-based early-warning radars.[39]

---

34. Jordan Wilson, "China's Expanding Ability to Conduct Conventional Missile Strikes on Guam" (Washington, D.C.: U.S.-China Economic and Security Review Commission, May 10, 2016), p. 8, https://www.uscc.gov/sites/default/files/Research/Staff%20Report_China%27s%20Expanding%20Ability%20to%20Conduct%20Conventional%20Missile%20Strikes%20on%20Guam.pdf.

35. Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," DIA-11-1207-161 (Washington, D.C.: Defense Intelligence Agency, 2017), p. 36, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf; and Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2017," annual report to Congress (Washington, D.C.: U.S. Department of Defense, 2017), p. 35, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770.

36. Daniel R. Coates, "Worldwide Threat Assessment of the U.S. Intelligence Community," statement for the record (Washington, D.C.: Office of the Director of National Intelligence, March 6, 2018), p. 13, https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf.

37. Second Artillery Corps, People's Liberation Army, *The Science of Second Artillery Campaigns*, unclassified U.S. government translation (Beijing: PLA Press, 2004), pp. 397–398. Given that this section discusses suppressing both missile and air defenses, this reference is probably to both missile and aircraft early-warning radars.

38. Zhao and Li, "The Underappreciated Risks of Entanglement," p. 51; and Chase, Erickson, and Yeaw, "Chinese Theater and Strategic Missile Force Modernization and Its Implications for the United States," p. 83.

39. Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," p. 31.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

## Escalation Pathways: Effects of Entanglement on Conflict Dynamics

One consequence of growing entanglement is the possibility of "incidental attacks" on an opponent's nuclear forces or their enabling capabilities. In such an attack, one state strikes an adversary's dual-use assets to influence the outcome of a conventional conflict but, in the process, inadvertently degrades its nuclear capabilities.[40] Strikes against dual-use C3I capabilities—communication and early-warning assets, in particular—would probably represent the most consequential type of incidental attack. Incidental attacks could also result, however, from strikes against dual-use weapon delivery platforms, such as aircraft and missiles.

Incidental attacks have the potential to be escalatory, in no small part because it could be effectively impossible for the target to distinguish them from deliberate attacks intended to undermine its ability to conduct nuclear operations (including obtaining warning of an incoming nuclear strike). The general difficulty of assessing intent would likely be compounded by the fog of war, which would probably be thick in any major conventional conflict and further exacerbated by likely attacks against ISR capabilities. Moreover, as Barry Posen argued, a variant of the security dilemma might arise: prudence could require a state to treat attacks on its nuclear forces or their enabling capabilities as deliberate and take actions to protect them; to assume that surviving assets were not threatened would carry the risk that they might be destroyed if the enemy's intent had been misjudged.[41]

There are three distinct pathways—misinterpreted warning, the damage-limitation window, and crisis instability—through which actual or threatened incidental attacks could spark inadvertent escalation.

### MISINTERPRETED WARNING

In a conventional war between two nuclear-armed states, nonnuclear attacks against an opponent's dual-use enabling capabilities motivated by conventional warfighting goals could be indistinguishable from operations intended to prepare the battlespace for nuclear use. Such attacks, therefore, could create misinterpreted warning—especially if the state launching them was in danger of losing the war.

Although a state concerned about becoming the target of a nuclear attack might not use nuclear weapons immediately, its concern might lead it to act in ways that could catalyze further escalation, raising the likelihood of nuclear

40. This definition is somewhat different from the one in Posen, *Inadvertent Escalation*, p. 2.
41. Ibid., pp. 12–16.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

use later on. The state would be motivated by a desire to avoid or mitigate the potentially catastrophic costs of becoming the target of even a limited nuclear strike; in contrast to crisis instability, these escalation pressures could be felt even if the state was not concerned about its nuclear forces being vulnerable or its ability to transmit employment orders to them.

Two questions arise when assessing the escalation risks of misinterpreted warning. First, how likely is it that the target would interpret nonnuclear strikes against its dual-use C3I assets as possible preparations for nuclear use? Second, if the target did become concerned that it might shortly be on the receiving end a nuclear strike, would it be likely to react in ways that tended to catalyze further escalation?

Because Moscow and Beijing have different nuclear postures and doctrines, there are somewhat different reasons why their striking dual-use U.S. enabling assets might generate misinterpreted warning. U.S. incidental strikes on dual-use Chinese or Russian C3I assets could also lead to misinterpreted warning, though this possibility is not discussed further here.

HOW MISINTERPRETED WARNING COULD OCCUR. The United States government has indicated its belief that, in a conventional conflict, Russia might opt for limited nuclear use in an attempt to compel the United States into backing down—a strategy sometimes termed "escalate to de-escalate" in the Western discourse.[42] It also appears to worry that, if a limited nuclear war escalated, Russia might launch large-scale damage-limitation strikes against U.S. nuclear forces (even though such strikes could not deprive the United States of a second-strike capability today).[43] Whether these beliefs accurately reflect Russian strategy is essentially immaterial for current purposes; rather, they are important because, right or wrong, they would likely inform the United States' assessment of Russia's intentions in a conflict. In this way, for at least three reasons, these beliefs create the potential for Washington to misinterpret Russian incidental strikes against dual-use U.S. C3I assets as preparations for nuclear use.

First, Russia might attack ground-based or space-based U.S. early-warning assets to defeat European missile defenses that were proving effective in inter-

42. U.S. Department of Defense, "Nuclear Posture Review," p. 30; and Robert Work and James Winnefeld, prepared statement, *Nuclear Deterrence in the 21st Century*, hearing before the Committee on Armed Services, U.S. House of Representatives, 114th Cong., 1st sess., June 25, 2015, p. 4, http://docs.house.gov/meetings/AS/AS00/20150625/103669/HHRG-114-AS00-Wstate-WinnefeldJrUSNJ-20150625.pdf.

43. The emphasis that the United States places on force survivability in official policy can only be explained by concerns about damage-limiting Russian strikes.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

cepting its nonnuclear missiles. Washington might see such attacks, however, as preparations to ensure that limited nuclear strikes by Russia could penetrate the United States' homeland missile defenses. Government-affiliated Russian experts have publicly advocated "limited strategic strikes" against the U.S. homeland under a variety of circumstances (including if Russia became concerned that the United States was about to embark on a conventional counterforce campaign against its nuclear forces).[44] Such experts have also expressed concern that U.S. missile defenses might be capable of defeating such strikes. Indeed, the United States has declared that homeland defenses "would be employed to defend the United States against limited missile launches from any source" (even if such defenses cannot cope with large-scale attacks).[45] In response, Russian strategists have suggested that, prior to launching limited strategic strikes, Moscow should try to neutralize those defenses by attacking the U.S. early-warning system.[46] If Washington interpreted strikes against its early-warning capabilities in this light, misinterpreted warning could arise.

Second, Russia could attack dual-use U.S. communication assets to undermine a variety of American nonnuclear operations. Washington could interpret such attacks, however, as an attempt to forestall a proportionate U.S. response to the limited use of low-yield nuclear weapons. Nuclear-armed aircraft might well be the United States' preferred means of responding to a limited nuclear strike, because the B-61 gravity bomb has the lowest-yield nuclear option in the U.S. arsenal.[47] The communication links for deployed aircraft, however, are particularly vulnerable to being severed.[48] Russian incidental strikes might destroy the satellites and ground-based transmitters that could enable communications with aircraft operating over or around Russia. Meanwhile, communication aircraft operating over the United States would probably be too distant to direct operations in that region. Washington, therefore, could interpret Russian attacks against U.S. communication links as an attempt to deny the United States the ability to respond in kind to a low-yield

44. Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," pp. 20–21.
45. U.S. Department of Defense, "Ballistic Missile Defense Review Report" (Washington, D.C.: U.S. Department of Defense, February 2010), p. 13, http://archive.defense.gov/bmdr/docs/BMDR%20as%20of%2026JAN10%200630_for%20web.pdf.
46. Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," p. 31.
47. The 2018 Nuclear Posture Review calls for the acquisition of additional submarine-based low-yield nuclear capabilities. Whether and when these weapons will be deployed remains to be seen. See U.S. Department of Defense, "Nuclear Posture Review," pp. 54–55.
48. In theory, the United States could still use aircraft for nuclear operations by "pre-programming" targets at take-off or shortly afterward. This approach, however, would undermine the maintenance of positive control throughout a flight, which is a key rationale for maintaining nuclear-armed aircraft.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

nuclear strike in the hope that it would be deterred from a more forceful response by the fear of further escalation.

Third, Russian attacks against dual-use U.S. early-warning or communication assets would risk being seen as a signal of Russia's resolve to use nuclear weapons unless the United States conceded to its demands. In an effort to deter limited nuclear use by Russia, senior U.S. officials have publicly stressed the risk of escalation to a strategic nuclear war, stating, for example, that "anyone who thinks they can control escalation through the use of nuclear weapons is literally playing with fire."[49] Because Russian incidental strikes against dual-use U.S. C3I assets could help Russia fight a strategic nuclear war, they could be interpreted by Washington as an effort to enhance the credibility of limited nuclear use. For example, degrading the U.S. early-warning system might prevent the United States from launching ICBMs, dispersing bombers, or sheltering national leaders before they were eliminated in a nuclear attack. Similarly, disabling communication systems might slow a U.S. nuclear response to a Russian counterforce strike, giving Russia time for follow-up damage-limitation strikes.

To be sure, the United States' interpretation of Russian strikes against dual-use U.S. enabling assets would likely depend on the context. Had Russia raised the alert level of its nuclear forces, dispersed them, or even issued orders to prepare them for nuclear employment? Had Moscow put into action plans to try to ensure the continuity of government in the event of a nuclear war? What messages was the government sending to its own population? Would it be threatened from within if it lost the war? In practice, such questions could be extremely difficult to answer because, by the time that Russia had attacked dual-use U.S. early-warning and communication assets, it would probably have launched extensive attacks against U.S. ISR capabilities, potentially denying much needed contextual information to the United States.[50] In the absence of this information, Washington might feel its most prudent course of action was to assume the worst about Moscow's intentions.

