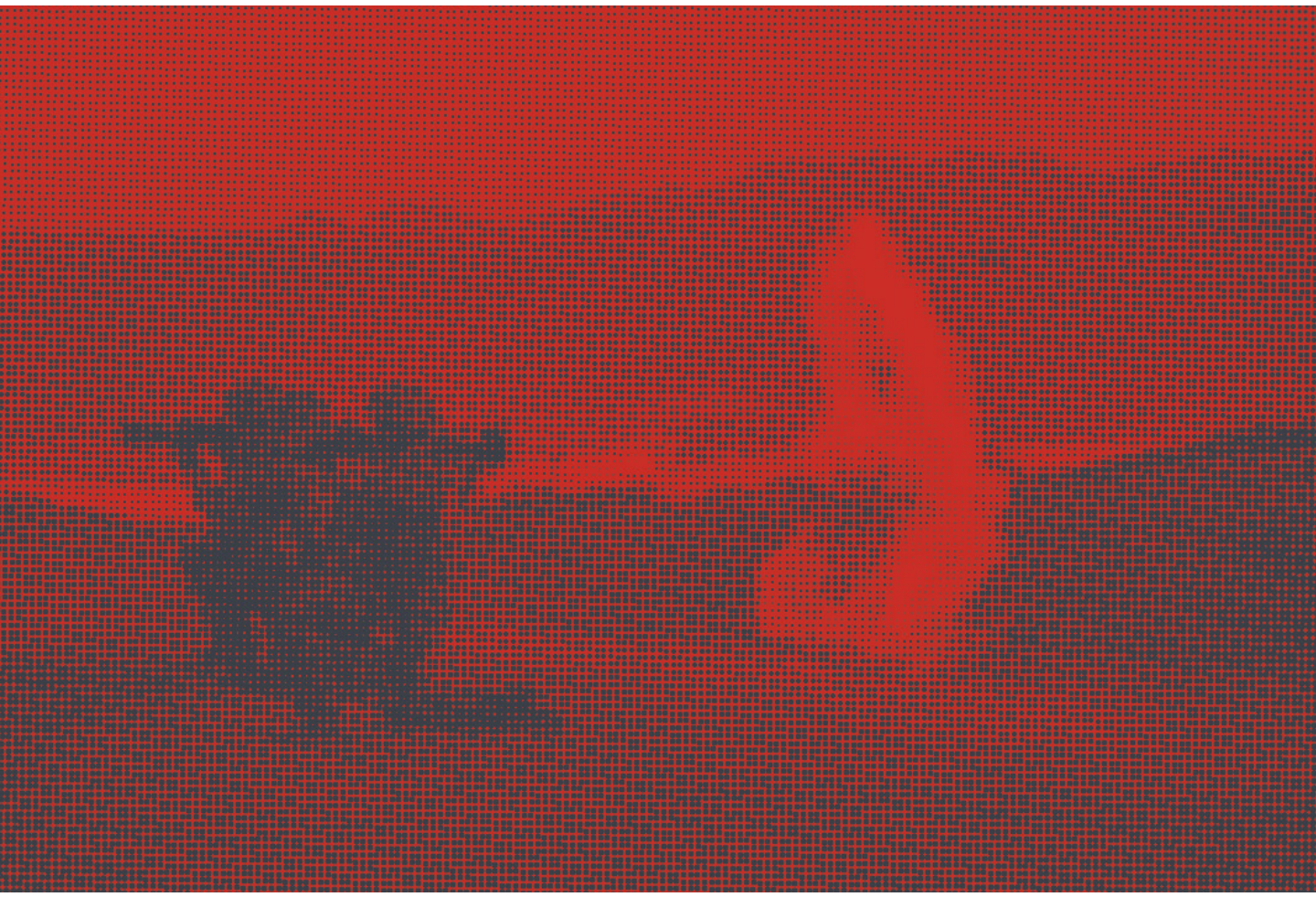
Texas National Security Review: Volume 3, Issue 3 (Autumn 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

WORMHOLE ESCALATION IN THE NEW NUCLEAR AGE

Rebecca Hersman



Increasingly capable and intrusive digital information technologies, advanced dual-use military capabilities, and diffused global power structures will reshape future crises and conflicts between nuclear-armed adversaries and challenge traditional ways of thinking about escalation and stability. This emerging security environment will require new concepts and tools to manage the risk of unintended escalation and reduce nuclear dangers.

On Oct. 24, 1962, the United States raised its alert levels to defense readiness condition (DEFCON) 2, for the first — and thus far only — time in its history. In a televised address, President John F. Kennedy made clear that any nuclear attack from Cuba would be construed as an act of war, and that the United States would retaliate in kind. Had these events taken place today, the signaling almost certainly wouldn't have stopped — or started — there. A chorus of pre-established online trolls messaging a Soviet-orchestrated storyline and all-caps Twitter threats would likely have come next. A targeted campaign to weaponize social media, turn elements of the American public against the president, and undermine the institutional authority and credibility of America's deterrent did not arise because the technology to do so in real time did not exist. Instead, Kennedy stood "eyeball to eyeball" with Soviet First Secretary Nikita Khrushchev during the 13-day standoff until cooler heads prevailed. Flash forward and today's global pandemic crisis offers a glimpse into how a toxic mix of disinformation, conspiracy theories, and digital technology can complicate effective crisis management, fuel competition and rivalry, shift blame, and sow mistrust.

Unlike traditional concepts of escalation, which suggest linear and somewhat predictable patterns from low-level crisis to all-out nuclear war,[1] escalatory pathways in this new era of strategic competition will be less predictable. Indeed, increasingly sophisticated sub-conventional tactics such as disinformation and weaponized social media, the blurring of nuclear-conventional firebreaks, and the continuing diffusion of global power to regional nuclear states are adding new challenges and additional complexity to crisis management even as an increasingly competitive and contested security environment fuels greater coercive risk-taking among nuclear-armed states, in particular, the United States, Russia, and China.

The increasing use of hybrid warfare and gray-zone tactics by China and Russia reflects the view that their strategic aims are best achieved through coercive means below the level of direct conventional military interaction. Of course, these countries are not strangers to information warfare, propaganda, and deception, or even using proxy and covert warfare as tools of strategic competition (nor is the United States). Cold War history is littered with such cases from election manipulation to state-sponored rebel insurgencies. Moreover, from the Color Revolutions to Stuxnet, U.S. government actions, both real and imagined, have fed perceptions of a United States bent on shrinking Russia's and China's spheres of influence and shaping regional balances of power on favorable terms. And yet, in the aftermath of the Soviet Union's collapse, America's conventional military primacy, its ability to utilize the institutions and alliances of the liberal international order to advance U.S. interests, and its domestic political commitments to a free press and open internet have limited both the need and ability of the United States to compete aggressively in the gray zone.[2] Both Russia and China, on the other hand, have felt compelled to challenge institutional structures and avoid direct traditional military competition, while pursuing asymmetric approaches to competition "below and beyond" traditional one-upmanship in the conventional military domain. Through broad, sub-conventional influence campaigns and the engagement of digital

1 Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).

2 Kathleen Hicks et al., "By Other Means Part I: Campaigning in the Gray Zone," *Center for Strategic and International Studies,* July 8, 2019, https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone.

proxies, these states hope to advance their interests without clear attribution or risk of escalation.

These strategies of strategic competition in the sub-conventional domain may not be entirely new, but the tools that enable them have transformed the strategic significance of the unconventional battlespace and the coercive power of hybrid warfare. Fueled by technological innovation — particularly in digital media-based technology as well as cyber operations, artificial intelligence (AI), and machine learning — today's competitive landscape is more complex and dynamic than before. The growing number of weapons in the sub-conventional arsenal include a range of kinetic and non-kinetic coercive tools, tactics, and strategies. The rise of the cyber domain; connectivity of global commerce, finance, and communications; speed and penetration of the internet; and prevalence and intimacy of social media that reaches nearly 40 percent of the world's population have reshaped the competitive domain now commonly called the "gray zone".[3] Today's proxies and surrogates look more like online trolls who wander freely inside one's digital homeland, enabled by advanced cyber and disinformation tools and weaponized social media, rather than armed guerillas fighting internal wars with black-market weaponry in distant territories. Moreover, these new forms of influence and information warfare are not the exclusive domain of great powers. Rather, the accessibility of information technology suggests a leveling of the playing field for great powers, non-state actors, states, and non-government entities alike.

This technological transformation is not limited to the sub-conventional domain. Advanced technology is also blurring the threshold between conventional and strategic conflict, including the increasing commingling of nuclear and conventional payloads on non-ballistic missile delivery systems such as hypersonic vehicles, long-range cruise missiles, or extended-range torpedoes, as well as ever more effective missile defenses. Similarly, conventional and strategic warning and surveillance assets and advanced command-and-control capabilities continue to be integrated in ways that potentially undermine escalatory firebreaks by creating new counterforce or precision strategic-strike opportunities and enhancing the potential efficacy of missile defenses. These developments may bolster incentives to move first and fast in a high-end conventional fight. As traditional firebreaks between conventional and nuclear warning and delivery systems erode and the strategic effects of cyber and space operations multiply, the ability to manage and maintain strategic stability grows more difficult.

Moreover, today's major powers do not have the playing field to themselves. The bipolarity that characterized strategic competition during the Cold War has disappeared and the U.S.-dominated unipolarity that characterized the immediate aftermath of the Soviet Union's collapse has largely dissipated. Instead, today's security environment is characterized by complex asymmetries, multi-domain conflict, and nine nuclear-armed states with widely divergent capabilities and intentions. Indeed, the rise of smaller nuclear powers has widened the nuclear shadow and its regional implications, particularly in areas where asymmetries in conventional capabilities and interests may create divergent beliefs about the utility of nuclear weapons in crisis bargaining scenarios.[4] In parallel, states can now draw upon a growing range of strategic options, including long-range nuclear weapons; advanced conventional munitions; and space, cyber, and information capabilities. In this more fragmented competitive environment, emerging technologies, especially in the digital information space, can level the playing field, providing smaller states virtual expeditionary forces with global reach.

