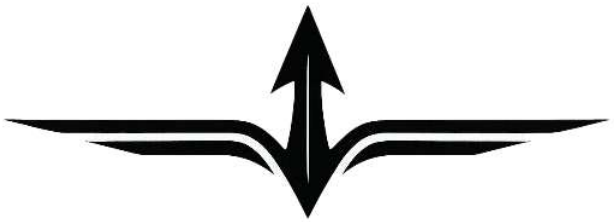
Chapter 15



Organizing Power

Elizabeth Kunce and Elsa Kania

"Power corresponds to the human ability not just to act but to act in concert."[2]

— Hannah Arendt
On Violence (1970)

Introduction: Organizing Power Under Pressure

In an era defined by great-power competition, rapid technological transformation, and persistent societal disruption, national power cannot be measured solely by military capability or technological innovation. A decisive variable is the speed, legitimacy, and coherence with which states organize whole-of-society resilience and civil-military integration under pressure. From this perspective, resilience must therefore be understood not as the capacity to recover from

shock, but as a form of governance under sustained strain—one that aligns government, the military, the private sector, and civil society while preserving public trust and democratic legitimacy.

This chapter advances three core claims. First, resilience has become a central determinant of strategic advantage under conditions of persistent competition short of war. Second, the United States and the People's Republic of China pursue fundamentally different models of civil-military and societal integration, with distinct implications for legitimacy, adaptability, mobilization capacity, and escalation control. Third, multinational technology corporations now occupy a structural position within national security ecosystems that existing governance frameworks are ill-equipped to manage, which creates challenges and opportunities for new forms of partnership.

Through a comparative analysis of democratic coordination in the United States and military-civil fusion within China's authoritarian innovation ecosystem, the chapter situates contemporary U.S. initiatives, such as the 2025 Genesis Mission,[3] within a longer American tradition of civil–military–industrial mobilization. We conclude with policy-relevant recommendations for institutionalizing democratic resilience as a core national security function, arguing that technological capability alone is insufficient without the institutional capacity to coordinate and mobilize resources coherently, legitimately, and at speed under sustained pressure.

Resilience as Democratic Governance

Contemporary great-power competition is shaped not only by advances in military and technological capability but by the compression of time, authority, and legitimacy amid persistent

contestations. Increasingly, emerging technologies and techniques, including big data analytics, artificial intelligence (AI), cyber operations, space systems, and biotechnology, are accelerating decision cycles, blurring civil-military boundaries, and exposing domestic economic, informational, and infrastructural systems to continuous pressure and strategic threats. These dynamics are increasingly visible in competition below the threshold of war—where states contest influence through coercion, disruption, and pressure short of open conflict—and require whole-of-government and whole-of-society responses.[4]

In this environment, the decisive question is no longer simply whether states possess capability, but whether their governments, in concert, can integrate and employ it quickly and legitimately under pressure. A nation's resilience—defined here as the capacity to absorb shocks, adapt rapidly, and sustain coordinated action without fracturing political legitimacy or societal cohesion—has become a core dimension of national power.

Yet resilience can convey a range of connotations within modern security discourse. The importance of resilience has been invoked in describing phenomena ranging from individual psychological endurance to infrastructure hardening and supply-chain redundancy. This breadth risks reducing resilience to a rhetorical placeholder rather than an operational principle. For the purposes of this chapter, resilience refers to a society's ability to mobilize, adapt, and recover at speed while sustaining democratic legitimacy, public trust, and unity of effort across government, the military, industry, and civil society.[5] Confronting contemporary challenges, resilience is not merely a technical attribute or a crisis-response capability; rather, it is a governing function that determines whether a state can act decisively

and mobilize resources without eroding the social contract on which its authority rests.

The factor that distinguishes the current strategic environment centers not only on the scale of technological change but also on the velocity at which disruption cascades across domains. Information manipulation, cyber intrusions, economic coercion, and supply-chain shocks now unfold faster than traditional governance and civil-military coordination mechanisms can respond. Under these conditions, a degree of institutional fragmentation itself becomes a strategic vulnerability. Increasingly, strategic advantage accrues to systems capable of synchronized, whole-of-society action, rather than those relying on isolated economic or military superiority or technological dominance.