The risk of the United States' misinterpreting Chinese nonnuclear strikes against dual-use U.S. C3I assets as preparations for nuclear use would probably be lower than in the case of Russia for two reasons. First, in contrast to Moscow, Beijing has adopted a no-first-use pledge. Second, unlike their

49. Work and Winnefeld, prepared statement, p. 4. See also U.S. Department of Defense, "Nuclear Posture Review," p. 30.
50. Forrest E. Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment" (Santa Monica, Calif.: RAND Corporation, 2010), p. 19, http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG916.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Russian counterparts, Chinese leaders can have absolutely no doubt that nuclear first use would do nothing to meaningfully limit the damage their country would suffer in a nuclear war with the United States. As a result, Washington would be unlikely to interpret Chinese nonnuclear strikes as preparations to fight and win a strategic nuclear war.

That said, the United States could still interpret Chinese attacks against its early-warning system as preparations for limited nuclear strikes intended to terrify the United States into terminating a conflict on terms not too unfavorable to Beijing. Fairly or not, Washington does not have complete confidence in the reliability of China's no-first-use pledge.[51] In particular, skeptics typically argue that Beijing would be most likely to abandon this pledge if China were in danger of losing a war over Taiwan—an outcome that could jeopardize the continued rule of the Chinese Communist Party.[52] If, in this circumstance, China attacked critical U.S. early-warning assets—satellites, in particular—in an effort to help its conventional ballistic missiles penetrate U.S. defenses, Washington might conclude that desperate Chinese leaders were preparing limited nuclear strikes, against either the United States or regional targets.[53]

Again, much would depend on context. The likelihood of misinterpreted warning would probably increase if, in addition to attacking dual-use U.S. enabling capabilities, China had dispersed or alerted nuclear-armed missiles. Although this step could be a standard defensive precaution to protect the missiles' survivability in a major conflict, it might also exacerbate concerns in Washington about the possibility of Chinese first use. Some nuclear-armed medium-range DF-21A ballistic missiles appear to be targeting U.S. assets in the West Pacific.[54] The alerting of these missiles could be seen by the United States, therefore, as preparations for regional nuclear strikes. The alerting of

51. These concerns are strongly suggested, although not stated explicitly, in U.S. Department of Defense, "Nuclear Posture Review," p. 32.

52. Mark Schneider, "The Nuclear Doctrine and Forces of the People's Republic of China" (Fairfax, Va.: National Institute Press, November 2007), pp. 7–8, http://www.nipp.org/wp-content/uploads/2014/12/China-nuclear-final-pub.pdf.

53. Early in a conflict, probable Chinese attacks on regional missile-defense radars would likely be less escalatory, because China would probably not be facing defeat then and because such radars are not critical to nuclear operations. The PAVE PAWS radar in Taiwan is a special case and discussed below.

54. Because certain Chinese missile brigades (notably, the 807 brigade in Anhui, but also perhaps the 810 brigade in Liaoning and the 816 brigade in Jilin) are not within range of important Russian or Indian targets, it is difficult to see what other role they could serve. See Jeffrey Lewis, *Paper Tigers: China's Nuclear Posture*, Adelphi 446 (Abingdon, U.K.: Routledge for the International Institute for Strategic Studies, 2014), p. 116. See also U.S. Department of Defense, "Nuclear Posture Review," p. 31.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

China's ICBM force, meanwhile, could be interpreted as an attempt to threaten the U.S. homeland and so deter nuclear retaliation to Chinese first use against regional targets. The escalation pressures might be more serious still if China had conducted extensive attacks against U.S. ISR assets, denying the United States contextual information that might be helpful in interpreting Chinese intentions correctly.

HOW THE UNITED STATES MIGHT RESPOND TO MISINTERPRETED WARNING. The United States' response to misinterpreted warning would probably depend on a range of factors, including its assessment of the likelihood of nuclear use by the adversary. Nonetheless, an overriding consideration would probably be to deter such use or, if deterrence failed, to limit the damage that the United States would suffer in a nuclear war—a goal explicitly articulated in the 2018 Nuclear Posture Review.[55] As such, misinterpreted warning could lead to at least three general types of U.S. response; none of which is mutually exclusive and all of which could spark further escalation.

First and most immediate, the United States would probably seek to protect surviving elements of its nuclear C3I system because of their importance to damage-limitation efforts, including counterforce attacks and missile defense operations. As described below, for these efforts to have any hope of success, the United States would have to preserve much more than just the relatively basic capability needed to transmit employment orders to survivable nuclear forces. Steps to preserve surviving C3I capabilities could prove escalatory. For example, the United States might attack ASAT weapons that it believed could threaten important U.S. satellites. If these weapons were located deep inside China or Russia, then such attacks could spark escalation, especially if the United States had previously avoided striking far inside its adversary's borders in an effort to keep the war limited. Alternatively, or additionally, the United States could launch tit-for-tat strikes against equivalent Chinese or Russian enabling assets in an attempt to coerce Beijing or Moscow into ceasing attacks on U.S. C3I assets—potentially leading the adversary to fear for the survivability of its nuclear forces and generating crisis instability.

Second, misinterpreted warning might prompt the United States to alert bombers and send additional ballistic missile submarines (SSBNs) to sea. Although neither China nor Russia could hope to disarm the United States, both could plausibly threaten U.S. submarines in port and bombers at their bases. In consequence, enhancing the survivability of these platforms might seem

55. U.S. Department of Defense, "Nuclear Posture Review," p. 23.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

to Washington like a sensible precaution. If the adversary were not planning to use nuclear weapons, however, this precaution could appear to be threatening. In particular, Beijing or Moscow might worry about the possibility of attacks with very short warning times launched from forward-deployed stealthy bombers or from SSBNs firing SLBMs on depressed trajectories from near its coasts. In turn, China or Russia might respond by taking steps to enhance the survivability of its nuclear forces, such as dispersing mobile missiles, which could appear to confirm Washington's fears. In this way, misinterpreted warning and crisis instability could exacerbate each other.

Third, the United States could threaten to use—or even use—nuclear weapons in response to misinterpreted warning. Following attacks on dual-use U.S. C3I assets, Washington might threaten to use nuclear weapons if the attacks continued or if the adversary employed nuclear weapons. Such a threat, however, could trigger an escalation cycle similar to the one that might be sparked by the dispersal of U.S. SSBNs and bombers. Alternatively, if the adversary did not judge the threat to be credible and continued to attack U.S. C3I assets, the United States might feel compelled to follow through on its threat and resort to nuclear use. Although it could attempt a disarming first strike, the limited use of nuclear weapons would probably be more likely. U.S. leaders—mirroring the precise logic that they were ascribing to their Chinese or Russian counterparts—might hope that such strikes would terrify the adversary into complying with U.S. demands.

It is even possible that the United States would respond directly to attacks on dual-use C3I assets with the use of nuclear weapons, without first issuing a nuclear threat. Although such a response would be disproportionate and thus unlikely, Washington might feel that having threatened, in the 2018 Nuclear Posture Review, to use nuclear weapons in this eventuality, it had to follow through or else risk damaging its credibility and very undermining other elements of U.S. declaratory policy.[56]

### THE DAMAGE-LIMITATION WINDOW

Although all nuclear operations require C3I capabilities, the enabling requirements for damage-limitation operations would be particularly demanding. Significant damage to a state's nuclear C3I system would preclude any possi-

56. For an analysis of why immediate nuclear use would be disproportionate, see James Acton, "Command and Control in the Nuclear Posture Review: Right Problem, Wrong Solution," *War on the Rocks*, February 5, 2018, https://warontherocks.com/2018/02/command-and-control-in-the-nuclear-posture-review-right-problem-wrong-solution/.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

bility of such operations being effective. Because many enabling capabilities are dual use and could be attacked or threatened in a conventional war, a state with a damage-limitation doctrine might conclude that it had only a narrow window of opportunity near the start of a conflict in which it could realistically try to attack its opponent's nuclear forces and to defend against whatever it failed to destroy. Fear that this damage-limitation window might close could create pressures for the state to conduct counterforce strikes preemptively or, more likely, initiate aggressive military operations to try to preserve the option of conducting damage-limitation operations later on.[57]

These escalation pressures differ from those created by crisis instability in that escalation would be motivated by the goal of holding an adversary's nuclear forces at risk, not of ensuring the survivability of the state's own forces. Although there are some similarities between the damage-limitation window and misinterpreted warning—particularly in that they might spark aggressive efforts to protect surviving C3I capabilities—there is one critical difference. Escalation driven by fear of the damage-limitation window's closing stems from the unavoidable possibility that a war between two nuclear-armed states might ultimately turn nuclear and could be felt even if neither state believed its adversary was currently preparing for nuclear use.

Damage-limitation operations would consist of counterforce attacks, backed up by missile defenses. The United States openly acknowledges that it plans for counterforce attacks. Specifically, according to the 2013 "Report on Nuclear Employment Strategy of the United States," the most recent authoritative public statement on U.S. targeting policy, "guidance requires the United States to maintain significant counterforce capabilities against potential adversaries."[58] Meanwhile, Washington appears to assume that Moscow might also launch counterforce attacks. By contrast, there is no evidence that Beijing contemplates such attacks, not least because it lacks the capability to conduct them on a meaningful scale. Fear of the damage-limitation window's closing, therefore, could generate escalation pressures on Russia but not China—though this section again focuses on the United States.

57. Charles L. Glaser and Steve Fetter observe, in a parallel line of reasoning, that the possibility of an adversary alerting its nuclear forces could create escalation pressures by complicating damage-limitation operations. See Glaser and Fetter, "Should the United States Reject MAD? Damage Limitation and U.S. Nuclear Strategy toward China," *International Security*, Vol. 41, No. 1 (Summer 2016), pp. 61–62, doi:10.1162/ISEC_a_00248.