Of course, sub-conventional tactics, including information warfare and the use of surrogates, figured prominently throughout the Cold War and the many crises and close calls that characterized the period. During this time, while full-scale war between the United States and the Soviet Union was averted, lower-level conflict was widespread. In 1965, Glenn Snyder first proposed the existence of a "stability-instability paradox" to explain why mutually deterred, nuclear-armed adversaries sometimes engage in extensive, seemingly unstable, conflict and competition even while preserving comparative stability at the strategic level.[5] As Robert Jervis later described it, "To the extent that the military balance is stable at the level of all-out nuclear war, it will become less stable at lower

3 J. Clement, "Number of Global Social Network Users 2010–2023," *Statista,* April 1, 2020, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

4 Christopher P. Twomey, "Asia's Complex Strategic Environment: Nuclear Multipolarity and Other Dangers," *Asia Policy 11,* no. 1 (2011): 51–78, https://doi.org/10.1353/asp.2011.0006.

5 Glenn H. Snyder, "The Balance of Power and the Balance of Terror," in *The Balance of Power,* ed. Paul Seabury (Scranton: Chandler, 1965), 185–201.

levels of violence."[6] In other words, strategic stability at the nuclear level could actually encourage or enable conflict at lower levels of the spectrum, especially through the use of surrogates or proxies. Seemingly, this allowed great powers not only to keep small wars and big wars separate, but also to engage in levels of sub-strategic conflict and competition even as the risks of nuclear war appeared to abate. Several behavioral rules seemed to help limit escalatory risks associated with this type of conflict, including not attacking the central territory of the adversary state, operating via surrogates and third parties where possible, and encouraging strategic transparency and crisis communications, especially following the Cuban Missile Crisis.

It is unclear if these same rules for strategic stability apply in today's environment. Gray-zone competitions can now be deeply intrusive: Using witting and unwitting proxies within enemy territory, these tactics can strike at the heart of a country's institutions, values, and populations well inside its digital homeland. Moreover, in this more fragmented, competitive landscape, the stabilizing of benefits of transparency and an assured second strike are unclear for countries with smaller arsenals and limited strategic geographic depth. Finally, while states continue to make use of proxies and surrogates, these digital soldiers may be both more intrusive and less controllable than those of the Cold War. This suggests the potential for a new nuclear paradox: As states drive to compete and win at the sub-conventional level — in the gray zone — the risk of strategic crisis may increase, even as the risk of conventional conflict between nuclear-armed states declines.

This new era of strategic competition will require renewed thinking about the tools and concepts of deterrence and escalation — adapting older ideas and developing new ones. Herman Kahn's 44-rung "escalation ladder," which describes a continuous, linear escalation path between low-level crisis and all-out strategic conflict, was built on potentially problematic expectations of proportionality and universally shared conceptions of deterrence. The blurring of conflict across sub-conventional, conventional, and strategic levels as well as the proliferation of actors across that landscape challenge this conceptualization of escalation and call into question its utility. Rather than progressing (more or less) stepwise, with clear thresholds between behavior that would elicit a conventional or nuclear response, crisis or conflict between nuclear-armed adversaries in this new environment is far more complex and unpredictable. And yet, even as academics and policymakers question the representative value of this conceptual ladder, the imagery has proven difficult to shake.

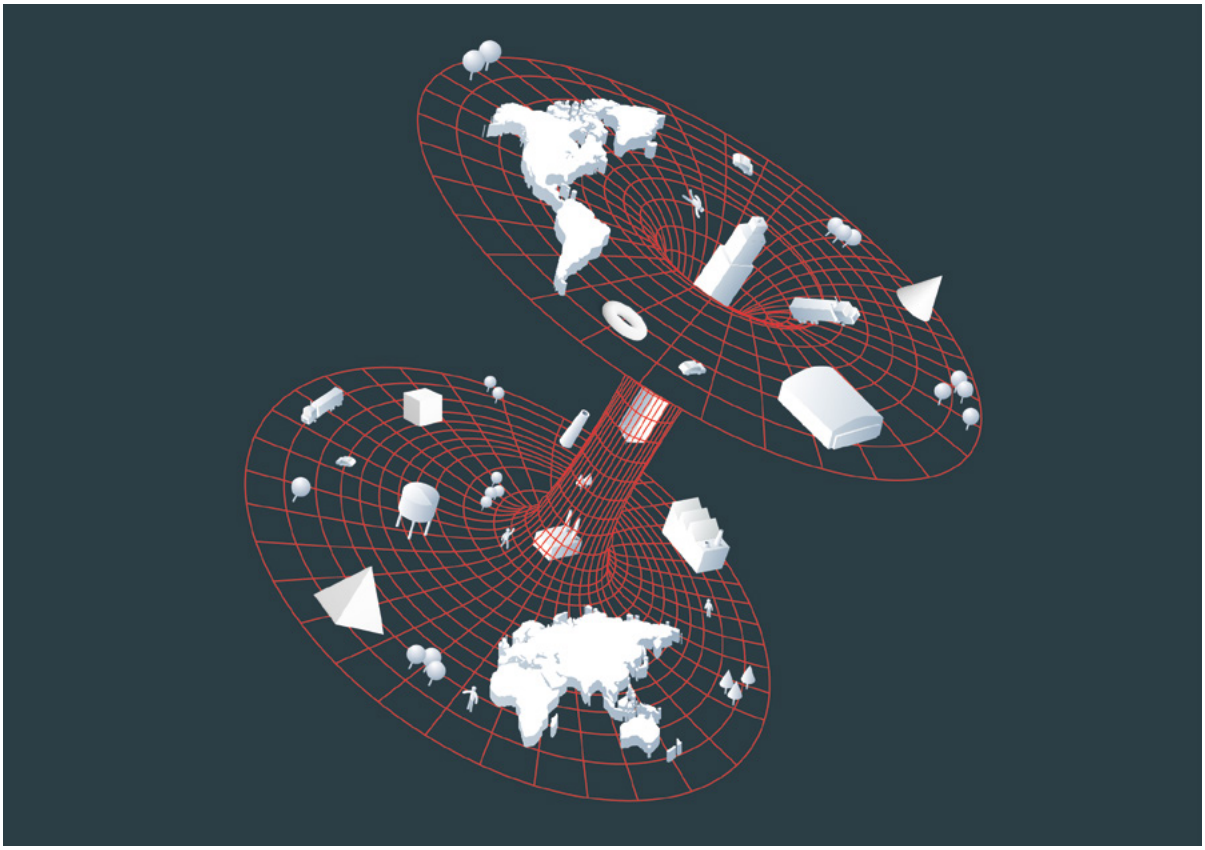
The challenges of managing conflict escalation in today's strategic environment call for a different metaphor. Drawing from science fiction and physics, the trends described above suggest that alternative and less predictable escalatory pathways are likely and that crisis escalation may instead follow a "wormhole" dynamic. Holes may suddenly open in the fabric of deterrence through which competing states could inadvertently enter and suddenly traverse between sub-conventional and strategic levels of conflict in accelerated and decidedly non-linear ways.[7]

The challenges of managing conflict escalation in today's strategic environment call for a different metaphor.

This article explores three ways in which these wormhole dynamics — fueled by the pursuit of asymmetric advantage, advanced technology, and the diffusion of global power — could unfold between nuclear-armed states. The first section explores the challenges that sub-conventional tactics pose to crisis stability, especially through complex influence campaigns including disinformation and weaponized social media. The second section outlines the unexpected escalatory potential of conflicts that take place along the conventional-nuclear interface where a breakdown of clear firebreaks between a range of technology-enabled strategic capabilities, including warning, surveillance, and communication systems, is blurring the lines be-

6 Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca, NY: Cornell University Press, 1984), 31. For an empirical test of the implications of the stability-instability paradox, see, Mark S. Bell and Nicholas L. Miller, "Questioning the Effect of Nuclear Weapons on Conflict," *Journal of Conflict Resolution* 59, no. 1 (2015): 74–92, https://doi.org/10.1177/0022002713499718.

7 First theorized in 1916 by Austrian physicist Ludwig Flamm and expanded upon by Albert Einstein and Nathan Rosen in 1935, wormhole theory proposes the presence of "bridges" or shortcuts connecting two widely separated regions of space-time.



tween conventional and strategic — including nuclear — domains. The third section examines how sudden, non-linear strategic crises could emerge in a multipolar world of regionally oriented nuclear weapons possessors. The final section discusses both the risks and opportunities these escalatory dynamics may portend for crisis management, arms control, and deterrence.

New Weapons, New War: Strategic Crisis in the Gray Zone

Today, both Russia and China increasingly rely on sub-conventional, non-military weapons as primary instruments of coercion. As explained by Dmitry Adamsky, "Uninterrupted informational deterrence ... augmented by nuclear signaling, and supplemented by the intrawar coercion constitutes an integrated cross-domain campaign" in Russian strategic thinking.[8] Hence, "cross-domain coercion" includes non-nuclear, informational, and nuclear influence, and succeeds when it dissuades the adversary from aggression or forces the other side to de-escalate. The weaponization of social media, enabled by advanced cyber and disinformation tools, ranks among the most effective of these new capabilities, particularly in its ability to achieve strategic effects at great distances and amid high levels of deniability. The United States should expect Russia's sub-conventional arsenal to be used broadly to neutralize its adversaries both before and during a crisis or conflict as part of its plan to contest and compete across the spectrum of conflict.[9] Take, for example, Russia's swift annexation of Crimea in 2014. In the months leading up to the forced and falsified referendum, Moscow targeted Russian-speaking Ukrainians through Russian-backed media and social media platforms. Through these platforms, Russian government-backed entities manipulated online videos and photos, symbolically drawing parallels to Kosovo, where the American-led NATO alliance took unilateral military action in 1999. The fabricated feed of disinformation targeting the minority Russian-speaking population was reinforced by coercive intimidation techniques employed by Russian special forces, fortifying the cross-domain coercion to achieve both military and non-military victory.