Fragmentation of Power

Historically, the nation-state served as the primary organizer of security, crisis response, and economic mobilization. That organizational monopoly has eroded. Increasingly, multinational technology corporations control critical data infrastructures, communications platforms, and innovation ecosystems that underpin both civilian life and military effectiveness. Driven primarily by market incentives rather than public accountability, these firms nonetheless shape conflict, public trust, escalation dynamics, and strategic stability in ways once reserved for sovereign governments.

Today, technological innovation is driven largely outside traditional government research and development institutions. Operating across borders and often beyond the reach of existing regulatory frameworks, multinational technology corporations have

emerged as central actors shaping security environments at both national and international levels. Their control over data, platforms, and digital infrastructure enables them to influence international norms, economic dependencies, and strategic outcomes—frequently with limited transparency or democratic oversight.

While these firms can enhance state power through technological innovation and scale, they also introduce systemic vulnerabilities. Platforms and infrastructures essential to national defense and public life are largely governed by commercial incentives rather than security imperatives. Where the "arsenal of democracy" once referred to industrial production capacity, today's technology enterprises are constructing the digital geography of the global commons—often without clear guardrails, public oversight, transparency, or mechanisms for democratic control. In an era of deep digital interdependence, private corporate decisions can rival, and at times exceed, the strategic impact of state action, particularly when corporate systems directly shape combat operations.

As a result, technology companies have become embedded actors in international security rather than peripheral suppliers. Governments confronting challenges related to AI, cyber defense, data governance, and information integrity increasingly engage directly with companies. This shift has given rise to tech diplomacy, the practice of engaging major technology firms as strategic stakeholders in global security.[6]

Through tech ambassadors, special envoys, and sustained engagement with innovation hubs such as Silicon Valley, governments increasingly treat major technology companies as de facto geopolitical stakeholders.[7] Yet this redistribution of power has

created a growing mismatch between where strategic capabilities reside and where democratic accountability can be readily exercised, generating a new category of strategic risk and challenges centered on the alignment of incentives.

Corporate Actors, Dual-Use Platforms, and Escalation Control

Traditional approaches to civil-military integration have treated technology primarily as equipment or enabling capability, paying insufficient attention to the growing role of private industry as an operational actor within modern conflict. The war in Ukraine has demonstrated that multinational technology corporations now occupy positions of structural influence within the battlespace, shaping information flows, communications resilience, and escalation dynamics in ways previously reserved for state authorities.

Ukrainian civilians, using commercially available smartphones, satellite connectivity, and private-sector applications, have provided real-time imagery and operationally relevant intelligence through government reporting platforms.[8] In doing so, civilians have become participants in a battlespace increasingly defined by networked information systems rather than territorial control. This evolution blurs the boundary between civilian support and direct participation in hostilities, complicating long-standing legal and operational distinctions.

These challenges scale significantly when applied to multinational technology firms. By enabling or constraining satellite networks, managing cloud infrastructure, moderating digital platforms, or adjusting algorithmic systems, private corporations now shape

operational environments with direct and sometimes decisive effects on military outcomes. Their decisions influence force survivability, command-and-control resilience, intelligence flows, and public perception—often in real time and across multiple theaters.

The Ukraine war provides a clear illustration. The Starlink satellite communications system, owned and operated by a private U.S. company, has functioned as critical battlefield infrastructure. Reports of service limitations in September 2022, reportedly linked to concerns about escalation risks, underscored how corporate actors can exercise de facto control over operational tempo and escalation pathways.[9] In practice, a single private firm could enable, constrain, or suspend connectivity essential to military operations. This concentration of influence exposes a growing governance gap. Existing legal frameworks and civil-military arrangements offer limited guidance for managing situations in which privately owned systems become operationally indispensable. The longstanding assumption that states control the tools, timing, and thresholds of warfare no longer reflects operational reality. Technology companies, whether intentionally or inadvertently, now function as strategic intermediaries whose decisions shape deterrence stability, escalation risk, and operational continuity.