58. U.S. Department of Defense, "Report on Nuclear Employment Strategy of the United States Specified in Section 491 of 10 U.S.C." (Washington, D.C.: U.S. Department of Defense, June 2013), p. 4, http://www.defense.gov/Portals/1/Documents/pubs/ReporttoCongressonUSNuclearEmploymentStrategy_Section491.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

The importance of C3I capabilities to damage-limitation operations is difficult to overstate. Attacking dispersed mobile missiles would be particularly challenging. Despite much debate among U.S. strategists about how effective such efforts might prove, there is no disagreement that without high-quality ISR to detect and track missiles, along with fast and reliable communications to relay targeting data, they would be certain to fail.[59] Anti-submarine warfare operations by the United States against an enemy's SSBNs would also benefit from sophisticated enabling capabilities. Such efforts would be more likely to succeed if the operations of U.S. aircraft, surface ships, and attack submarines were coordinated, and if these platforms could share information, placing a premium on high-bandwidth communications. Meanwhile, early-warning capabilities would enable U.S. ICBMs to be launched before they were destroyed by a large-scale Russian nuclear strike (potentially enabling the United States to target any nuclear forces held in reserve by Russia). Early-warning capabilities would also be important because of their role in both regional and homeland missile defense operations. Interestingly, in this way, the existence of missile defenses is not guaranteed to reduce time pressure on the United States to act, but can, in some circumstances, actually increase it.

Even during the Cold War, when many enabling capabilities were reserved exclusively for nuclear operations and were largely invulnerable to an adversary's nonnuclear weapons, there was concern that nuclear threats to C3I assets could create escalation pressures by threatening to preclude damage limitation.[60] Today, this escalation risk is magnified by the possibility that such assets could be degraded, through incidental attacks, over the course of a conventional war.

The possibility of U.S. damage-limitation operations becoming infeasible could spark serious concern in Washington. In extremis, the United States might respond by launching counterforce attacks preemptively, while its C3I capabilities were still intact. In less extreme circumstances, it might initiate

59. For recent contributions to this debate see, for example, Glaser and Fetter, "Should the United States Reject MAD?" pp. 63–70; Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, Vol. 38, Nos. 1–2 (2015), pp. 38–73, doi:10.1080/01402390.2014.958150; and Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security*, Vol. 41, No. 4 (Spring 2017), pp. 9–49, https://doi.org/10.1162/ISEC_a_00273.

60. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, N.Y.: Cornell University Press, 1989), p. 165. For a Cold War analysis of how attacks on C3I capabilities could blunt the effectiveness of nuclear operations, see Ashton B. Carter, "Assessing Command System Vulnerability," in Carter, John D. Steinbruner, and Charles A. Zraket, eds., *Managing Nuclear Operations* (Washington, D.C.: Brookings Institution Press, 1987), pp. 555–610.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

escalatory military operations, such as those described above, to protect these capabilities and hence preserve the option of conducting counterforce operations at a later time. As with misinterpreted warning, the United States could also threaten that further attacks against key U.S. C3I capabilities would precipitate a nuclear response. If attacks continued, it might follow through on this threat.

### CRISIS INSTABILITY

Crisis instability could be induced by threats to the survival of a state's nuclear forces or their enabling capabilities.[61] In assessing the significance of such threats, the "key question," argues Caitlyn Talmadge, "would not be whether the target state expected to suffer complete nuclear disarmament . . . [but whether it] feared the erosion of its nuclear capabilities past some threshold considered vital to its security."[62] (In the general political science literature, the term "crisis instability" is often used in a somewhat different sense to describe the tendency to resort to the use of force in a crisis.)

In the Cold War, analysts generally assumed that if crisis instability led to nuclear first use, such use would be in the form of a large-scale preemptive first strike. Today, if the United States or, much more likely, Russia felt its nuclear forces or associated C3I capabilities to be in severe danger (whether from nuclear or nonnuclear threats), it might conceivably launch such a strike. Other responses, however, would probably be much more likely—including by China, which lacks the capability for effective large-scale preemption.[63] For example, a state might enhance the survivability of its nuclear forces by dispersing mobile weapons. The national leadership might pre-delegate nuclear launch authority to field commanders. To try to scare its opponent into backing down from threatening its nuclear forces, a state might threaten to use nuclear weapons or even use them in a limited way.[64] All of these steps could spark further escalation, albeit with varying likelihoods.

The possibility that nonnuclear operations might induce crisis instability was first discussed by scholars toward the end of the Cold War, in part because

61. The literature on crisis stability is vast, but the seminal discussion is Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard University Press, 1960), chap. 9. For the concept's historical origins, see Michael S. Gerson, "The Origins of Strategic Stability: The United States and the Threat of Surprise Attack," in Elbridge A. Colby and Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, Pa.: U.S. Army War College Press, 2013), chap. 1, http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1144.
62. Talmadge, "Would China Go Nuclear?" p. 63; see pp. 57–64 more generally.
63. Michael S. Gerson, "No First Use: The Next Step for U.S. Nuclear Policy," *International Security*, Vol. 35, No. 2 (Fall 2010), pp. 35–39, doi:10.1162/ISEC_a_00018.
64. Talmadge, "Would China Go Nuclear?" pp. 58–59.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

of the potential for such operations to degrade C3I capabilities. Most significantly, in his 1991 study, *Inadvertent Escalation*, Posen argued that, as the Soviet early-warning network was degraded over the course of a conventional war in Europe, Moscow might come to believe that the United States was about to decapitate the Soviet nuclear C3I system and launch a preemptive first strike.[65] At about the same time, Bruce Blair identified the vulnerability of the U.S. nuclear C3I system to Soviet nonnuclear weapons as another potential trigger of crisis instability.[66]

More recently, scholarly discussions of the implications of C3I vulnerability for crisis instability have focused on the possibility of U.S. nonnuclear attacks on Chinese C3I capabilities located in the theater of operations—in particular, the communication system for China's land-based mobile missiles, but also its air-defense radars.[67] Other C3I assets, including Chinese and Russian early-warning capabilities and U.S. communication capabilities, are also entangled, creating escalation risks that have not been identified before in the academic literature.

Russia has developed various capabilities to provide early warning of an incoming attack with nuclear-armed ballistic missiles. China, meanwhile, appears to be in the process of doing so. One potential purpose of such capabilities is to enable a state to launch nuclear weapons before they are destroyed. Russian nuclear doctrine is generally believed to include this option, known as "launch under attack" or "launch on warning" (neither term has a universally accepted definition, although the United States adopts the former in describing its own policy). There is evidence, including in the 2013 edition of *Science of Military Strategy*, a textbook published by the People's Liberation Army Academy of Military Sciences, that China may be moving in the same direction (though if so, it may be planning to alert its forces in a crisis rather than keep them on day-to-day alert).[68] Separately, both states have extensive air-

65. Posen, *Inadvertent Escalation*, chaps. 2–3. See also Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington, D.C.: Brookings Institution Press, 1993), pp. 270–271.
66. Bruce G. Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, D.C.: Brookings Institution, 1985), pp. 207, 296–297; and Bruce G. Blair, "Alerting in Crisis and Conventional War," in Carter, Steinbruner, and Zraket, *Managing Nuclear Operations*, pp. 107–108.
67. On attacks against communication assets, see Chase, Erickson, and Yeaw, "Chinese Theater and Strategic Missile Force Modernization and Its Implications for the United States," pp. 105–106; Pollack, "Emerging Strategic Dilemmas in U.S.-Chinese Relations," pp. 57–58; Christensen, "The Meaning of the Nuclear Evolution," p. 468; Cunningham and Fravel, "Assuring Assured Retaliation," pp. 42, 44; and Talmadge, "Would China Go Nuclear?" pp. 78–79. On attacks against air defenses, see Talmadge, "Would China Go Nuclear?" pp. 78–79." On attacks against air defenses, see Talmadge, "Would China Go Nuclear?" pp. 77–78.
68. Gregory Kulacki, "The Chinese Military Updates China's Nuclear Strategy" (Cambridge, Mass.: Union of Concerned Scientists, March 2015), p. 4, http://www.ucsusa.org/sites/default/files/attach/2015/03/chinese-nuclear-strategy-full-report.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

defense systems, which probably play an important role in protecting their nuclear forces and associated C3I capabilities from the perceived threat of nuclear or nonnuclear attack by U.S. aircraft and cruise missiles.

At least three types of Chinese or Russian early-warning assets are already entangled—or could become entangled—and, therefore, might be subject to incidental attacks by the United States, with the consequent risk of crisis instability. First, the United States might target China's or Russia's small collection of over-the-horizon radars, which can detect some threats at much greater distances than conventional line-of-sight radars.[69] As other analysts have noted, the United States might have a variety of incentives, in a conventional conflict, to strike these radars—especially, perhaps, Chinese ones with a role in locating U.S. aircraft carriers.[70] What has not been noted before (at least in the context of a discussion of escalation risks) is that China and Russia appear to regard their over-the-horizon radars as perhaps their best means of gaining at least some warning of a U.S. attack with stealthy aircraft or cruise missiles, which they worry pose a serious threat to the survivability of their nuclear forces.[71] The loss of these radars, therefore, could be particularly disquieting to Beijing or Moscow.

Second, an even more serious escalation risk that appears to have gone entirely unnoticed by analysts is incidental attacks on BMEWRs—particularly the network of these radars that rings Russia. These dual-use radars are probably Russia's most important assets for space situational awareness up to a few thousand kilometers in altitude and so enable Russia to hold numerous U.S. satellites at risk.[72] In consequence, the United States could strike this network

69. Pavel Podvig, "Russia Begins Deployment of Over-the-Horizon Radars," *Russian Strategic Nuclear Forces* blog, December 3, 2013, http://russianforces.org/blog/2013/12/russia_begins_deployment_of_ov.shtml; and Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2014," annual report to Congress (Washington, D.C.: U.S. Department of Defense, 2014) pp. 40, 69, http://www.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf.

70. Twomey, "Asia's Complex Strategic Environment," p. 64. Of the two types of over-the-horizon radars, skywave and groundwave, the former could have a role in detecting both ships and air-breathing threats.