8 Dmitry "Dima" Adamsky, "Strategic Stability and Cross-Domain Coercion: The Russian Approach to Information (Cyber) Warfare," in *The End of Strategic Stability? Nuclear Weapons and the Challenge of Regional Rivalries*, ed. Lawrence Rubin and Adam N. Stulberg (Washington, DC: Georgetown University Press, n.d.), 164.

9 Adamsky, *The End of Strategic Stability?*, 154.

Nuclear powers can engage their competitors' core strategic interests directly, intrusively, and coercively (and perhaps unintentionally), well below traditional forms of armed conflict, especially through cyber, economic, and media-based attacks. It isn't clear that nuclear strategic stability, particularly in the form of a secure second-strike capability, sufficiently mitigates these risks. It may even provide false assurance. In fact, as a recent Center for Strategic and International Studies report points out, "U.S. success at deterrence by credible threat of escalation to military conflict has increased incentives for rivals to use gray zone tactics, which are attractive precisely because they make the risk of vertical escalation appear too great."[10] As cyber weapons and disinformation are deployed across the globe, states are adapting sub-conventional tactics in pursuit of their own strategies for escalation dominance — the ability to achieve strategic impact while limiting strategic risk.[11] The possibility of misperception associated with new non-nuclear capabilities is especially acute because there is no clear understanding between rivals regarding where these tactics fit in the escalation hierarchy.[12]

The "stability-instability" paradox would suggest that such sub-conventional or gray zone forms of competition can exist without risking strategic conflict as long as each country's second-strike capability remains secure and the risks of miscalculation remain checked. What if, however, sub-conventional tactics can achieve strategic-level effects? What if political decapitation can be achieved (or feared) through the weaponization of social media coupled with information-based cyber attacks? What if, by undermining and manipulating institutions of government and political leaders, states can use gray-zone tactics to divide publics from their leaders and institutions, foment internal conflict, and impede senior decision-making? Moreover, what if such actions were to take place, perhaps through advanced pre-deployment, during a crisis or conflict rather than during a period of relative peace?

Advances in digital technology, from deep fakes to AI-enabled social media campaigns, are transforming the speed and precision with which influence campaigns can reach and manipulate their desired targets. Adversaries can amplify effects, obscure attribution, and prime the information space to their advantage long before a crisis begins, as well as shape it during such a crisis. By promoting false narratives, flooding the information zone with conflicting data points, manipulating social and economic institutions, and instigating general or targeted social unrest, potential adversaries can break confidence in U.S. and allied institutions, increase distrust and confusion, and coerce desirable outcomes at lower levels of conflict. The dueling "false flag" narratives surrounding the origins of the COVID-19 pandemic involving the United States and China are worrying indicators of how such narratives can quickly move into the mainstream of political discourse, sow confusion about attribution, and disrupt confidence and transparency between the United States and potential great-power adversaries when they must engage in crisis communications.[13]

Through tactics ranging from election meddling[14] to the hacking of government personnel systems,[15] Russia and China have leveraged cyber attacks and disinformation campaigns to challenge the United States through nonmilitary means. Such approaches are even more aggressively employed to diminish the roles and influence of the United States and its allies in China and Russia's near abroad. And yet, these new, digital "proxy wars" do not take place on foreign shores nor beyond the public eye but rather deep inside the U.S. homeland.

Fake News Meets Deep Fakes

Disinformation and other sub-conventional tools that target public perception, institutional legitimacy, and leadership credibility can potentially trigger escalation to the strategic echelon of conflict. This could unfold in several ways. First, it's possible that disinformation could cause a "fake-out" in which

10 Kathleen Hicks et al., "By Other Means Part I," 27.

11 Kahn, *On Escalation*. Kahn introduced the concept of "escalation dominance" to describe one's ability to maintain superiority over an adversary at each of the 44 rungs along the metaphorical escalation ladder. In this way, a rival would always be disadvantaged by further escalation.

12 Michael Fitzsimmons, "The False Allure of Escalation Dominance," *War on the Rocks*, Nov. 16, 2017, https://warontherocks.com/2017/11/false-allure-escalation-dominance/.

13 For additional context on COVID-19 "false-flag" disinformation, see, Philip Ball and Amy Maxmen, "The Epic Battle Against Coronavirus Misinformation and Conspiracy Theories," *Nature*, May 27, 2020, https://www.nature.com/articles/d41586-020-01452-z; Renée DiResta, "For China, the 'USA Virus' Is a Geopolitical Ploy," *The Atlantic*, April 11, 2020, https://www.theatlantic.com/ideas/archive/2020/04/chinas-covid-19-conspiracy-theories/609772/; Max Fisher, "Why Coronavirus Conspiracy Theories Flourish. And Why It Matters," *New York Times*, April 8, 2020, https://www.nytimes.com/2020/04/08/world/europe/coronavirus-conspiracy-theories.html.

14 Philip Bump, "Here's the Public Evidence that Supports the Idea that Russia Interfered in the 2016 Election," *Washington Post*, July 6, 2017, https://www.washingtonpost.com/news/politics/wp/2017/07/06/heres-the-public-evidence-that-supports-the-idea-that-russia-interfered-in-the-2016-election/.

15 Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," *Washington Post*, June 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

false information proves so compelling that leaders advocate for, or even take, hasty action before the falsehood is revealed. While by no means the only manifestation of this phenomenan, deep-fake technology — machine-learning techniques and programs that manipulate and distort audio and video to create realistic forgeries — presents a new and particularly vexing tool for cross domain coercion. In September 2018, three members of Congress expressed concern in a letter to Daniel Coats, the then-director of national intelligence, regarding the threat that deep-fake technology poses to America's national security.[16] Today, the United States and its allies must anticipate a world in which more sophisticated deep fakes could be employed strategically by adversaries during momentous events, such as elections, civil unrest, or even acts of terrorism or cyber attacks, to influence and manipulate public perception in a way that promotes an adversary's preferred outcome.

As deep-fake capabilities become more readily available and realistic, they will become more prevalent as a tactic to circumvent traditional war-fighting strategies, disrupt and delay adversary responses, and weaken adversary resolve. The utility of deep-fake techniques is not confined to one geographic region or a single adversary and will most certainly become an attractive tactic to gain an asymmetric advantage by state and non-state actors alike. Deep fakes could also be used to decouple military alliances by eroding political and public support and driving wedges between critical partners. For example, the *Military Times* reported last year that during a NATO training exercise in the Baltics, a deep fake was deployed after American Stryker vehicles collided on a road in Lithuania. The deep fake image suggested that the Americans had killed a local Lithuanian child in the collision. During a 2018 meeting with NATO officials, Lithuanian Defense Minister Raimundas Karoblis said of the fabricated event, "We have no doubt that this was a deliberate and coordinated attempt aiming to raise general society's condemnation to our allies, as well as discredit the exercises and our joint efforts on defense strengthening."[17] In effect, then, deep fakes could give rise to a "deception revolution," where elements of the public, deceived by a disinformation campaign, become unwitting soldiers on behalf of an adversary.[18]

Walking Through the Front Door

Adversaries could also use disinformation tactics to prompt a leader to take action prematurely or, alternatively, to resist a necessary response, despite knowing certain details to be false or incomplete, as a result of increasing domestic political pressure and perceptions of political weakness. The current interactions between disinformation and domestic politics surrounding the wearing of face masks and maintaining social distance in response to the coronavirus pandemic are suggestive of this dynamic.[19] In a nuclear crisis, in which government decision-making would be far less transparent and decentralized, vulnerability to such pressures could be exacerbated by the very systems designed to protect sensitive information and preserve secrecy. For example, the architecture, procedures, and policies on which America's current nuclear command, control and communications (NC3) system depends, which were first developed during the Cold War, were optimized for security, speed, and secrecy — not public scrutiny. Public confidence in the system was assumed as U.S. citizens and their congressional

The luxury of truly private, secret, and controlled decision-making will likely not be available to future presidents, especially when the adversary holds the keys to the timing and validity of who knows what and when.

16 Adam B. Schiff, Stephanie Murphy, and Carlos Curbelo, "Letter to the Honorable Daniel R. Coats, Director of National Intelligence," Office of Congressman Adam Schiff, Sept. 13, 2018, https://schiff.house.gov/imo/media/doc/2018-09%20ODNI%20Deep%20Fakes%20letter.pdf.

17 Kyle Rempfer, "Ever Heard of 'Deep Fake' Technology? The Phony Audio and Video Tech Could Be Used to Blackmail U.S. Troops," *Military Times*, July 19, 2018, https://www.militarytimes.com/news/your-air-force/2018/07/19/ever-heard-of-deep-fake-technology-the-phony-audio-and-video-tech-could-be-used-to-blackmail-us-troops/.