As public and private dimensions of conflict increasingly overlap, traditional distinctions between civilian, military, and commercial domains have become operationally obsolete. Dual-use platforms simultaneously support civilian life and combat functions. Satellite networks enable emergency communications and targeting intelligence; cloud services host both commercial data and military logistics; content moderation influences morale, legitimacy, and international narratives. These systems operate under commercial

governance structures that are not designed for crisis decision-making under conditions of armed conflict.[10]

This convergence raises fundamental questions of authority, accountability, and risk management. Who determines acceptable operational tradeoffs when commercial interests conflict with military requirements? How are liability and neutrality defined when platforms underpin combat operations? Under what conditions can states rely on privately controlled infrastructure for deterrence and warfighting?

In the absence of institutionalized governance mechanisms, these decisions are often made ad hoc, through informal negotiations between corporate leadership and government officials, with limited transparency or democratic oversight. Regulatory ambiguity enables corporations to consolidate strategic influence while insulating themselves from political and legal responsibility for escalating outcomes. Over time, this misalignment of authority and accountability creates systemic vulnerability.

For defense policymakers, the central challenge is not whether private-sector capabilities are indispensable—they are—but whether they can be integrated into national security architectures without ceding escalation control, operational continuity, or political legitimacy. Failure to resolve this governance gap risks fragmented crisis response, delayed mobilization, and unilateral corporate decisions that may constrain military options at critical moments.

Addressing this challenge requires moving beyond episodic public-private cooperation toward durable institutional arrangements. Whole-of-society resilience depends on establishing clear expectations, authorities, and decision pathways for privately owned systems that function as critical security infrastructure. This includes

pre-negotiated protocols for crisis operations, continuity of service, information sharing, and escalation management, aligned with legal authorities and democratic oversight.

The implications extend beyond bilateral U.S.–China competition. In an interconnected global system, privately controlled platforms increasingly mediate coalition operations, alliance interoperability, and multinational crisis response. Without shared norms and governance frameworks, jurisdictional seams and regulatory fragmentation will continue to undermine collective resilience.

Absent sustained institutional reform, the boundary between commercial innovation and strategic intervention will continue to erode, with consequences for the law of war, human rights, and crisis stability. Where governance fails to keep pace with technological integration, legitimacy erodes—and legitimacy remains the center of gravity for democratic resilience and sustained strategic advantage.

Competing Models of Integration: Democratic Resilience and Military-Civil Fusion

Declining trust in democratic institutions compounds the challenge of organizing power under pressure. As documented by the Edelman Trust Barometer, confidence in government, media, business, and NGOs has eroded across democratic societies.[11] This erosion is not merely a social concern; it constitutes a strategic vulnerability. Civil-military integration, public compliance during crises, and sustained public-private cooperation all depend on institutional legitimacy, transparency, and shared purpose.

The recent findings suggest that erosion has entered a more destabilizing phase, characterized by heightened grievance and declining confidence that institutions act in the public interest. Under such conditions, the social cohesion required for rapid, coordinated national mobilization is strained. Where trust weakens, authority fragments, compliance becomes conditional, and coordination slows—creating exploitable seams for adversaries employing information operations, cyber intrusions, and economic coercion.

Against this backdrop, the United States and China represent fundamentally different models of civil-military and societal integration. These approaches diverge not only in political values but in their organizing logic: who directs mobilization, how incentives are aligned, how rapidly capabilities can be surged, and how legitimacy is sustained under stress.

Operation Warp Speed (OWS) provides a critical empirical case of how the United States mobilizes under such conditions. Through mission-bounded integration of federal agencies, the Department of War (then Department of Defense), private industry, and state and local distribution networks, OWS combined public risk absorption, contractual incentives, decentralized innovation, and military logistics to accelerate vaccine development and delivery. Rather than structurally fusing civilian and military systems, OWS relied on voluntary participation, parallel experimentation, and legal oversight to align diverse actors around a time-limited national objective. This model enabled rapid capability surge while preserving institutional boundaries and market autonomy, demonstrating the latent organizing power of democratic public-private cooperation when legitimacy and incentives are aligned.[12]

At the same time, OWS also revealed the centrality of trust to democratic mobilization.[13] Vaccine uptake, compliance with public health measures, and sustained intersectoral cooperation were directly affected by public confidence in institutions and information environments. Where trust eroded, coordination costs increased, and operational effectiveness declined, underscoring that legitimacy functions as a force multiplier and potential failure point in the U.S. integration model.