71. Zhou Wanxing, "Tianbo Chaoshiju Leida Fazhan Zongshu" [Summary of the development of Skywave over-the-horizon radar], *Journal of Electronics*, Vol. 39, No. 6 (2011), pp. 1375–1376 (in Chinese; the author thanks Tong Zhao for translating the relevant section of this article); Podvig, "Russia Begins Deployment of Over-the-Horizon Radars"; and "I See You: Russian-Made Sunflower Radar Is Capable of Detecting F-35 Jets," Sputnik, July 2, 2016, http://sputniknews.com/science/20160702/1042341025/russia-podsolnukh-radar-f35.html.

72. Pavel Podvig, "Status of the Russian Early-Warning Radar Network," *Russian Strategic Nuclear Forces* blog, January 13, 2013, http://russianforces.org/blog/2013/01/status_of_the_russian_early-warning.shtml.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

in an effort to protect its satellites. Such attacks could generate severe crisis instability, given Russia's reliance on launch under attack.

At least two Chinese BMEWRs can be identified from publicly available satellite imagery—although it is unclear how many such radars China possesses or how many it ultimately intends to construct.[73] Chinese BMEWRs have an inherent capability to contribute to space situational awareness and hence enable ASAT operations, making them potential U.S. targets. Moreover, China may be building BMEWRs to enable the switch to a launch-under-attack posture. If it does so, China could view U.S. strikes against those radars as an attempt to undermine the survivability of its nuclear forces.

Other technological developments could exacerbate the escalation risks associated with attacks on BMEWRs yet further. Today, Chinese and Russian BMEWRs would be generally incapable of tracking most U.S. nonnuclear weapons, such as aircraft and cruise missiles (not least because of the relatively low altitude at which such weapons fly). The United States, however, is considering acquiring long-range nonnuclear ballistic missiles, which could be tracked by BMEWRs.[74] If the United States decides to deploy nonnuclear ballistic missiles, it might attack such radars, in a conflict, to suppress Chinese or Russian defenses.

Third, for a similar reason, U.S. strikes against Russian or possible Chinese early-warning satellites, which seem unlikely today, could become more plausible in the future. Since November 2015, Russia has deployed two satellites as part of a new space-based early-warning system, and it has ambitious plans to deploy "about ten" by 2020.[75] Even if such plans are only partially realized, Russia may significantly increase its reliance on space-based early warning. Meanwhile, the U.S. Department of Defense assesses that China also has an interest in acquiring early-warning satellites.[76] In fact, according to me-

73. These were identified by Catherine Dill and are located at 46.528085°N, 130.755181°E (in Heilongjiang) and 30.286637°N, 119.128591°E (in Zhejiang). Given its location, a similar radar at 41.641422°N, 86.237161°E (in Xinjiang) is probably used for monitoring China's own testing activities. Author's personal communications with Catherine Dill and Jeffrey Lewis, 2016–2018.

74. A requirement in the Fiscal Year 2018 U.S. National Defense Authorization Act is likely to involve the Department of Defense studying the feasibility of converting missile-defense interceptors into land-attack ballistic missiles. See *National Defense Authorization Act for Fiscal Year 2018*, Public Law 115-91, 115th Cong., 1st sess. (December 12, 2017), sec. 1243.(c).(2).

75. William Graham, "Soyuz 2-1B Launches Tundra Missile Detection Spacecraft," nasaspaceflight.com, May 25, 2017, https://www.nasaspaceflight.com/2017/05/soyuz-2-1b-launches-tundra-missile-detection-spacecraft/; and "Russia to Launch Ten Missile Attack Warning Satellites by 2020," TASS, December 20, 2016, http://tass.com/defense/920880.

76. Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2017," p. 61.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

dia reports China had developed plans, by as early as 2014, to deploy its first such satellite.[77] For the time being, Russian and possible Chinese satellites may not contribute enough to nonnuclear military operations for them to become plausible targets of incidental U.S. strikes. If, however, the United States deploys nonnuclear ballistic missiles or hypersonic boost-glide weapons, which such satellites could track, that calculus could change, creating additional potential triggers of crisis instability.[78]

Even more dramatically, over the next decade or two, actual or threatened nonnuclear attacks by Russia against the United States could generate crisis instability, most likely by incidental strikes against dual-use U.S. communication capabilities. (In the more distant future, if China develops significant counterforce capabilities, it too could generate crisis instability through such attacks, though that possibility is not considered further here.)

The United States has acknowledged three "layers" of capabilities for sending employment orders to deployed nuclear forces: satellites, ground-based transmitters, and airborne transmitters.[79] The two U.S. satellite constellations for communicating with nuclear forces—the legacy Milstar system and newer AEHF system—are dual use. Because these satellites are in high-altitude geostationary orbits, there would be particular challenges in attacking them (including the possibility of evasive maneuvering by the target satellite in the time required for a direct-ascent weapon to reach it after launch). Such challenges notwithstanding, these satellites are likely to be vulnerable soon—if they are not already.[80] Russia has reportedly preserved—and may be enhancing—legacy Soviet direct-ascent ASAT weapons able to reach geostationary orbit and, in 2015, demonstrated an apparent co-orbital capability against satellites in that orbit.[81]

The United States also operates two networks of dual-use ground-based

77. "China Plans to Launch Test Satellite for Missile Defense," Japan Economic Newswire, August 24, 2015.
78. Indeed, media reports claim that both China's and Russia's early-warning satellites have the capability to contribute to missile-defense operations. See ibid.; and Graham, "Soyuz 2-1B Launches Tundra Missile Detection Spacecraft."
79. It is possible that the United States has additional classified systems. Because only a handful of technologies can communicate over long distances, however, any such systems would be likely to suffer from vulnerabilities similar to those of acknowledged systems.
80. The U.S. intelligence community assesses that "Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years." This wording may suggest that nondestructive ASAT weapons may already be operational. See Coates, "Worldwide Threat Assessment of the U.S. Intelligence Community," p. 13.
81. Brian Weeden, "Dancing in the Dark Redux: Recent Russian Rendezvous and Proximity Operations in Space," *Space Review*, October 5, 2015, http://www.thespacereview.com/article/2839/1; and Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," pp. 33–35.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

transmitters that it can use to send employment orders to nuclear forces. The Fixed Submarine Broadcast System appears to comprise nine transmitters located mostly around the peripheries of the Atlantic and Pacific Oceans.[82] The High Frequency Global Communications System for communicating with bombers (and perhaps other nuclear delivery systems, too) consists of thirteen transmitters spread across the globe.[83] All of these transmitters are large fixed structures that (with one exception) are located near coasts, making them vulnerable to Russian sea- and air-launched cruise missiles, in particular.[84]

In a conventional conflict against NATO, Moscow might attack U.S. communication assets in an effort to further its warfighting goals. Russian strategists "can hardly imagine [such a] conflict failing to spread from the Euro-Atlantic region to the Far East-Pacific."[85] As a result, even in a European conflict, Russia might not limit its attacks to U.S. communication assets located in or around Europe. In fact, Russia could plausibly launch incidental strikes (most likely in a series of waves) against dual-use land-based transmitters spread around the Euro-Atlantic and Asia-Pacific areas, and, even more significantly, against perhaps three out of the four AEHF satellites (depending on exactly how the constellation is configured after Milstar satellites are retired). Washington would surely have little confidence that any remaining space- and land-based assets for communicating with nuclear forces would survive for long.

In this scenario, the United States would become critically dependent on E-4B and E-6B aircraft, which are designed to protect national and military leaders and facilitate communications with both nuclear and nonnuclear forces.[86] Indeed, a recent U.S. Strategic Command exercise, Global Thunder 2018, involved an adversary's attacking U.S. nuclear C3I assets until "the last thing remaining [was] the jet."[87] For now, these aircraft would likely be surviv-

82. U.S. Department of the Navy, "Submarine Communications Master Plan."
83. Dwayne Harris, "HFGCS Status" (Boston: Rockwell Collins, February 4, 2010), p. 5, http://www.hfindustry.com/meetings_presentations/presentation_materials/2010_feb_hfia/presentations/HFGCS_HFIA_Feb_2010.pdf.
84. The exception is a High Frequency Global Communications System transmitter in Nebraska. Given its location, however, it is unlikely to be involved in directing operations involving forward-deployed aircraft.
85. Alexei Arbatov, "Gambit or Endgame? The New State of Arms Control" (Moscow: Carnegie Moscow Center, March 2011), p. 6, http://carnegieendowment.org/files/gambit_endgame.pdf.
86. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, "Nuclear Matters Handbook 2016" (Washington, D.C.: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, 2016), p. 75, https://www.acq.osd.mil/ncbdp/nm/NMHB/docs/NMHB_2016-optimized.pdf.
87. Quoted in Sydney J. Freedberg Jr., "When the Football Comes Out, Who Watches the Presi-

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

able, because they could probably be protected by friendly forces while operating from U.S. airspace.

The survivability prospects of E-4B and E-6B aircraft over the longer term, however, are questionable. Because these aircraft use modified commercial airframes, they lack both the speed to escape threats and the stealth characteristics to avoid detection. Indeed, given that their fundamental purpose is communications, their eventual replacements could not be stealthy either. Russia, therefore, may be able to develop capabilities, such as long-range air-to-air weapons, that could threaten communication aircraft, even while operating over the United States. If so, incidental attacks on these aircraft—or even, perhaps, apparent preparations for such attacks—could generate crisis instability by appearing to be an attempt to undermine the U.S. nuclear deterrent by cutting off the ability of national leadership to communicate with deployed nuclear forces.

#### ESCALATION REDUX

Misinterpreted warning, the damage-limitation window, and crisis instability are not mutually exclusive. Multiple escalation pressures could arise simultaneously and even interact with one another. That said, for escalation to occur along any pathway, specific technological and doctrinal conditions would have to be fulfilled, as summarized in table 1. In abstract terms, each mechanism involves an "attacker" that launches or threatens nonnuclear attacks against a "target." Some conditions are necessary for the target to experience pressures to escalate the conflict. Others are contributory in that they increase the likelihood of escalation, but escalation can occur even if they are not fulfilled. For example, the target must have dual-use C3I capabilities, and those capabilities must be attacked or threatened for misinterpreted warning to occur. If the attacker has a counterforce nuclear doctrine (as Russia does), escalation is more likely. Nonetheless, escalation can still occur if the attacker does not plan for counterforce operations (as in the case of China).