18 Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail," *Foreign Affairs* 98, no. 3 (May/June 2019), https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

19 Cat Zakrweksi, "The Technology 202: Mask Scams and Misinformation Still Present on Social Media despite Tougher Policies," *Washington Post*, April 1, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/04/01/the-technology-202-mask-scams-and-misinformation-still-present-on-social-media-despite-tougher-policies/5e8378ee88e0fa101a75708f/; Nick Timiraos, "U.S. Officials Press President Trump to Wear Mask in Coronavirus Fight," *Wall Street Journal*, June 28, 2020, https://www.wsj.com/articles/u-s-officials-press-president-trump-to-wear-mask-in-coronavirus-fight-11593369136; "Coronavirus Myths, Rumors and Misinformation," *Johns Hopkins Medicine*, June 30, 2020, https://www.hopkinsmedicine.org/coronavirus/articles/coronavirus-myths-rumors-misinformation.html.

representatives largely deferred to presidential authority in this domain and entrusted the military with wide-ranging responsibilities of execution and communication. Traditionally, the public has had little authoritative, fact-based information about many essential aspects of highly classified nuclear decision-making processes and the technical systems and organizations that support it. That very opacity, however, can in turn elevate the risks disinformation could pose before and during a crisis in ways that could seriously harm the legitimacy of, and confidence in, the NC3 system, especially in a crisis of longer duration in which the opportunity for greater public scrutiny and skepticism emerges.

Direct, back-door cyber attacks designed to disable or disrupt nuclear command-and-control systems and capabilities have long been of concern because of their escalatory potential. However, less focus has been dedicated to "front-door" attacks on institutions and decision-makers that depend on the system — attacks conducted through the weaponization of social media and the manipulation of information. Disinformation campaigns by adversaries who seek to sow public distrust in the command and control system itself can focus on softer targets accessible through less well-defended networks to erode confidence in systems and architectures without targeting or disabling those systems directly. The nuclear command-and-control system provides the means by which the U.S. president can authorize the use of nuclear weapons in a crisis or conflict, as well as the means to prevent unauthorized or accidental use of such weapons. The manipulation of social media could exacerbate a crisis by casting doubt on the credibility of decision-makers and reliability of these processes as publics latch on to information spread maliciously by adversaries.

Disinformation campaigns employed in conjunction with other political or military actions can seek to distract decision-makers and slow their response time enough to confer a tactical or operational advantage during a crisis. The United States needs to think more about how to maintain situational awareness across the information ecosystem in a crisis to sustain the legitimacy and reliability of its NC3 systems and protect presidential decision-making in the event of such tactics. Secrecy and opacity, while helpful in countering some threats to the NC3 system, offer little protection to disinformation campaigns since these attacks need not penetrate the NC3 system directly to be disruptive. Amplification of adversary messaging through conspiracy theorists and automated bots as well as the strategic use of deep fakes are just a few examples of how the new age of information warfare could disrupt secure and reliable presidential decisionmaking simply by moving so much of the policy discourse outside of that closed and secretive system. The luxury of truly private, secret, and controlled decision-making will likely not be available to future presidents, especially when the adversary holds the keys to the timing and validity of who knows what and when.

Flood the Zone

Disinformation could create confusion and delay among decision-makers by flooding the information zone and causing informational paralysis as information management systems, and the policymakers who rely on them, struggle to distinguish fact from fiction within a loud and crowded information environment. Some have alleged the United States, for example, developed tactics during the Cold War toward these ends, planning to utilize computer-simulated voices to mimic authentic orders and deceive Soviet personnel with false commands during a crisis or conflict.[20] In the context of strategic stability, this changes the calculus for escalation, especially among modern democracies, where leaders have more to prove if they lack the confidence of their citizenry. Because disinformation is compounded over time, its net effect on crisis stability may only be realized after it's too late to roll back the damage. It is also possible that disinformation could delay or even prevent attribution and accountability, including retaliation, by impeding investigations and undermining decision-makers and institutions.

Following the 2018 assassination attempt on Sergei Skripal and his daughter using an advanced chemical weapon agent in the United Kingdom, a King's College London study found that 138 contradictory narratives were spread through Russian broadcast media sources *RT* and *Sputnik* in the four weeks following the attack.[21] Recent reports indicate this operation and others throughout Europe were likely executed by a specialized Russian intelligence unit in an ongoing and coordinated

20 Benjamin B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps," *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (September 2014): 431–64, https://doi.org/10.1080/08850607.2014.900290.

21 Gordon Ramsay and Sam Robertshaw, *Weaponising News: RT, Sputnik and Targeted Disinformation* (London: King›s College London, 2019), 6, https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

campaign to destabilize Europe.[22] Though immediately following the attack the United Kingdom launched a fairly successful counter-disinformation campaign, the broader information war associated with this crisis has proven quite enduring, particularly in terms of raising doubts among citizens of the United Kingdom, as well as the European Union, about their own intelligence agencies and other sources of official or authoritative information. Initially, the United Kingdom was able to rally strong international support behind its response to the attack: Several Western countries expelled a total of over 150 Russian diplomats in a sign of solidarity and imposed punishing economic sanctions on Russia.[23] Nonetheless, a "coalition of the unwilling" emerged, comprised of several E.U. states that were reluctant to expel Russian diplomats or to otherwise criticize Russia too harshly for the brazen attack.[24] With a less vigilant counter-disinformation strategy, the outcome could easily have tilted the other way.

This incident demonstrates how contradictory stories and disinformation have the potential to slow response time and alter the way actors perceive risk. While the United Kingdom gained important experience countering Russian disinformation, Moscow appears to have learned from the incident as well, continuing to adapt and evolve its information and influence campaigns in ways that promote and amplify internal anti-government voices, including supposed independent, authoritative, online activist sources.[25] In the future, advances in quantum computing and and AI-enabled digital technology will allow states to flood the zone during a future crisis with even greater effectiveness. For example, the creation and dissemination of computational propaganda — human- and automation-driven disinformation distributed through social media[26] — may make it easier to bypass online encryption algorithms and access or tamper with sensitive data. This would allow malign actors to change content after it is published and plant false narratives in articles from otherwise trustworthy news sources, which would hinder crisis communication and make it even more difficult to separate truth from fiction during a crisis.

Technology Trojans and Unwitting Allies

Finally, a state or non-state actor could use targeted influence campaigns to enlist elements of an adversary's population to defy or protest their own government and institutions in highly disruptive ways. Such information warfare could be deployed in anticipation of a crisis or attack in order to amplify its impact and impede effective governmental responses. This would allow an actor to shape the information environment early, perhaps even before the receiving nation perceives an attack is underway, sow division, erode public confidence, and delay effective responses. These invisible, virtual "sleeper cells" can be awakened with a keystroke — think "Trojan horse" meets "flash mob."

The India-Pakistan crisis in February 2019, which culminated with widespread disinformation and highly escalatory rhetoric on both sides demonstrates the potential "out of control" nature of sub-conventional information warfare. In the immediate aftermath of the terror attack in India's Jammu and Kashmir state that killed 40 Indian paramilitary members, an aggressive disinformation campaign was launched to link the incident to India's upcoming parliamentary elections.[27] Notably, disinformation spread via WhatsApp that claimed that a leader of the Indian National Congress party, the opposition party, had offered a bribe to the suicide bomber's family.[28] Additional narratives were also disseminated, many of which portrayed

22 Michael Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say," *New York Times*, Oct. 8, 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html.

23 Katie Rogers and Eileen Sullivan, "Trump and Western Allies Expel Scores of Russians in Sweeping Rebuke Over U.K. Poisoning," *New York Times*, March 26, 2018, https://www.nytimes.com/2018/03/26/world/europe/trump-russia-diplomats-expulsion.html.

24 Julia Borger, Patrick Wintour, and Heather Stewart, "Western Allies Expel Scores of Russian Diplomats Over Skripal Attack," *The Guardian*, March 27, 2018, https://www.theguardian.com/uk-news/2018/mar/26/four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack.

25 Kate Starbird, "Information Operations and Online Activism Within NATO Discourse," in *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*, ed. Harold A. Trinkunas, Herbert S. Lin, and Benjamin Loehrke (Stanford, CA: Hoover Institution Press, 2020).

26 Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," University of Oxford, Project on Computational Propaganda, Working Paper no. 2017.11, 2017, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

27 Neha Thirani Bagri, "Back Story: When India and Pakistan Clashed, Fake News Won," *Los Angeles Times*, March 15, 2019, https://www.latimes.com/world/la-fg-india-pakistan-fake-news-20190315-story.html; "India, Pakistan and the Pulwama Crisis," Congressional Research Service, Feb. 26, 2019, https://fas.org/sgp/crs/row/IN11057.pdf.

28 Snigdha Poonam and Samarth Bansal, "Misinformation Is Endangering India's Election," *The Atlantic*, April 1, 2019, https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/.

the opposition party as "being soft on militancy"[29] in Kashmir. Because Indian Prime Minister Narendra Modi's Bharatiya Janata Party had 1.2 million volunteers operating the party's social media campaign for the elections, misinformation and false narratives about the escalating crisis with Pakistan spread rampantly. In the days following the attack in Kashmir, Facebook removed hundreds of fake accounts linked to Indian political parties and Pakistan's military. Yet, this disinformation campaign ultimately reached over 2.8 million Facebook users.[30] What was once intended to influence domestic politics to bolster support for the Bharatiya Janata Party seemed to spiral out of control even as both countries came to the brink of a broader military conflict.