China's strategy of military-civil fusion, by contrast, seeks to mobilize society in service of state-defined priorities through centralized direction and compulsory alignment, supplemented by incentives for bottom-up initiative.[14] Unlike public-private partnerships in democratic systems, military-civil fusion can start to erode meaningful boundaries between civilian and military domains subject to direct Party control.

Although China's approach draws partly upon lessons from U.S. civil-military integration, it reflects a uniquely systemic effort to create an integrated national strategic system.[15] This includes mechanisms for employing civilian assets for military purposes, ranging from organized militias to dual-use logistics and transportation platforms, such as roll-on/roll-off ferries designed for rapid conversion from civilian to military use.[16] China's large-scale mobilization of thousands of fishing vessels through its maritime militia system to create apparent barriers at sea, such as could support a potential blockade, also demonstrates the potential for these capabilities to be leveraged at scale as a tool for coercion or in conflict.[17] The implications for crisis stability and conflict preparation are significant: highly integrated mobilization architectures can

compress warning timelines, accelerate escalation dynamics, and complicate signaling and decision-making.

For the United States, preserving the democratic character of resilience is therefore not a constraint on power, but a strategic imperative. The challenge is not to emulate authoritarian integration—which tends to achieve speed by subordinating transparency, pluralism, and feedback—but to institutionalize democratic resilience: a model capable of achieving unity of effort at speed without sacrificing accountability, rights, or legitimacy.

America's Strategic Inheritance: When Integration Worked

The United States possesses a rich legacy of civil-military-industrial cooperation that offers guidance for renewing national resilience and competitiveness. During World War II, President Franklin D. Roosevelt's "Arsenal of Democracy" mobilized industrial, scientific, and societal capacity on an unprecedented scale.[18] Civilian manufacturers rapidly retooled for wartime production, while labor and research communities aligned around national objectives. Coordinated through the War Production Board, this effort not only contributed decisively to victory, but also generated enduring innovations—from mass-produced penicillin to the Manhattan Project—that reshaped postwar power.

In the postwar period, the National Security Act of 1947 restructured U.S. national security governance, enabling enduring coordination among military, scientific, and civilian institutions.[19] The establishment of the National Science Foundation and the expansion of federal investment in research forged durable linkages among national defense, academia, and industry.[20] The Soviet launch of

Sputnik in 1957 further catalyzed this model, leading to the creation of the Advanced Research Projects Agency (ARPA, later renamed the Defense Advanced Research Projects Agency, or DARPA) and institutions such as RAND, a federally funded research and development center that provides strategic analysis to the U.S. government.[21] Together, these organizations formed a sustained innovation pipeline linking government requirements with civilian scientific ambitions. DARPA, in particular, became a mechanism for advancing high-risk, high-reward technologies with lasting dual-use impact.[22]

During the Cold War and Space Race, this approach matured into a system capable of addressing new technological frontiers by aligning military requirements with civilian innovation. By the Vietnam era, dual-use technology had become an explicit focus, laying the groundwork for later breakthroughs in GPS, microelectronics, and biotechnology. In the 1990s, the Technology Reinvestment Project further formalized these relationships by incentivizing joint ventures among defense contractors, private firms, and universities as defense spending declined.[23] Although the U.S. industrial base has contracted in subsequent decades, this historical record demonstrates that the United States has repeatedly organized power effectively when strategic leadership aligned institutions, incentives, and public purpose.

The post–September 11 era marked a renewed shift toward whole-of-government and whole-of-nation approaches as the United States confronted hybrid and transnational threats.[24] National security planning expanded beyond traditional defense to include the protection of critical infrastructure, reflected in institutions such as the Cybersecurity and Infrastructure Security Agency, which

institutionalized public-private coordination to defend essential national systems.[25]

This tradition continued during the COVID-19 pandemic. Operation Warp Speed demonstrated the capacity for rapid, cross-sector mobilization to accelerate vaccine development and deployment at unprecedented speed and scale.[26] Widely regarded as a successful example of innovation under pressure, it reinforced the enduring potential of coordinated public-private action when leadership, authority, and urgency are aligned effectively.