## *Early Warning: Technical Vulnerabilities and Their Consequences*

Two questions arise when assessing the severity of the escalation risks described above. First, how important to nonnuclear warfighting are the assets involved in nuclear C3I? The more important they are, the more likely they

dent?" *Breaking Defense*, November 9, 2017, https://breakingdefense.com/2017/11/stratcom-wargames-its-own-death-who-watches-the-president/.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Table 1. Technological and Doctrinal Conditions for Escalation to Occur as a Result of Entanglement

| | Misinterpreted Warning | Damage-Limitation Window | Crisis Instability |
|---|---|---|---|
| Target's nuclear forces have been attacked by—or are perceived to be threatened by—attacker's nonnuclear weapons | | | ××[a] |
| Target's nuclear C3I (command, control, communication, and intelligence) capabilities have been attacked by—or are perceived to be threatened by—attacker's nonnuclear weapons | ×× | ×× | ××[a] |
| Target's nuclear delivery systems are dual use or superficially similar to nonnuclear delivery systems | | | × |
| Target's nuclear C3I capabilities are dual use | ×× | ×× | × |
| Attacker's nuclear doctrine calls for damage limitation | × | | × |
| Target's nuclear doctrine calls for damage limitation | × | ×× | |
| Attacker's conventional warfighting doctrine calls for attacks against C3I capabilities | × | × | × |

×× = necessary condition

× = exacerbating condition

[a]At least one of these conditions is necessary for crisis instability.

might be threatened or attacked in a conventional conflict. Second, how badly would strikes against dual-use enabling capabilities degrade the target's ability to prosecute a nuclear war? If the target's nuclear C3I system were highly resilient and limited strikes would do little to undermine its overall effectiveness, then the escalation risks of incidental strikes would probably be small. By contrast, if the loss of a few key enabling assets—in the worst case, just one—severely undermined the target's ability to conduct nuclear operations, escalation would be more likely.

This section demonstrates that the United States' early-warning system is deeply integrated into its conventional operations and that even limited strikes could lower its effectiveness significantly and so create serious escalation risks. Separately, it considers the risks of cyber interference with dual-use Chinese,

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Russian, and U.S. early-warning capabilities. These risks have some important differences from those that might result from kinetic strikes.

Threats to early-warning assets are important in generating escalation risks through crisis instability, misinterpreted warning, and in the cases of Russia and the United States, the damage-limitation window. For reasons of space, threats to other enabling capabilities are not considered here, though are potentially no less significant. Indeed, in a real conflict, it is possible that multiple enabling systems could be attacked or threatened—potentially very early in a conflict, especially where ISR is concerned—magnifying escalation risks.

As with Russia, early warning would be necessary for the United States to execute any of the launch-under-attack options included in its nuclear war plans.[88] Under its policy of "dual phenomenology," Washington requires "two independent information sources using different physical principles" in assessing a potential attack.[89] To this end, the United States has deployed two distinct missile early-warning capabilities.[90] Space-based infrared detectors can identify the hot gases that are expelled from a ballistic missile while its motor is firing. Later in flight, large land-based radars can monitor the incoming reentry vehicle, potentially from a distance of thousands of kilometers.

If U.S. launch-under-attack plans include the option to launch nuclear weapons before any nuclear detonations on American soil—as was the case toward the end of the Cold War and appears to be true today—then the United States' early-warning architecture has no redundancy at the systems level; the loss of early-warning data from either satellites or radars could prevent Washington from meeting its own requirement for dual phenomenology.[91]

### Threats to U.S. space-based early-warning assets

In 2018, the United States completed deployment of the Space-Based Infrared System (SBIRS) to replace the legacy Defense Support Program system for space-based early warning. The SBIRS constellation comprises six satel-

88. Bureau of Arms Control, Verification, and Compliance, "U.S. Nuclear Force Posture and De-Alerting," fact sheet (Washington, D.C.: U.S. Department of State, December 14, 2015), https://web.archive.org/web/20170101112527/https://www.state.gov/t/avc/rls/250644.htm.
89. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, "Nuclear Matters Handbook 2016," p. 76.
90. In addition, various systems can detect the detonations of nuclear warheads, but these are less useful for enhancing force survivability.
91. According to the U.S. State Department, "The President would have less than 30 minutes in which to make a decision to launch our ICBMs under attack." This timeline strongly suggests that a launch could take place before incoming warheads detonated. Bureau of Arms Control, Verification, and Compliance, "U.S. Nuclear Force Posture and De-Alerting." On Cold War policy, see Blair, *The Logic of Accidental Nuclear War*, pp. 168, 192.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

lites.[92] Four dedicated SBIRS GEO satellites are in geostationary orbits, about 36,000 kilometers above fixed points near the Equator. In addition, to provide coverage of the northern polar region, two more SBIRS HEO detectors are hosted by "classified" satellites, whose primary purpose is reportedly electronic-intelligence collection, in highly elliptical orbits.[93] These satellites spend most of their orbits in the Northern Hemisphere, reaching latitudes as high as 65°N.

As with U.S. communication satellites, it is likely that if SBIRS satellites are not already vulnerable, they will be soon.[94] The U.S. intelligence community assesses that both China and Russia are "advancing directed-energy weapons technologies for the purpose of fielding ASAT weapons that could blind or damage sensitive space-based optical sensors, such as those used for . . . missile defense."[95] Moreover, like Russia, China is funding the development of direct-ascent ASAT weapons and, in 2013, probably tested an ASAT weapon that may be capable of threating geostationary satellites.[96]

In a conventional conflict, an adversary could have at least two significant motivations for launching incidental attacks against the United States' SBIRS constellation. First, the electronic-intelligence collection satellites that reportedly host SBIRS HEO detectors are in orbits ideally suited for monitoring military activities in Russia's north, making them potential targets. One particularly strong motivation for Moscow to attack them might be to interfere with U.S. efforts to collect intelligence on the movements of the surface ships and submarines of Russia's Northern Fleet, which is based inside the Arctic Circle. In such strikes, the SBIRS HEO detectors would be collateral damage.

Second, China or Russia could target the SBIRS constellation because of its role in enabling nonnuclear operations. The constellation's most important

92. The United States has purchased additional satellites for replenishment purposes; more than six satellites, therefore, may temporarily be in orbit.
93. Office of the Secretary of Defense, "Report to the Defense and Intelligence Committees of the Congress of the United States on the Status of the Space Based Infrared System Program" (Washington, D.C.: U.S. Department of Defense, March 2005), p. 31, http://nsarchive.gwu.edu/NSAEBB/NSAEBB235/42.pdf; and Michel Capderou, *Handbook of Satellite Orbits: From Kepler to GPS*, trans. Stephen Lyle (Cham, Switzerland: Springer, 2014), p. 428 n. 133.
94. Attacks against ground-based uplinks or downlinks are also a threat, but are not considered further here.
95. Coates, "Worldwide Threat Assessment of the U.S. Intelligence Community," p. 13.
96. Brian Weeden, "Through a Glass, Darkly: Chinese, American, and Russian Anti-Satellite Testing in Space" (Broomfield, Colo.: Secure World Foundation, March 17, 2014), pp. 4–19, https://swfound.org/media/167224/through_a_glass_darkly_march2014.pdf; and U.S.-China Economic and Security Review Commission, "2015 Report to Congress" (Washington, D.C.: U.S. Government Printing Office, November 2015), pp. 292–298, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

such functions are providing early warning of, and cueing defenses against, nonnuclear ballistic missiles. In general, the more satellites were attacked, the more the performance of U.S. defenses would be degraded. SBIRS satellites are involved in other nonnuclear missions, including "intelligence collection" and "battlespace characterization," which includes "battle damage assessment, suppression of enemy air defense, [and] enemy aircraft surveillance."[97] In a few circumstances, these auxiliary functions could be sufficiently important to motivate an adversary to launch incidental attacks. For example, China might attack SBIRS satellites because of their ability to detect nonnuclear ballistic missiles early in flight and hence provide targeting data that the United States would find useful if it sought to hunt the mobile launchers from which such missiles were being launched.[98]

Not only might China or Russia attack SBIRS satellites in a conventional conflict, but such attacks—even if limited—could have serious negative implications for the United States' ability to monitor launches of the adversary's nuclear-armed ballistic missiles.[99] With six satellites, the SBIRS constellation can be—and, after the retirement of the remaining Defense Support Program satellites, presumably will be—configured so that most areas from which nuclear-armed missiles might plausibly be launched are monitored by at least three or four satellites at all times, providing some margin of redundancy. In practice, however, this margin could be worn away quickly. If Beijing or Moscow sought, in a conventional conflict, to undermine U.S. missile defenses by degrading the SBIRS constellation to point where it could not monitor nonnuclear missile launches from, respectively, Eastern China or Western Russia, the United States would also lose the capability to monitor the majority of its adversary's nuclear forces continuously from space.

The margin of redundancy for some potential launch sites is even thinner. For example, if Russia destroyed just two SBIRS satellites—either of the host satellites for SBIRS HEO detectors, and the western-most SBIRS GEO satellite (which would contribute significantly to ballistic missile defense operations in Europe)—it would deprive the United States of the space-based capability

97. Office of the Secretary of Defense, "Report to the Defense and Intelligence Committees of the Congress of the United States on the Status of the Space Based Infrared System Program," p. 4.
98. Morgan, "Deterrence and First-Strike Stability in Space," p. 20.
99. This discussion is based on the author's own analysis using NASA's General Mission Analysis Tool orbital modeling software and data about satellite orbits from Chris Peat, *Heavens Above* (website), http://www.heavens-above.com; and Jonathan McDowell, "Geostationary Orbit Catalog," *Jonathan's Space Report*, n.d., http://www.planet4589.org/space/log/geo.log. It assumes that, after legacy Defense Support Program satellites have been retired, SBIRS GEO 4 will be placed in an orbit at or near 66°E, where a Defense Support Program satellite is currently located.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

to continuously monitor potential Russian SSBN patrol areas in the North Atlantic Ocean close to Europe.