Ultimately, misinformation and disinformation brought the most basic facts of the crisis into dispute. On February 26, the Indian Air Force (IAF) launched airstrikes against targets it said were terrorist bases in Balakot, Pakistan. In retaliation, Pakistan sent fighter planes over the Line of Control to bomb Indian administered Kashmir. During the resulting firefight, Pakistan shot down an Indian MiG-21 fighter jet and captured its pilot.[31] Subsequently, India claimed that the IAF pilot shot down one of Pakistan's F-16 fighter planes before his jet was downed. In an April 2019 *Foreign Policy* article, two U.S. defense officials stated that the United States had counted Pakistan's F-16s and found none missing.[32] The next day, Indian press refuted the U.S. report in *The Wire*, saying that radio signature confirmed the downed aircraft.[33] Such an incident should have been easy to fact check, but instead the episode remains in truth limbo. This contradiction of facts in the F-16 case represents a wider rift in U.S.-India reporting of the incident, and possibly an information vulnerability that Pakistan could capitalize on in the future. In a *Washington Post* article, South Asia experts Sameer Lalwani and Emily Tallo stated, "This [incident] will no doubt raise questions both inside and outside of India about the [Indian Air Forces's] conventional advantage if it is unable to punish a weaker adversary to reestablish deterrence."[34]

This crisis also raised troubling questions about the informational basis on which strategic stability rests. By creating and propagating their own alternative, and even incompatible, perceptions of victory, can states secure the benefits of de-escalation while forgoing the political costs of military defeat? This appears to have been the outcome of the 2019 Pulwama crisis, and yet this would seem to be a shaky foundation for sustaining strategic stability between nuclear-armed adversaries. Rather, in stability terms, such a "victory" may simply be borrowed time — a house of cards ready to collapse even more precipitously with the next crisis. Moreover, this dynamic suggests that information and influence campaigns can take on a highly competitive dynamic with each subsequent crisis raising the information escalation threshold — a form of "disinformation racing." How India or Pakistan, or even China, might seek to use this chaotic stream of disinformation and its escalatory effect to its advantage in the future merits closer examination, as does the vulnerability of the United States to similar dynamics and pressures, especially when employed against partners and allies as a decoupling strategy.

Driving Strategic Risks in the Gray Zone

Moving forward, emerging technologies will exacerbate these challenges and risks. Technologically advanced influence operations can use AI to precisely and efficiently target vulnerable individuals and communities with tailored messages and influence strategies, while also enhancing the speed and responsiveness of messages focused on the broader public. AI algorithms can enable microtargeting using social media to specifically influence local communities regarding sensitive facilities, military communities, or individuals predisposed to — or particularly receptive to — influence, all with the intention of disrupting the government's ability to defend, and protect its institutions and manage crises. Such influence tactics need not be limited to disinformation — groups and individuals are also

29 Poonam and Bansal, "Misinformation Is Endangering India's Election."

30 Shashank Bengali and Aoun Sahi, "Facebook Removes Fake Accounts Tied to Indian Political Parties, Pakistan's Military," *Los Angeles Times*, April 1, 2019, https://www.latimes.com/world/la-fg-facebook-india-pakistan-20190401-story.html

31 Sameer Lalwani and Emily Tallo, "Did India shoot down a Pakistani F-16 in February? This just became a big deal," *Washington Post*, April 17, 2019, https://www.washingtonpost.com/politics/2019/04/17/did-india-shoot-down-pakistani-f-back-february-this-just-became-big-deal/?noredirect=on&utm_term=.062d844de7c3

32 Lara Seligman, "Did India Shoot Down a Pakistani Jet? U.S. Count Says No," *Foreign Policy*, April 4, 2019, https://foreignpolicy.com/2019/04/04/did-india-shoot-down-a-pakistani-jet-u-s-count-says-no/.

33 "IAF Refutes U.S. Report on Pakistan's F-16 Jets, Says Radio Signature Confirms Downed Aircraft," *The Wire*, April 5, 2019, https://thewire.in/security/india-pakistan-f-16-balakot.

34 Sameer Lalwani and Emily Tallo, "Did India Shoot Down a Pakistani F-16 in February? This Just Became a Big Deal," *Washington Post*, April 17, 2019, https://www.washingtonpost.com/politics/2019/04/17/did-india-shoot-down-pakistani-f-back-february-this-just-became-big-deal/?noredirect=on&utm_term=.062d844de7c3.

highly vulnerable to ransomware, encrypted bribes, doxing, and other techniques. In addition, various Trojan horse methods can allow Russia and China to use cyber-networked influence operations to make Russian or Chinese efforts look homegrown and complicate attribution, especially through the use of digital "sleeper cells" that can lie dormant until awakened during a crisis.

Once unleashed, information warfare is not easily stopped. Governments — or their bots — may start the war, but the effective weaponization of information, especially through social media, depends upon surrogates — witting or unwitting — who amplify messages, lend credibility within their media circles, and increase the originating state's ability to deny responsibility. Yet, many of those surrogates, including the conspiracy theorists and online trolls who fuel today's information wars, often behave according to their own pathologies and may have little awareness or regard for the interests of the originating state. Instead, they further proliferate and distort false or harmful information in pursuit of their own interests or conspriratorial proclivities.

In 2018, an MIT study examined a data set of rumor cascades (the spreading pattern of a statement or story) on Twitter from 2006 to 2017.[35] The research found that new social technologies increase the rate at which information sharing occurs and that falsehoods travel exponentially faster than truths. According to the study, "whereas the truth rarely diffused to more than 1000 people, the top 1% of false-news stories routinely diffused to between 1000 and 100,000 people."[36] In fact, the research concluded that "falsehoods were 70% more likely to be retweeted than the truth … even when controlling for the account age, activity level, and number of followers of the original tweeter, as well as whether the original tweeter was a verified user."[37] Even when falsehoods are exposed, fact-checking efforts may come too late and have less reach. For example, a self-described cardiologist named Thomas Binder claimed in April 2018 that a photo of two child victims of a Syrian gas attack was faked. His purported medical expertise made his assertion about the victims seem more credible and online activists quickly picked up the tweet and amplified it. While his original false tweet received 12,569 retweets in less than one week, his reluctant correction and admission of wrongly assessing the condition of the victims just two days later was only retweeted 43 times.[38] Disinformation that provides a constant barrage of false information is often durable and leads to long-term "truth decay," characterized by the blurring of the line between opinion and fact and the declining trust in formerly respected sources of information.[39]

Most recently, the COVID-19 pandemic has highlighted the speed at which falsehoods can spread and the power of mis- and disinformation to sow public apprehension and mistrust of the government in the midst of a crisis. Perhaps the most vivid recent example is the falsehood-ridden, conspiracy-theorist "documentary" *Plandemic* — a 26-minute online video which mainstreamed a number of hoaxes and lies about the novel coronavirus. In this case, QAnon conspiracy theorists, anti-vaxxers, and a handful of supposedly reputable "experts" who offered validation and amplification of false narratives helped the video get more than 8 million views within a week of its internet release and before mainstream platforms attempted to contain and discredit its malicious content.[40] Now, imagine a future crisis with a determined and technologically savvy adversary who seeks to force a coercive outcome while avoiding attribution, maintaining deniability, and without having to fire a single conventional shot. Unfortunately, in such a scenario, "wormhole" escalation dynamics may not be confined to science fiction.

Eroding the Conventional-Nuclear Firebreak

Wormhole escalation risks, however, are not confined to the gray zone. They can also exist along the increasingly complex interface between conventional and strategic levels of conflict. For much of the nuclear age, the concepts and tools

35 Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

36 Vosoughi, Roy, and Aral, "The Spread of True and False News Online," 1158.

37 Vosoughi, Roy, and Aral, "The Spread of True and False News Online," 1159.

38 Caroline Orr, "Arc Digital," *Arc Digital* (Medium, May 28, 2018), https://arcdigital.media/how-one-doctors-false-claim-was-used-to-erase-atrocities-in-syria-d76459ffa4e2.

39 Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life* (Washington, DC: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2314.html.

40 Sheera Frenkel, Ben Decker, and Davey Alba, "How the 'Plandemic' Movie and Its Falshoods Spread Widely Online," *New York Times*, May 20, 2020, https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html; Craig Silverman, "The Information Apocalypse Is Already Here, and Reality Is Losing," *BuzzFeed News*, May 22, 2020, https://www.buzzfeednews.com/article/craigsilverman/coronavirus-information-apocalypse.

Today, the distinctions between the upper echelons of conflict have become blurry as states rely more and more on non-nuclear capabilities to achieve strategic ends.

of strategic warfare — nuclear weapons systems and the systems that supported nuclear command, control, and warning — and those of the conventional battlefield were distinct and highly compartmentalized. The separation between the systems that were used for nuclear and conventional warfighting reduced the possibility that inadvertent escalation would occur. This compartmentalization helped create a firebreak — a barrier designed to slow or prevent accidental or automatic escalation to nuclear conflict in a conventional crisis.

Today, the distinctions between the upper echelons of conflict have become blurry as states rely more and more on non-nuclear capabilities to achieve strategic ends. On the one hand, cyber- and space-based threats are ever more capable of achieving strategic effects, raising concerns about the role of nuclear weapons in deterring their use. At the same time, most nuclear-armed states are expanding advanced dual-use (nuclear and conventional) delivery systems and integrating many of their early warning, command-and-control, and surveillance capabilities across conventional and nuclear missions. For example, all U.S., Chinese, Russian, Indian, and Pakistani nuclear-capable aircraft also support conventional systems, and Russia deploys dual-use, ground-launched cruise missiles. Both India and Pakistan have multiple types of ground-launched missiles suspected to be dual-use, and China's DF-26 intermediate-range ballistic missile can carry conventional and nuclear payloads.[41] In addition, advanced technologies, such as remote sensing, AI, and hypersonic delivery systems are accelerating the precision, lethality, and survivability of conventional tools of warfare in ways that will challenge traditional notions of stability and potentially open new avenues for escalation to strategic crisis in cases where vertical and horizontal escalation converge — all with wormhole effects.