The New Test: Technology, Time Compression, and National Mobilization

Whereas previous generations of integration challenges focused on aligning industry, science, or government institutions with military requirements; today's challenge is fundamentally different—organizing power across globally networked, privately controlled systems under conditions of continuous competition and compressed time.

The United States now faces a new generation of integration challenges: aligning civilian, military, public, and private capabilities at speed across domains such as AI, cyber operations, quantum technologies, and infrastructure resilience. These domains constitute the next frontiers of strategic competition and national defense. Unlike previous eras, the contemporary "arsenal of democracy" relies as much on software, data, and globally distributed digital infrastructure as it does on physical production capacity. As a result, multinational technology corporations operating across borders and jurisdictions

have become indispensable partners in both the U.S. economy and its national security architecture.

Among these challenges, AI and quantum technologies differ from earlier military innovations in that they are inherently systemic rather than sectoral. Their development relies on civilian data ecosystems, commercial computing infrastructure, global supply chains, and highly mobile talent pools—collapsing traditional distinctions between civilian resilience and military effectiveness. Recognizing this shift, the Department has pursued new mechanisms to integrate private-sector expertise, including initiatives such as Detachment 201: the Executive Innovation Corps, which confers reserve officer status on select technology leaders to accelerate defense-relevant innovation.[27]

Within this lineage of national mobilization, the Genesis Mission announced in November 2025 may represent the next structural inflection point. It introduces a presidential directive for coordinated action across government, industry, and scientific institutions to catalyze innovation and resilience in frontier technology domains with direct national security implications.[28] Rather than a finished model, Genesis should be understood as a test case for whole-of-society mobilization at speed, seeking to operationalize coordination across federal agencies, state and local governments, private technology firms, academia, and civil society.

Whereas earlier periods of innovation were often catalyzed by government-led research and development, today's technological advances are largely driven by multinational technology firms. Their global reach, control over data, and technical expertise allow them to shape international norms, economic dependencies, and even strategic

stability—often with limited regulatory oversight or democratic accountability. This reality intensifies the leadership challenge of organizing power across dispersed, non-sovereign actors under conditions of time compression and strategic competition—where failure to coordinate becomes a strategic rather than an administrative inconvenience.

Authoritarian Mobilization as a Stress Test

The emerging integration challenge is not theoretical. China provides a prominent real-world example of how power can be rapidly organized under centralized authority. This model enables speed and coordination, but it does so by subordinating legal constraint, transparency, and voluntary consent to directive control—an approach that carries significant implications for legitimacy, adaptability, and escalation stability.[29]

China's approach to national security is uniquely holistic and comprehensive. The "comprehensive national security concept" (总体国家安全观), introduced by Xi Jinping in April 2014, defines security as encompassing political, economic, military, scientific, technological, cultural, and societal domains, among others. This expansive conception of security reflects both strengths and pathologies. While it enables coordinated action across sectors, it is ultimately shaped by the Chinese Communist Party's overriding priority of political and regime security, which conditions how information flows, incentives are structured, and risk is assessed.

Within this framework, China's national strategy of military-civil fusion aims to establish an integrated national strategic system that advances both economic and military power. Military-civil fusion

serves as a strategic organizing principle that aligns civilian and military resources through centralized direction. Its scope extends well beyond technology, encompassing talent management, data-sharing, logistics, and national defense mobilization. By deliberately collapsing the distinction between civilian and military domains, Beijing aims to accelerate capability development and societal mobilization across multiple sectors simultaneously.

Linked to and enabled by military-civil fusion, China's national defense mobilization system has evolved into a comprehensive nationwide architecture extending down to provincial and local levels. In a crisis, this system could facilitate rapid mobilization, compress warning time, and complicate adversaries' escalation management by blurring the distinction between civilian and military activity. Beyond frequently cited examples such as the maritime militia, the People's Liberation Army has prioritized the development of new-type militia units focused on unmanned systems, cyberspace, and psychological operations—further blurring the boundaries between participation, support to operations, and outright engagement in combat.[30]

China's emphasis on national security also seeks to align development and security across both traditional and non-traditional domains. In May 2024, Beijing released a white paper on *National Security in the New Era*, emphasizing scientific and technological self-reliance as a central component of national security.[31] While China's increasing securitization of its economy and technology base presents clear strategic challenges for the United States and its allies, it also reveals Chinese leaders' concerns about internal vulnerabilities, dependency, and resilience while facing sustained pressure.