Moreover, the SBIRS constellation features a single-point vulnerability: the United States could not continuously monitor the northern polar region from space if either of the SBIRS HEO detectors were rendered inoperable. With just one of these detectors in operation, there would be slightly more than four-and-a-half hours each day during which the United States had no coverage of the northern polar region or only partial coverage. Gen. William Shelton, then commander of U.S. Space Command, was almost certainly referring to this weakness when, in 2014, he acknowledged, without further explanation, the existence of a single-point vulnerability in the SBIRS constellation.[100]

Historically, monitoring the northern polar region has not been a U.S. priority, presumably because so much of it used to be covered by ice year round that it was an undesirable area from which to launch ballistic missiles.[101] Indeed, until the first SBIRS HEO detector was launched in 2006, the United States relied solely on land-based radars for this task. As climate change further reduces the sea ice coverage of the Arctic Ocean, however, especially during summer, monitoring the northern polar region is probably becoming more important.

### THREATS TO U.S. LAND-BASED EARLY-WARNING ASSETS

The United States operates six land-based early-warning radars designed primarily to detect missile attacks against the United States: five PAVE PAWS radars are located in California, Massachusetts, Greenland, the United Kingdom, and Alaska, where a COBRA DANE radar is also based.[102] All of these ballistic missile early-warning radars are large and immobile, and hence potentially vulnerable to precise conventional weapons, including air- and sea-launched cruise missiles. In general, opening a complete hole in the U.S. network of BMEWRs would require the destruction of at least two or three radars.[103]

---

100. William L. Shelton, "Space and Cyberspace—Foundational Capabilities for the Joint Warfighter and the Nation," speech at the Air Force Association Air Warfare Symposium, Orlando, Florida, February 21, 2014, http://web.archive.org/web/20141225171206/http://www.afspc.af.mil/library/speeches/speech.asp?id=747.

101. Russian SSBNs reportedly had some capability to launch missiles from under relatively thin ice. Valery E. Yarynich, "$C^3$: Nuclear Command, Control Cooperation" (Washington, D.C.: Center for Defense Information, May 2003), p. 147, https://www.scribd.com/doc/282622838/C3-Nuclear-Command-Control-Cooperation.

102. Technically, after PAVE PAWS radars are upgraded to contribute to missile-defense operations, they are renamed Upgraded Early Warning Radars. Forward-deployed missile-defense radars, such as the AN/TPY-2, could also contribute to early warning.

103. In theory, the destruction of the radar in either California or Massachusetts would create such

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Although the primary mission of U.S. BMEWRs is to detect and track an incoming nuclear strike, they also contribute significantly to two nonnuclear operations. First, they have a significant role in tracking space objects, including U.S. satellites and potentially Chinese and Russian ASAT weapons. As a result, Beijing or Moscow might plausibly attack U.S. BMEWRs to maximize both the effectiveness and consequences of ASAT operations.

Second, like early-warning satellites, the United States' BMEWRs have (or, in some cases, are currently being upgraded to gain) the capability to contribute to defending against nonnuclear ballistic missile strikes. Indeed, both China and Russia evince an interest in holding ground-based U.S. ballistic missile defense assets at risk.[104] That said, today at least, only one BMEWR—the one based at Fylingdales in the United Kingdom—could likely become involved in defending against Chinese or Russian nonnuclear ballistic missile strikes and so be subject to incidental attacks.[105] Given the location of other U.S. BMEWRs, the only Chinese or Russian ballistic missiles that they would be likely to track would be SLBMs or ICBMs, all of which are currently nuclear armed.

The U.S. Fylingdales BMEWR is not only the radar most likely to suffer an incidental attack; it is also the most important radar for providing early warning of a Russian nuclear strike. Because it is based so far east of the continental United States, this radar could detect Russian ICBM and SLBM launches from most deployment areas much earlier than other U.S. BMEWRs. As a result, especially if Russia succeeded in partially or completely disabling the SBIRS constellation, follow-on attacks against the Fylingdales radar could be particularly escalatory. Looking forward, if China or Russia eventually develops nonnuclear ICBMs or SLBMs, then U.S. BMEWRs other than Fylingdales could take on a significant role in nonnuclear missile defense operations, creating new targets for incidental attacks and thus potential triggers of escalation.

---

a hole, but it is currently unlikely that either of these radars and no other would be subject to incidental attacks. The discussion in this section is based on the author's own analysis using Google Earth. The author thanks Geoffrey Forden and Pavel Podvig for assistance with, respectively, visualizing ballistic missile trajectories and radar fans. Data about the capabilities of U.S. BMEWRs are available from Missile Defense Agency, "Elements: Sensors" (Washington, D.C.: U.S. Department of Defense, January 22, 2018), https://www.mda.mil/system/sensors.html.

104. Second Artillery Corps, "The Science of Second Artillery Campaigns," pp. 318, 396–397; and Andrew E. Kramer, "Russian General Makes Threat on Missile-Defense Sites," *New York Times*, May 3, 2012, http://www.nytimes.com/2012/05/04/world/europe/russian-general-threatens-pre-emptive-attacks-on-missile-defense-sites.html.

105. The author estimates that the Fylingdales radar, if angled at 3 degrees above the horizontal, could track an Iskander ballistic missile with a range of 500 kilometers fired from Kaliningrad to western Poland for about 150 kilometers of its trajectory.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

Intriguingly, there may be an Asia-Pacific analogue to the Fylingdales radar—even if it is not a U.S. radar. In 2013, Taiwan commissioned a PAVE PAWS early-warning radar that it purchased from the United States. Taipei has stated that the sole purpose of this radar is to track Chinese short-range nonnuclear ballistic missiles.[106] This radar, however, does have an inherent capability to detect Chinese ICBMs early in flight. In fact, it could provide significantly more warning of a Chinese ICBM strike than any U.S. BMEWR, and a senior Taiwanese lawmaker has claimed that data from this radar is shared with the United States.[107] If this claim is correct, then incidental Chinese strikes against the radar could have significant escalation consequences. To be sure, China might attack this radar in the early phases of a conflict, while the war's outcome was still uncertain. At that juncture, the escalation risks would probably be modest, because China's incentives to use nuclear weapons would be minimal. If, however, China began to lose the conflict and subsequently attacked the United States' SBIRS satellites, then the already serious escalation consequences of attacking early-warning satellites would likely be compounded by China's earlier attack on the radar.

### cyber threats to early-warning systems

There are credible reports of cyber interference with early-warning systems. Most notably, when Israel destroyed Syria's clandestine plutonium-production reactor in 2007, it reportedly first disabled the Syrian air-defense system using a variety of tools, including cyberweapons, to reduce risks to the aircraft conducting the attack.[108] To be sure, nuclear C3I networks in China, Russia, and the United States are presumably protected by much better cyber defenses than Syria's air-defense system was a decade ago. Nonetheless, these states have launched efforts to enhance the cyber defenses of networks used for nuclear C3I, implying that they believe cyber threats to them are credible; indeed, the United States military has said so explicitly.[109] Yet, eliminating cyber vul-

106. "Taiwan Deploys Advanced Early Warning Radar System," *Straits Times*, February 3, 2013, http://www.straitstimes.com/asia/taiwan-deploys-advanced-early-warning-radar-system.
107. "Long-Range Radar Budget Surges by NT$10 Billion," *China Post*, January 6, 2013, https://web.archive.org/web/20130108092745/http://www.chinapost.com.tw/taiwan/national/national-news/2013/01/06/366468/Long-range-radar.htm.
108. David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot: Israel Shows Electronic Prowess: Attack on Syria Shows Israel Is Master of the High-Tech Battle," *Aviation Week & Space Technology*, November 26, 2007, pp. 28–31. See also Joshua Berlinger and Juliet Perry, "China Tried to Hack Group Linked to Controversial Missile Defense System, U.S. Cybersecurity Firm Says," *CNN*, April 27, 2017, http://www.cnn.com/2017/04/27/asia/china-south-korea-thaad-hack/.
109. See, for example, Michael Pillsbury, "The Sixteen Fears: China's Strategic Psychology," *Sur-*

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

nerabilities entirely may be impossible. The U.S. Defense Science Board, for example, has stated baldy that it is "impossible" for the U.S. Department of Defense to fully defend its networks.[110]

The existing literature on cyber threats to early-warning systems has not considered the possibility that dual-use early-warning capabilities might be subject to incidental cyber interference for the purpose of influencing the outcome of a conventional war.[111] (Because some physical early-warning assets in China, Russia, and the United States are dual use, at least some of the networks that support them must also be dual use.[112]) The term "cyber interference" is used here to include both cyber espionage (gathering information for intelligence purposes without damaging the operation of the target system) and cyberattack (attempting to undermine the target system's functionality by compromising the integrity or availability of its data).

The severity of the escalation risks stemming from incidental cyber interference with early-warning capabilities depends on at least two factors. One factor, as Erik Gatrzke and Jon Lindsay note, is whether the target detects the cyber interference.[113] The other is whether, if the interference is detected, the target correctly assesses the attacker's intent.

---

*vival*, Vol. 54, No. 5 (October/November 2012), p. 157, doi:10.1080/00396338.2012.728351; "Cyber Security Units to Protect Russia's Nuclear Weapons Stockpiles," *RT*, October 17, 2014, https://www.rt.com/news/196720-russia-missile-forces-cybersecurity/; and Benjamin D. Katz, "U.S. Beefs Up Cyber Defenses to Thwart Hacks of Nuclear Arsenal," *Bloomberg*, March 24, 2016, https://www.bloomberg.com/news/articles/2016-03-24/u-s-beefs-up-cyber-defenses-to-thwart-hacks-of-nuclear-arsenal.