Most research to date on entanglement — the commingling of conventional and nuclear forces — has focused on dual-use delivery systems capable of carrying both conventional and nuclear payloads, the integration of nuclear and conventional support structures such as command and control, and non-nuclear threats to nuclear weapons systems.[42] Far less work has been done on the informational aspects of conventional-nuclear entanglement and the implications for unexpected escalatory effects, especially with regard to situational awareness, surveillance, and warning capabilities.[43]

For most of the nuclear age, the ability to characterize the operating environment, detect nuclear and conventional strategic attacks, and discern real attacks from false alarms has been viewed as a benefit to crisis stability. In conventional conflicts with non-nuclear adversaries, information dominance, much like air superiority, has been a fundamental component of precision warfare and a central feature of American conventional military superiority in the post-Cold War period. Throughout this period, the United States has enjoyed the benefits of information dominance and the asymmetric advantage it offered. In fact, information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage.[44] Similarly, at the nuclear level, by improving the accuracy and timeliness of warning, improving overall visibility and clarity on adversary actions, and increasing decision time, enhanced situational awareness and strategic warning seemed to reduce the risk of nuclear miscalculation and the use-it-or-lose-it pressures that could incentivize a nuclear first strike.

In addition, the clear line between warning systems used for conventional and nuclear missions also meant that these assets were secure and compartmentalized. The systems that provided this strategic warning operated at long range, from outside adversary territories, and generally in ways that were not visible or particularly concerning to an adversary because they offered little in terms

41 James M. Acton, "Is It a Nuke? Pre-Launch Ambiguity and Inadvertent Escalation," Carnegie Endowment for International Peace, April 9, 2020, https://carnegieendowment.org/2020/04/09/is-it-nuke-pre-launch-ambiguity-and-inadvertent-escalation-pub-81446.; Hans M. Kristensen, Robert S. Norris, and Julia Diamond, "Pakistani Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74, no. 5 (Aug. 31, 2018): 355, https://doi.org/10.1080/00963402.2018.1507796; Hans M. Kristensen and Matt Korda, "Indian Nuclear Forces, 2018," *Bulletin of the Atomic Scientists* 74, no. 6 (2018): 363, https://doi.org/10.1080/00963402.2018.1533162.

42 James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99, https://doi.org/10.1162/isec_a_00320; Acton, "Is It a Nuke?"

43 One recent contribution on this topic came from the Project on Nuclear Issues at the Center for Strategic and International Studies. Rebecca Hersman et al., "Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking," Center for Strategic and International Studies, March 18, 2020, https://ontheradar.csis.org/analysis/final-report/.

44 John A. S. Ardis and Shima D. Keene, "Maintaining Information Dominance in Complex Environments," U.S. Army War College, Strategic Studies Institute, October 2018, https://publications.armywarcollege.edu/pubs/3658.pdf

of first-strike advantage.[45] Operating in space or remote geographic locations, nuclear warning, command, and control systems were traditionally difficult to target kinetically and contained substantial redundancies designed to ensure their survivability in the event of a nuclear attack. Moreover, countries had limited incentives to target strategic warning and situational awareness systems in a conventional conflict, as doing so would not limit an adversary's ability to conduct conventional operations and would unambiguously signal the advent of a nuclear attack.

Today, the capabilities designed to provide situational awareness and support senior decision-makers in crises and conflicts tend to be consolidated into a single conventional-nuclear ecosystem. Convenience, reduced costs, and flexibility are motivating decision-makers to rely more and more on strategic tools such as early-warning and communications systems for conventional operations — tools traditionally reserved for nuclear command and control. While attacks on, or intrusive surveillance of, these assets were considered highly escalatory and off-limits during conventional conflicts of the past, their dual-use nature today means adversaries may have difficulty discerning U.S. intent during a crisis. As a recent Center for Strategic and International Studies report suggests, this consolidation could force decision-makers in the future to weigh the benefits of rapid, decisive military victory afforded by information dominance against the high-stakes risks of nuclear escalation.[46]

Whereas the traditional command, control, surveillance, and warning systems focused either on nuclear warning (nuclear strategic situational awareness systems) or on providing intelligence to commanders about the conventional battlefield (conventional strategic situational awareness systems), today dual-use strategic situational awareness capabilities may be tasked to conduct both missions. Moreover, the combination of new enabling capabilities — such as advanced sensor technologies and the platforms for their deployment, high-bandwidth networks, and AI tools — are expanding the field of view at the conventional and nuclear levels of conflict. The speed and precision of these capabilities may expand decision-makers' knowledge of adversary forces, deployments, and actions sooner than was previously possible, but some of this information may also be vulnerable to intentional disinformation and other gray-zone activity.[47] Also, the sheer amount of information itself poses another challenge insofar as processing and deriving useful knowledge from the raw data can be overwhelming for analysts and decision-makers alike.[48]

In addition, advanced nuclear-armed states may become dependent upon conventional surveillance and targeting systems to provide strategic warning. For example, hypersonic weapons, boost-glide systems, long-range cruise missiles, and other capabilities are designed to elude traditional U.S. early-warning systems (e.g., radars and satellites), reduce confidence in strategic warning, and defeat American missile defenses. To counter these new delivery systems, the United States may have to rely on conventional situational awareness systems, including systems that are more visible or intrusive, to provide nuclear warning, support nuclear missions, and supplement strategic situational awareness. If an adversary were to discover and target these surveillance systems, would such an attack be considered conventional or strategic?

These dependencies and entanglements cut both ways. For example, conventional missile warning currently relies on these dual-use surveillance capabilities, increasing the risk that they could be targeted in a conventional conflict for conventional purposes but with profound strategic implications. Emerging digital technologies coupled with advanced sensor and surveillance capabilities integrated across space and cyber domains can provide vast amounts of data more quickly and precisely than ever before, including information about strategic threats that may prove elusive to traditional warning systems. But given the stakes involved, it is also difficult to imagine that in a conflict between nuclear powers, adversaries would allow such information dominance to proceed unchecked.

This reliance on strategic warning and communication assets in conventional conflicts is on the rise. As advanced, long-range, and often dual-use missile systems have proliferated dramatically in recent decades, including among a range of nuclear-armed adversaries, such reliance now must figure significantly into the planning and execution of conventional conflicts. For example, China has

45 One example is the U.S. Ballistic Missile Early Warning System, which became operational beginning in 1959 and was designed to detect incoming Soviet intercontinental ballistic missiles with a network of radars placed in Alaska, Greenland, and the United Kingdom — well outside of Soviet territory.

46 Rebecca Hersman et al., "Under the Nuclear Shadow."

47 Hicks et al., *By Other Means Part 1*.

48 Isaac R. Porche, III, et al., *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR315.html.

increasingly tasked its submarines, missiles, space assets, and other command and control infrastructure with both nuclear and conventional missions.[49] States have strong incentives to target command, control, warning, and surveillance systems early in a crisis in order to ensure conventional dominance, which will also threaten nuclear-related systems whether intentionally or unintentionally. As James Acton has argued, this type of action could leave the targeted state strategically blinded, introducing a variety of escalatory risks into the crisis, including nuclear escalation due to a "misinterpreted warning."[50] Others have suggested that even as China may intend to adhere to a No-First-Use posture, if it perceives a conventional strike by the United States as an attack on its nuclear retaliatory capability, it could escalate to the nuclear level nonetheless.[51] At the same time, surveillance systems designed principally for conventional missions may also have utility for nuclear missions as well. For example, the Global Hawk unmanned aerial vehicle was initially intended "to support joint combatant forces in worldwide peacetime, contingency and wartime operations."[52] However, as Keir Lieber and Daryl Press suggest, increasingly capable unmanned aerial vehicles, like the Global Hawk, with advanced stealth and sensor capabilities may also be useful to track a small country's mobile missiles — whether nuclear or conventional.[53] These and other dual-use capabilities contribute to the blurring of the line between conventional and nuclear spheres and the opening of unexpected gaps in escalatory restraint.

There is also the potential for states with smaller nuclear arsenals to draw big states into conflict in ways that defy the stability-instability paradox...

Distinctions or firebreaks between conventional and strategic situational awareness systems will likely continue to erode, creating a highly networked, real-time, dual-use landscape that is both more precise and more complex across all levels of conflict — sub-conventional, conventional, and strategic. The lack of distinction between the conventional and strategic domains will only intensify as new surveillance and warning systems come online. As such, the days of clear delineations between nuclear and non-nuclear situational awareness capabilities — which help maintain a sharp firebreak between conventional and strategic conflict — seem limited at best. Moving forward, the highly networked nature of conventional systems, as well as the dual-capable nature of many of them, may elevate the potential for conflict to spill over into the nuclear realm. Technical firebreaks have all but disappeared, opening the possibility that steps taken to gain information on conventional military capabilities will be easily confused with more escalatory intrusions into nuclear-related systems. Historically, the conceptual validity of the "stability-instability paradox" was reinforced by distinct and stratified conventional and strategic systems of warfare that amplified the division between nuclear and nonnuclear levels of war. In a world in which these systems have dual uses, the durability of that reassuring theoretical construct may be further called into question.

Nuclear Escalation in the Second Nuclear Age

The risk of asymmetric escalation is not exclusively a feature of direct competition and conflict between great-power adversaries. Sudden and indirect escalation to a strategic crisis can also result from the fragmentation of power on the global geopolitical landscape and the multipolar dynamics emanating from regional nuclear powers. Today's great-power competition occurs in a context of rising regional tensions and growing nuclear capabilities of previously second- or third-tier nuclear-armed states,

49 Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (April 2017): 50–92, https://doi.org/10.1162/ISEC_a_00274.

50 Acton, "Escalation through Entanglement," 58.

51 Talmadge, "Would China Go Nuclear," 50-92.

52 "RQ-4 Global Hawk," United States Air Force, Oct. 27, 2014, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/.

53 Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (Spring 2017): 37–46, https://doi.org/10.1162/ISEC_a_00273.

adding risk and complexity to escalatory dynamics and giving smaller states a larger vote in the nature and intensity of large-state competition. In addition, the lack of clear thresholds and triggers for possible conflict and divergent nuclear doctrine and declaratory policies further complicate attempts at escalation management.