110. Defense Science Board, U.S. Department of Defense, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat" (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013), p. 6, https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.

111. This literature focuses on two deliberate escalation risks. First, a malicious third party could try to catalyze a nuclear war between two nuclear-armed states by generating false warning of an incoming nuclear attack. Second, a state planning to launch a nuclear attack might first "blind" its opponent's early-warning system. See Global Zero Commission on Nuclear Risk Reduction, "De-Alerting and Stabilizing the World's Nuclear Force Postures" (Washington, D.C.: Global Zero, 2015), p. 30, http://www.globalzero.org/files/global_zero_commission_on_nuclear_risk_reduction_report_0.pdf; Andrew Futter, *Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security, and Strategy* (London: Royal United Services Institute for Defence and Security Studies, July 2016), pp. 24–25, https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf; and Stephen J. Cimbala, "Nuclear Cyberwar and Crisis Management," *Comparative Strategy*, Vol. 35, No. 2 (2016), p. 119, doi:10.1080/01495933.2016.1176458.

112. At the very least, the networks used to determine whether an incoming weapon was conventional or nuclear (and at all prior stages of the early-warning process) must be dual use.

113. Erik Gartzke and Jon R. Lindsay focus on deliberate attacks intended to undermine the target's nuclear deterrent. The escalation dynamics resulting from those attacks and incidental attacks would be different. See Gartzke and Lindsay, "Thermonuclear Cyber War," *Journal of Cyber Security*, Vol. 3, No. 1 (March 2017), pp. 37–48, doi:10.1093/cybsec/tyw017.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

In even a modest conventional conflict, a state's temptation to conduct cyber espionage against an enemy's C3I system could be very strong. In the case of dual-use early-warning networks, the state might focus on detecting its opponent's potential weaknesses—such as radars that were inoperative or performing poorly—so the state could exploit them to enable more effective offensive operations. Such cyber espionage could have escalation consequences only if the target discovered it. In this case, the espionage could contribute to misinterpreted warning, because the target might believe that its opponent was looking for weaknesses prior to using nuclear weapons. The exact consequences, though, would presumably depend on what the target believed the cyber espionage had revealed. For example, if Russia believed that the United States had discovered a serious weakness in its early-warning system, Moscow's confidence in the survivability of its nuclear forces could diminish, generating crisis instability on top of misinterpreted warning. By contrast, if Russia believed that the United States had failed to acquire anything of significance, the escalation consequences might be much more modest.

Cyberattacks designed to facilitate nonnuclear strikes by undermining the operation of an adversary's early-warning capabilities could also precipitate escalation. Once again, the attack could prove escalatory only if the target detected it. If a state did conclude that its early-warning system had been subject to a cyberattack, the escalation consequences could be as serious as if the system had been physically attacked, especially if the target believed that the damage could not be reversed quickly. In fact, the consequences might even be more serious because a cyberattack against a critical network (one responsible for fusing data from multiple sources, say) could disable an entire early-warning system, whereas kinetic strikes would have to pick off sensors one by one.

The risk of escalation could be further exacerbated by the challenges facing the target in determining the attacker's intent. Fully understanding the purpose of complex malware can be difficult and time consuming, and the target might be uncertain about its capabilities for a significant length of time—allowing considerable scope for worst-case thinking. For example, even if the malware were capable only of espionage, the target might worry it also contained a "kill switch" able to disable an early-warning system after activation. To create yet more uncertainty, a single penetration into a network can be used to insert multiple "payloads." For this reason, even if the target believed that ongoing interference was limited to espionage, it might worry that the vulnerability used by the attacker could be exploited for more nefarious ends (at least until that vulnerability had been identified and fixed).

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

In the final analysis, there would be at least two important differences between the escalation risks resulting from cyber interference with and physical attacks on dual-use early-warning systems. First, a physical attack on an early-warning asset would be significantly more difficult to conceal than cyber interference (even if not all physical attacks are equally obvious). Unlike plausible physical attacks, therefore, cyberattacks on early-warning systems might go undetected and have no escalation consequences. Second, with physical attacks on early-warning assets, the risk of inadvertent escalation would stem from the dual-use nature of the target. With cyber interference, this ambiguity would still exist but would be compounded by possible uncertainty about the interference's purpose. This "double ambiguity" is a major reason why the escalation risks of U.S. nonnuclear operations against China or Russia would be greater than previous academic analyses have suggested. It means that even limited cyber espionage, if detected, could prove highly escalatory.

## *Policy Implications*

In spite of the magnitude of the dangers, risk reduction is likely to prove extremely challenging. China, Russia, and the United States would be unlikely to agree to meaningful limits on nonnuclear capabilities designed to threaten potential adversaries' C3I assets because each state views such capabilities as critical for both conventional warfighting and deterrence. Moreover, each state is—or may become—resistant to disentangling its nuclear and nonnuclear forces and C3I assets. Russia's objection, according to Alexey Arbatov, is simply the financial costs of separation.[114] Some Chinese scholars, meanwhile, have argued that separating nuclear and nonnuclear forces and C3I assets could make U.S. attacks against Chinese nonnuclear capabilities less risky and hence more likely (even if these scholars also argue that China's adoption of dual-use capabilities was originally motivated by convenience and not strategy).[115] Indeed, the same logic may even end up holding sway in Washington. There is no evidence that the United States' use of dual-use C3I assets (or dual-use aircraft, for that matter) was motivated by anything other than convenience and cost. If, however, there was ever a serious discussion about

114. Alexey Arbatov, "Non-Nuclear Weapons and the Risk of Nuclear War: A Russian Perspective," discussion at the Carnegie Endowment for International Peace, Washington, D.C., November 29, 2017, http://carnegieendowment.org/2017/11/29/non-nuclear-weapons-and-risk-of-nuclear-war-russian-perspective-event-5762 (in particular, the comments at 38:44 of the recording).
115. Zhao and Li, "The Underappreciated Risks of Entanglement," p. 68.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

separating nuclear and nonnuclear C3I then it is not difficult to imagine advocacy for entanglement on deterrence grounds.

Yet, Beijing, Moscow, and Washington should still confront the question of whether the advantages of entanglement—both financial and strategic—are worth the escalation risks. After all, if the escalation risks are too great, then any benefits will be outweighed by an increase in the likelihood and probable costs of a war. If this article is correct—if the escalation risks are greater than widely realized and likely to increase further—then China, Russia, and the United States may already be on the wrong side of the line.

## UNDERSTANDING AND RAISING AWARNESS OF THE RISKS

A first-order task for Washington, Beijing, and Moscow, therefore, is to conduct their own analyses, most likely on a classified basis, of the potential benefits and risks of entanglement. These efforts should be informed by intelligence assessments about the extent to which potential adversaries' nuclear and nonnuclear forces and C3I assets are entangled, and about those rivals' perceptions of the intentions and capabilities of the state conducting the analysis. If such analyses concluded that the risks of entanglement did indeed outweigh the benefits, they could catalyze and inform the development of a risk-reduction strategy.

In principle, there are both unilateral and cooperative approaches to risk mitigation. Given the poor state of political relations between Washington and Beijing, and between Washington and Moscow, unilateral measures currently represent the only feasible starting point. Such measures certainly cannot eliminate the escalation risks of entanglement, but they could help to mitigate them and slow their rate of increase.

In this vein, the simplest risk-reduction measure would be to raise awareness, within governments and militaries, of the challenges created by entanglement for assessing an adversary's intent and, importantly, for the adversary in assessing the state's own intent. Given that crisis instability and misinterpreted warning are mediated by perceptions—or rather misperceptions—about the intent behind incidental strikes or threats, drawing the attention of decisionmakers to the difficulties of assessing intent might encourage restraint in a conflict and so help counteract inadvertent escalation pressures. Greater awareness of the risks could also catalyze peacetime preparations, such as enhancing the survivability of C3I assets, that might reduce the dangers associated with incidental strikes should a war occur. Such preparations might simultaneously mitigate the escalation risks resulting from the existence of

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

the damage-limitation window (which are not driven by misjudgments about intent).

To this end, China, Russia, and the United States could set up risk-reduction teams within their defense establishments.[116] Most important, during crises or conflicts, these teams could advise national and military leaders on the risks associated with entanglement and on ways to manage them. In peacetime, they could be tasked with ensuring that escalation risks were factored into both war planning and acquisition decisions for new strategic weapons and C3I capabilities (the teams could, for example, assess the different alternatives under consideration for their escalation implications, and be entitled to propose other options or object to the program entirely).

Ultimately, of course, high-level civilian or military leaders would be responsible for making decisions after considering escalation risks alongside more traditional strategic, military, and financial considerations. Risk-reduction teams, therefore, would have to be bureaucratically empowered (by being led by a suitably senior official, for example) to ensure their advice was heard. Such teams would also benefit by being made up from a broad range of experts, including civilian strategists, military planners, and intelligence officials with deep knowledge of potential adversaries' thinking.

In addition to their other tasks, risk-reduction teams could be tasked, in peacetime, with proposing unilateral risk-reduction measures. Changes to declaratory policy (which could be accomplished rapidly) and C3I system design (which could take years to implement) are examples of two different but complementary approaches.

### DECLARATORY POLICY

Declaratory policy is one tool for deterring incidental attacks on C3I assets by underscoring the risks. It is possible that the civilian officials or military officers responsible for authorizing such attacks might not appreciate the potential for their intentions to be misinterpreted. Such officials could hold very senior positions (kinetic ASAT attacks, in particular, might require authoriza-

116. James M. Acton, "Technology, Doctrine, and the Risk of Nuclear War," in Nina Tannenwald, Acton, and Jane Vaynman, *Meeting the Challenges of the New Nuclear Age: Emerging Risks and Declining Norms in the Age of Technological Innovation and Changing Nuclear Doctrines* (Cambridge, Mass.: American Academy of Arts and Sciences, 2018), pp. 54–55, https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/New-Nuclear-Age_Emerging-Risks/New-Nuclear-Age_Emerging-Risks.pdf. This idea was inspired by Posen, *Inadvertent Escalation*, pp. 212–218.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

tion from a head of state) and might not know that such assets were typically dual use; even if they did, they might not appreciate the implications.