Complex regional competition dynamics among nuclear-armed states will further complicate our understanding of nuclear escalation and crisis management. For example, the traditional measure of strategic stability — the presence of a secure second-strike capability — is problematic for smaller nuclear-armed states that may lack sufficient geographical depth or balance to credibly absorb an attack and still respond with sufficiently devastating effect. As Lieber and Press argue, regional nuclear powers are at a considerable resource disadvantage and may not be able to effectively conceal their nuclear arsenals from the rapidly improving intelligence, surveillance, and reconnaissance technologies of the United States.[54] Also, while movement toward increasing strategic transparency greatly facilitated strategic stability between the United States and Russia, the stabilizing effect of transparency among smaller nuclear powers is far less clear since many such states — Israel most notably — depend on opacity and ambiguity to manage complex regional dynamics and prevent costly arms racing. Multipolar strategic stability probably won't play out according to traditional concepts and rule sets — such as stability-instability — or at least not in the same ways as in the past.

Escalating Off-Ramps

Complex regional escalation dynamics that occur under a nuclear shadow may also play out at the geostrategic level such that "small-state" conflicts can escalate to "big-state" wars in unexpected ways. In a regional conflict or crisis, participants (states and actors who are directly engaged) and stakeholders (states and actors who are indirectly engaged) may possess different views about the value and risks of escalation. There is also the potential for states with smaller nuclear arsenals to draw big states into conflict in ways that defy the stability-instability paradox, which assumes that lower levels of conflict can be enabled rather than dampened by stability at the nuclear level because of self-regulating behavior by the states involved. However, this theory did not envision a circumstance in which smaller nuclear-armed countries might engage in more aggressive or violent competition because they believe that large countries will step in to create face-saving backstops or escalation "off ramps" and save them from themselves. Indeed, Feroz Khan has argued that deterrence in South Asia now depends on intervention by the United States to manage and minimize the consequences of either side's destabilizing behavior.[55] For example, amid an escalatory spiral with Pakistan, India may call on the United States to step in or risk allowing it to cross the nuclear threshold. In this scenario, both global and regional strategic stability dynamics shape the way these actors interpret conflict, and by extension their perceived freedom of action and relative dominance.

The 1999 Kargil Crisis is representative of a crisis-escalation scenario in which smaller nuclear-armed states perceive that bigger powers will swoop in to save them from nuclear confrontation. Just one year after India and Pakistan became overt nuclear powers, the two countries approached the brink of nuclear war. Following an attempted land-grab by Pakistan in the hotly contested Kashmir region, the United States provided an off-ramp to de-escalate the conflict. At the height of the crisis, Pakistani Prime Minister Nawaz Sharif "insisted" on meeting with President Bill Clinton, according to Clinton's senior director for Near East and South Asian affairs on the National Security Council, Bruce Riedel.[56] The United States stepped in after Clinton called both India's and Pakistan's leaders. Washington also sent its senior military commander in the region and a senior State Department official to Islamabad. Later, former deputy secretary of state Strobe Talbott wrote that the world was closer to nuclear confrontation than during the Cuban Missile Crisis.[57] Clearly, diplomatic interventions that can deescalate a crisis and forestall a nuclear conflict should always be pursued. However, expectations that the great powers will step in to rescue small nuclear states caught in an escalatory spiral may shift the burden of restraint and reduce accountability and responsibil-

54 Lieber and Press, "The New Era of Counterforce," 37–46.

55 Feroz Hassan Khan, "The Independence-Dependence Paradox: Stability Dilemmas in South," Arms Control Association, accessed June 30, 2020, https://www.armscontrol.org/act/2003-10/features/independence-dependence-paradox-stability-dilemmas-south.

56 Bruce Riedel, "American Diplomacy and the 1999 Kargil Summit at Blair House," in *Asymmetric Warfare in South Asia: The Causes and Consequences of the Kargil Conflict*, ed. Peter R. Lavoy (New York, NY: Cambridge University Press, 2009), 130–43.

57 Strobe Talbott, "The Day A Nuclear Conflict Was Averted," *YaleGlobal Online*, Sept. 13, 2004, https://yaleglobal.yale.edu/content/day-nuclear-conflict-was-averted.

ity for managing strategic stability among regional actors in ways that may reinforce rather than reduce risk-taking. In such a scenario, the United States may not initiate an escalation wormhole, so much as get pulled through one.

Reckless Driver Escalation

Third-party, "escalation pull" dynamics may also emerge through extended deterrence when a nuclear "protectee" feels emboldened in its interactions with regional nuclear powers due to protection under a larger state's nuclear umbrella. In these circumstances, smaller states — both nuclear and non-nuclear — may drive escalation in hopes of triggering intervention by other actors on their behalf. As the only country in the world to extend a formal nuclear umbrella over many of its formal treaty alliance partners, this risk is most acute for the United States. As Barry Posen writes, these "reckless drivers" may take bold actions with little regard for U.S. interests, despite their relative dependence on the United States.[58] These participants and stakeholders may have asymmetries of stakes and interests that drive their choices and behavior. In Asia, the complex dynamics between a small nuclear power (North Korea), larger nuclear powers (China and the United States), and extended deterrence alliance members (Japan and South Korea) underscore the challenge. In Europe, some of these dynamics play out along the "old NATO-new NATO" divide as states closer to the Russian periphery may feel the need to test NATO resolve. Some have argued risks of U.S. entrapment were not as high in the bipolar world of the Cold War, when the loss of any one smaller partner would not have dramatically upset stability, and there were no major differences in interests between the United States and its allies.[59] But today's more diffuse global power structure is more conducive to "reckless driving," as medium-size partners, such as India, may be more confident the United States would come to their aid given their greater importance to the global balence of power. Moreover, in a multipolar system, the interests of U.S. partners are more likely to diverge from the United States.

Equalizing Asymmetries

In recent years, sophisticated technologies have leveled the playing field for a range of actors to compete across various domains of conflict. Smaller nuclear states are not immune to the allure of gray-zone tactics and influence operations as means to coerce preferable outcomes at lower cost and risk. As cyber weapons and disinformation become more ubiquitous, regional powers are also learning how best to tailor sub-conventional tactics to enable their own strategies for escalation dominance. Moreover, asymmetric capabilities may encourage actors to engage in high-risk, escalatory behavior at lower levels of conflict in attempts to achieve victory, potentially outmaneuvering militarily superior states without ever having to pull the trigger.[60] Smaller states can compete in the digital information realm far more effectively than they could in traditional military competition. In fact, when it comes to disinformation racing, smaller regional powers can give larger states a serious run for their money. The advances in digital technology have transformed the internet into a 21st-century "wild west" where non-state actors and small powers can take on militarily superior states with disproportionate impact, high deniability and limited retaliatory risk. North Korea's infamous cyber attack on Sony in 2014 illustrates this point.[61] In this environment, cyber and advanced-technology tools obscure attribution and accelerate the time between launch and impact, making it difficult to trace where an attack originated or who was behind it. On this new frontier, anyone and any state can launch an attack with the click of a button. Just because a state can start a war, however, doesn't mean it can end it successfully on its own terms or avoid a sudden strategic crisis with a highly antagonized nuclear adversary.

Break Failure

The risk of unexpected escalation in a more regionalized, multipolar context stems not only from different strategic gambling or risk-taking by smaller nuclear powers, but also from the absence of escalation control measures that can tamp down or de-escalate a strategic crisis — most notably in the form of a secure second-strike capability or

58 Barry R. Posen, *Restraint: A New Foundation for U.S. Grand Strategy* (Ithaca, NY: Cornell University Press, 2014), 44.

59 Mira Rapp-Hooper, *Shields of the Republic: The Triumph and Peril of America's Alliances* (Cambridge, MA: Harvard University Press, 2020).

60 Dan Altman, "Advancing Without Attacking: The Strategic Game Around the Use of Force," *Security Studies* 27, no. 1 (2018): 58–88, https://doi.org/10.1080/09636412.2017.1360074.

61 Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," *USA Today*, Dec. 18, 2014, https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

enhanced transparency. Since the beginning of the Cold War, the U.S. and Soviet definitions of strategic stability rested on the notion that possessing a secure second-strike capability would disincentivize an adversary from launching a nuclear attack against the other with the understanding that a devastating counterattack was inevitable. This concept of stability fundamentally depends not only on the survivability of the arsenal — achieved by the advanced hardening and concealment of missiles — but also on sufficient strategic depth to make regime survival of such an attack plausible. In fact, most analysts believe that secure second strike was the principal enabler of strategic stability even in the face of conventional and sub-conventional conflicts that largely played out through and with non-nuclear subordinate states.

This form of strategic stability is, by definition, a "big-state" phenomenon. However, a second-strike capability may not be plausible for smaller countries, such as North Korea or Israel, that do not possess sufficient geographic strategic depth to absorb a first strike and then launch a second. For small states, then, strategic stability may need to rest on a different foundation, one that accounts for intense pressures to strike first in a crisis where the first move is also the only move. In such a scenario, the inability to launch a secure second strike may actually accelerate a crisis rather than simply fail to control it.

Similarly, the stabilizing benefits of transparency may play out differently in the multipolar landscape, where sudden or unexpected transparency may in fact open a new deterrence gap or wormhole — especially for states that possess smaller nuclear arsenals. At the great-power level, transparency regarding strategic-level capabilities, intentions, and processes has long been considered stabilizing. During the Cold War, transparency often accompanied arms control agreements and served to enhance strategic stability by preventing arms racing between the United States and the Soviet Union.[62] However, according to Steve Fetter, "transparency generally increases security only when states are reasonably comfortable with the status quo."[63] Among other nuclear arms possessors and aspirants, such as China, Israel, North Korea, and Iran, opacity instead has been viewed as more stabilizing by creating ambiguities that reduce the risk of conflict and reinforce deterrence. In a world where asymmetric capabilities are employed to gain escalation dominance, sub-conventional tactics might challenge deliberate opacity or ambiguity surrounding nuclear weapons programs by revealing capabilities or processes in ways that are destabilizing.

Exiting the Wormhole: Managing and Preventing Strategic Crisis in the New Nuclear Age

In today's security environment, sub-conventional weapons may no longer be confined to sub-strategic targets. Weaponized social media, widespread open-source information that used to be the exclusive domain of intelligence collection, and an increasingly "post-truth" atmosphere suggest a new and dangerous battlespace. In this context, small wars could quickly morph into big wars in ways that are difficult to anticipate or manage, perhaps rendering traditional military conflict "overrun by events" before the shooting starts and prompting consideration of tools and options normally reserved only for crises of existential proportion. Similarly, the inclination of competing states to pursue horizontal escalation options even as the separation between nuclear and conventional systems erodes suggests that the risks of wormhole escalation pervade the upper levels of the conflict spectrum as well. The ever-more interdependent and dual-use nature of emerging technologies, from advanced delivery systems to intrusive surveillance and warning systems, indicates that states may have more incentives to move first in a crisis, especially if warning and communication systems are compromised. Asymmetric war-fighting techniques at the sub-strategic level — cross-domain coercion, front-door information attacks, latent and out of control disinformation, and shifts from opacity to transparency — will shape the way states compete and change how they perceive their relative dominance across the spectrum of conflict.

In this unstable security environment, finding new ways to manage and reduce risk is critically important. In particular, managing strategic escalation risks that eminate from gray-zone influence operations requires breaking down long-standing silos between nuclear policy and other security policy experts. Developing a greater degree of political and societal resilience in the face of these manipulative tactics well ahead of crisis and conflict is also

62 Joseph S. Nye, Jr. "Farewell to Arms Control," *Foreign Affairs* 65, no. 1 (Fall 1986): 1–20, https://www.foreignaffairs.com/articles/russian-federation/1986-09-01/farewell-arms-control.

63 Nicholas Zarimpas, ed., *Transparency in Nuclear Warheads and Materials: The Political and Technical Dimensions*, Stockholm International Peace Research Institute, 2003, https://www.sipri.org/sites/default/files/files/books/SIPRI03Zarimpas/SIPRI03Zarimpas.pdf.

essential. Concepts of collective security, like "see something, say something," cannot just be about suspicious packages, but must include other illicit and nefarious intrusions into the fabric of national life. Some of the traditional tools of risk management, such as the establishment of clear firebreaks between nuclear and non-nuclear systems, may not be feasible. In the Center for Strategic and International Studies' two-year study of the impact of the emerging strategic situational awareness and information ecosystem, the authors concluded that "mutual dependencies between conventional and non-conventional capabilities, and the need for strategic [situational awareness] capabilities to address nuclear risks preclude relying on 'disentanglement' as a primary means of risk reduction."[64] Instead, familiarizing policymakers with this complex information ecosystem through realistic exercising of senior decision-making processes is essential to better understand and prepare for high escalation risk crises. In addition, expanding the topics and approaches for bilateral and multilateral stability talks, including a much broader perspective on risks associated with today's information ecosystem would be helpful.

While these sorts of crisis mitigation measures are important, they will not impose the types of limits or controls necessary to close escalation wormholes and prevent a destabilizing arms race. For that, clearer mutually agreed upon limits will be required. The same pressures that are increasing strategic competition and complicating escalation dynamics have also taken a toll on other traditional sources of strategic stability — particularly in terms of the transparency and restraint provided by arms control treaties. Following the demise of the Intermediate-Range Nuclear Forces Treaty and the announcement of Washington's intention to withdraw from the Open Skies Treaty, the New Start Treaty is the last remaining nuclear arms control treaty between the United States and Russia. Its expiration in February 2021 now seems nearly unavoidable. And yet, in a more competitive security environment characterized by high risks and limited resources, measures that build confidence, reduce miscalculation, enhance transparency, and restrain costly and dangerous military competition may increase both in value and applicability.

Arms control structures and institutions, along with their mechanisms for dispute resolution and compliance enforcement, can provide useful venues for addressing sources of conflict, adjudicating differences of view and perspective, and restraining impulsive or risky actions. But to be effective, arms control — and the arms control community — will have to adapt to the current security environments and account for rapidly evolving technological and informational factors. Arms control will need to move beyond overly rigid, stove-piped approaches and incorporate alternative structures and models, asymmetric use of trade space, and innovations in participation and inclusion of stakeholders and participants. In a recent *Journal of Strategic Studies* article, Heather Williams offers an asymmetric arms control framework that emphasizes the importance of *dynamism* in designing such agreements.[65] A dynamic approach would give states flexibility in their commitment to prospective agreements by allowing for mutual adjustment in force posture in ways that differ from the traditional "like-for-like" approach to arms control. Such issues should also be considered in the context of broader nuclear risk-reduction strategies. In today's multipolar world, there is an opportunity to address and limit asymmetric tactics by engaging in broader strategic stability talks and encouraging the development of alternative normative frameworks. In this context, the discussion of norms and codes of conduct for information and cyber warfare in strategic competition is long overdue.

Successful and durable arms control in this time of renewed major-power competition also requires thinking in a new way about verification and compliance in the face of an increasingly weaponized information environment. The growing accessibility, maturation, and diffusion of online platforms and digital tools have democratized information but also contributed to easy manipulation and misuse, which undermines credible and authoritative sources of information. Deep fakes, weaponized social media, and information sabotage will be used to discredit the negotiation, implementation, and verification of arms control. Such tactics will target not only governments but also non-governmental entities and individuals with the intention of shaping and manipulating information, not just stealing it. Moreover, the explosion of international open-source analysis means the days of proprietary, private, official sources and processes as an exclusive means of verification — particularly in the form of national intelligence — may be over. Open source information and analysis can and should be leveraged when accurate and accessible. Indeed, for some future arms control arrangements in which intrusive inspections

64 Hersman et al., "Under the Nuclear Shadow," 55.

65 Heather Williams, "Asymmetric Arms Control and Strategic Stability: Scenarios for Limiting Hypersonic Glide Vehicles," *Journal of Strategic Studies* 42, no. 6 (2019): 789–813, https://doi.org/10.1080/01402390.2019.1627521.

might not be agreeable or desirable, it presents a potential alternative. Open source information can only perform this function, however, if its authenticity and reliability can be ensured and the techniques and practices used to collect, analyze, and distribute this information are effective and ethical.

Furthermore, influence and information operations can sow doubt and distrust into the public's view of established institutions and can frustrate efforts to build multilateral consensus around treaties and their enforcement. States can amplify effects, obscure attribution, and prime the information space to their advantage before, during, and after negotiations. For example, AI-enabled microtargeted activities can be used to make organizations, individuals, and communities — including arms control negotiators, inspectors, and monitors — vulnerable to coercion through ransomware, encrypted bribes, doxing, and other techniques.

In a world characterized by global and regional strategic stability dynamics, escalation thresholds are being redefined across the spectrum of sub-conventional, conventional, and nuclear conflict and perceptions of strategic stability are transforming quickly. If a traditional, predictable escalation ladder ever existed, it certainly no longer does today. Instead, today's competitive and highly asymmetric security environment suggests the need for new concepts and metaphors to understand and manage emerging escalation risks. Fueled by an increasingly competitive security environment, transformational technologies, and a more fragmented global order, escalation wormholes may appear, likely with little warning. Asymmetries of tools, domains, and stakes will complicate this landscape as nuclear-armed states, both large and small, seek to navigate this new escalatory terrain. Wormholes are inherently, and indeed catastrophically, unstable. Whether in terms of space travel or nuclear escalation, they seem best avoided.

Rebecca Hersman *is a leading expert on nuclear, chemical, and biological weapons policy and crisis management. In addition to leading the preeminent national program designed to develop next-generation nuclear policy expertise, Ms. Hersman has authored numerous studies and reports on nuclear and chemical weapons policy, emerging technologies and strategic stability, and crisis management and decision-making. Ms. Hersman joined CSIS in April 2015 from the Department of Defense, where she served as deputy assistant secretary of defense for countering weapons of mass destruction (WMD) since 2009. In this capacity, she led Defense Department policy and strategy to prevent WMD proliferation and use, reduce and eliminate WMD risks, and respond to WMD dangers. Prior to joining the Defense Department, Ms. Hersman was a senior research fellow with the Center for the Study of Weapons of Mass Destruction at the National Defense University from 1998 to 2009. Ms. Hersman previously held positions as an international affairs fellow at the Council on Foreign Relations, a special assistant to the undersecretary of defense for policy, and a member of the House Armed Services Committee professional staff. She holds an M.A. in Arab studies from Georgetown University and a B.A. from Duke University.*

Acknowledgements: *This article reflects a yearlong consideration of escalation wormholes and how these phenomena might better describe many escalation dynamics in the emerging security environment. The article benefitted enormously from the assistance of several staff members and reviewers along the way. Annalise Ploostser provided much of the initial research and drafting assistance for early drafts. Suzanne Claeys supported many of the speeches and articles on disinformation that have been incorporated into this analysis. Maxwell Simon picked up all of the research support efforts in recent months and contributed greatly. Sameer Lalwani, Heather Williams, Rebecca Lissner, and Morgan Kaplan read earlier drafts and provided invaluable feedback. Finally, the editorial team at* TNSR *vastly improved the flow and readability of the argument. All remaining flaws are entirely my own.*

Photo: Matthew J. Bragg