The 2018 U.S. Nuclear Posture Review's threat to use nuclear weapons in response to attacks on nuclear C3I assets is presumably an attempt to warn potential adversaries about these implications. The disproportionate nature of this threat, however, risks its being dismissed by Beijing and Moscow as bluster. Instead, a somewhat vaguer formulation might ultimately prove more effective. For example, Washington could state that it considers dual-use communication and early-warning assets an integral part of its nuclear C3I system and would respond to attacks on them accordingly (Beijing and Moscow could make similar statements). As with all declaratory policy, such statements might influence potential adversaries' thinking more effectively if they were repeated periodically by very senior officials.

### TOWARD A MORE RESILIENT C3I ARCHITECTURE

Over the longer term, states could also develop C3I architectures that were both less likely to be subject to incidental attacks and more survivable if they were. Some analysts have suggested creating at least two separate C3I systems—one for nuclear or "strategic" operations and one (or more) for all other operations.[117] Even putting the costs of this idea aside, such disaggregation would reduce risks only if Washington, say, could convince Beijing and Moscow that it had separated nuclear and nonnuclear C3I functions, which would be no easy task. If the United States failed to do so, disaggregation could increase risks because the escalation consequences of China's or Russia's attacking C3I assets that were involved only in nuclear operations—out of the incorrect belief that they also enabled conventional operations—could be more severe than the consequences of attacking dual-use assets.

A somewhat different approach for early warning would be to create space-based capabilities that were less likely to be subject to incidental attack because they were incapable of contributing significantly to any mission other than detecting the launch of an adversary's missiles (whether nuclear or nonnuclear). In particular, as a matter of basic optics, physically small infrared

117. Elbridge Colby, "From Sanctuary to Battlefield: A Framework for a U.S. Defense and Deterrence Strategy for Space" (Washington, D.C.: Center for a New American Security, January 2016), p. 22, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Space-Report_16107.pdf; and Todd Harrison, "The Future of MILSATCOM" (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2013), pp. 40–42, http://csbaonline.org/uploads/documents/Future-of-MILSATCOM-web.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

detectors would be incapable of producing the kind of high-resolution imagery that would be most useful for cueing missile defenses and detecting the exact location of mobile missile launchers.[118] Because this limitation was the result of an observable and immutable property of the hardware, Washington, say, might be able to persuade Beijing and Moscow that it was real.

Another key advantage of small detectors is that they would not require their own satellite buses (which are generally very expensive to design and manufacture), but could instead be hosted by satellites used for other purposes. In this way, it might be possible to deploy them affordably in large numbers—tens, perhaps—creating a resilient architecture that would be the early-warning equivalent to AFSATCOM.[119] Although this author's judgment is that this kind of "dispersed" early-warning system would reduce the risks associated with incidental attacks, important challenges and trade-offs that deserve further study would arise.

For example, if the host satellites were attacked to undermine their primary function, their associated early-warning detectors would almost inevitably also be destroyed. To be sure, the likelihood of such attacks could be reduced by choosing host satellites that might not otherwise be targets (such as weather or commercial noncommunication satellites), and the consequences of such attacks would be mitigated by having multiple detectors in orbit. Nonetheless, a dispersed system could not eliminate the risks associated with incidental attacks.

Separately, deploying a dispersed system in addition to more capable dedicated early-warning satellites, such as SBIRS, might increase an adversary's incentives to attack the dedicated satellites (by reducing the escalation risks of doing so), and would be more expensive than fielding either system alone.[120] By contrast, deploying a dispersed system instead of dedicated satellites would lower the effectiveness of missile defenses.

Reducing an adversary's incentives to launch incidental attacks against space-based communication assets would be more difficult. Although a system that was capable of transmitting data only at low rates would be somewhat more useful for nuclear than nonnuclear operations, there would be no obvious way of demonstrating to adversaries that such a limitation was real

118. Eugene Hecht, *Optics*, 5th ed. (Boston: Pearson, 2017), p. 493.
119. Acton, "Command and Control in the Nuclear Posture Review."
120. If a dispersed system could be kept secret, its existence could not incentivize attacks against dedicated satellites. Under this approach, the United States would obviously not attempt to convince potential adversaries that the dispersed system was ineffective for any mission other than detecting missile launches.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

and permanent. Instead, risk-reduction efforts could focus on mitigating the consequences of incidental attacks against space-based communication assets by enhancing their resilience. One approach would be to create an upgraded version of AFSATCOM by hosting small communication transponders for nuclear operations on tens of satellites used for other purposes (though, again, trade-offs similar to those associated with a dispersed early-warning system would arise).

## *Conclusion*

As U.S.-Chinese and U.S.-Russian tensions have increased, albeit nonmonotonically, since the mid-2000s, warnings about the escalation risks that are inherent to the way that the United States would likely approach a great-power conflict have grown louder.[121] This focus on American doctrine and technology, however, has largely obscured another danger: the emerging Chinese and Russian ways of fighting wars are inherently escalatory too.

Both China and Russia, like the United States, seek to threaten potential adversaries' C3I assets and are improving their capabilities to do so. Because many enabling assets are dual use, however, attacks against them could, in the event of a conflict, degrade the target's nuclear C3I system just as a nuclear war was becoming all too imaginable. Crisis instability is one potential consequence. Indeed, its risks are more serious than generally understood because C3I assets that are space-based or distant from potential theaters of conflict could be subject to incidental kinetic attack or cyber interference. Additionally, C3I vulnerability could generate two other escalation pressures—misinterpreted warning and the damage-limitation window—that have not been previously discussed. Attacks against ISR assets, which would be likely in a major conflict, would exacerbate the risks by complicating the task of assessing an attacker's intent and by raising concerns about follow-on attacks against dual-use early-warning and communication assets.

In the future, the extent of entanglement—and hence the magnitude of these escalation risks—is likely to increase. Early-warning capabilities are likely to become more entangled with nonnuclear weapons as China and Russia modernize early-warning systems, and especially if one of them or the United States deploys nonnuclear SLBMs, ICBMs, or long-range hypersonic boost-

121. This literature has a broader focus than the vulnerability of nuclear forces and C3I assets. See, for example, Keir A. Lieber and Daryl G. Press, "The Nukes We Need: Preserving the American Deterrent," *Foreign Affairs*, Vol. 88, No. 6 (November/December 2009), p. 43.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

glide weapons, which could be monitored in flight with capabilities primarily designed to detect a nuclear strike. Other nuclear C3I capabilities could also become more deeply integrated into nonnuclear missions. Because dual-use weapon-delivery systems may become more common, for example, the overlap between nuclear and nonnuclear enabling capabilities (such as communication and mission planning systems) is also likely to increase.

Nonnuclear threats to dual-use C3I capabilities are also likely to become more serious. For example, as part of U.S. efforts to enable forces to "take advantage of freedom of action in one domain to . . . challenge an adversary in another," the United States could develop or enhance ASAT capabilities—including kinetic ones, perhaps—for targeting dual-use Chinese and Russian communication and ISR satellites.[122] Meanwhile, if Beijing or Moscow develops long-range nonnuclear hypersonic boost-glide weapons, it may be able to threaten the uplinks and downlinks for U.S. satellites across the world, including in the continental United States—potentially endangering the functionality of multiple dual-use U.S. C3I systems.

If these risks are to be ameliorated—or, at the very least, if their rate of increase is to be stemmed—China, Russia, and the United States will first have to conclude that the risks of entanglement outweigh the benefits. If one or more of them reaches that conclusion then, for the time being, unilateral risk-reduction measures (including the use of declaratory policy to underscore the risks of attacking dual-use C3I assets and the development of more resilient C3I systems) offer the most promising way forward. Establishing risk-reduction teams would help institutionalize and inform these efforts and, perhaps most importantly, raise awareness of the risks within governments and militaries, thus helping to mitigate them.

Over the longer term, cooperative risk-reduction measures could be adopted to further mitigate the risks, particularly the threat to dual-use C3I capabilities. Although there is little prospect of such measures being negotiated today, the level of interest in them could rise in the future—because of a thaw in political relations, perhaps, or a dangerous crisis that shocked political leaders into action. States could, for example, commit not to engage in cyber interference with one another's nuclear C3I systems.[123] They could also agree to prohibit

122. Air-Sea Battle Office, "Air-Sea Battle," 4. See also Biddle and Oelrich, "Future Warfare in the Western Pacific," pp. 44–45; and Christensen, "The Meaning of the Nuclear Evolution," p. 472.
123. Richard J. Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies" (Washington, D.C.: Center for a New American Security, July 2014), pp. 24–27, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Poisoned Fruit_Danzig.pdf.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024

the testing of ASAT weapons capable of threatening objects in geostationary orbit (where the most important space-based nuclear C3I assets are located).[124] Such prohibitions could prove effective if each participant assessed that the costs of violating the agreement—most obviously, the possibility that potential adversaries would engage in reciprocal violations—outweighed the disadvantages of compliance.

To make such prohibitions workable, significant technical challenges would need to be overcome. How would a prohibition against interfering with nuclear C3I systems be defined? What command-and-control systems would be covered given that so many of them are dual use? Similarly, what kind of weapons—precisely—would be included in a ban on testing ASAT weapons capable of reaching geostationary orbit? While challenging to answer, these questions are not necessarily unanswerable. In fact, the process of designing unilateral risk-reduction measures might stimulate and facilitate thinking about cooperative risk reduction by creating enhanced understanding of the risks associated with entanglement as well as the expertise to manage them. In this way, by embarking on unilateral risk-reduction processes now, China, Russia, and the United States could better position themselves to take advantage of any political opportunities for negotiations on cooperative measures that might arise in the future.

124. Arbatov, Dvorkin, and Topychkanov, "Entanglement as a New Security Threat," pp. 40–41.

Downloaded from http://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320 by guest on 28 March 2024