For U.S. and allied strategists, the significance of China's model as a competitive challenge lies not in emulating authoritarian integration but in understanding how centralized mobilization architectures can compress warning timelines, alter escalation dynamics, and reshape the strategic environment. The comparative challenge is ensuring that democratic systems can organize power with sufficient speed and coherence to compete—without sacrificing legitimacy, accountability, or control, which remain foundational sources of long-term strategic advantage.

Conclusions and Policy Implications

Looking forward, the central challenge for the United States is not a lack of capability, but the ability to organize and sustain legitimate, coordinated action under the conditions of time compression, technological interdependence, and persistent competition in crisis and conflict. Resilience is not merely the capacity to endure disruption; it is the capacity to govern effectively under pressure—aligning authority, responsibility, and action across government, the military, the private sector, and civil society while preserving public trust and confidence.

In an environment shaped by hybrid coercion, dual-use technological dependence, and contested information space, governance capacity—and the legitimacy that underwrites it—has become a determinant of national power. Failure to institutionalize democratic resilience risks slower mobilization, fragmented response, ad hoc escalation decisions by private actors, and erosion of public confidence—each of which adversaries can exploit.

To strengthen whole-of-society resilience as a core national security function, the United States should prioritize the following governance-oriented actions:

1. **Establish public-private governance mechanisms for dual-use technology platforms.** Public-private engagement must move beyond procurement toward shared governance of critical digital infrastructure. This includes pre-established protocols for continuity of services, crisis decision-making, and responsibilities in conflict environments, ensuring that essential private-sector capabilities can be mobilized rapidly without ceding escalation control or undermining democratic accountability.
2. **Strengthen mobilization capacity and redundancy to enable protracted competition and conflict**. The United States should invest in redundancy and surge capacity across critical supply chains, including stockpiles of essential minerals likely to be disrupted in conflict. The design of legislative authorities and institutional arrangements should be reviewed in advance to ensure that industrial and technological capabilities can be mobilized at speed, rather than constrained by ad hoc deliberation. This imperative is particularly acute in emerging domains such as biotechnology, where the ability to pivot from commercial production to medical countermeasures and biosecurity defenses is essential.[32]
3. **Institutionalize enduring coordination measures across levels of government and sectors**. Effective resilience requires clearly defined roles, decision rights, and escalation

pathways that extend beyond federal levels to state and municipal authorities, where much operational capacity resides. Initiatives such as the 2025 Genesis Mission can serve as a test case for integrating federal, subnational, and private-sector actors into a coherent coordination architecture without displacing legal parameters or civilian authorities.

4. **Deepen allied and partner resilience coordination and interoperability**. Resilience is increasingly collective. The United States should expand its collaboration with core allies and partners, especially in the Indo-Pacific, through joint exercises, information sharing, supply-chain coordination, and the adoption of aligned standards for infrastructure security and technology governance. Shared approaches can reduce vulnerabilities created by jurisdictional seams and deny adversaries opportunities to fragment interconnected systems.

5. **Build shared understanding of risks and threats through routine cross-sector exercises.** Whole-of-society resilience depends on common situational awareness, which requires the capacity for information sharing and interoperable systems. Scenario planning and stress testing should routinely integrate government agencies, the military, critical infrastructure owners, technology firms, academia, and civil society. Priority should be given to scenarios involving cyber-enabled disruption, supply-chain coercion, information manipulation, and cascading infrastructure failures.

6. **Shift from reactive responses to anticipatory planning centered on resilience**. Planning should look beyond static

contingency frameworks and drive toward forward-looking assessments of vulnerabilities most likely to be targeted. This includes accounting for nontraditional actors, complex societal crises, and interdependent infrastructure failures, as well as ensuring that legal authorities and public communication frameworks are prepared in advance to sustain legitimacy during rapid escalation.

7. **Reinforce civil-military trust as an operational enabler.** Civil-military trust is not an abstract value but a functional requirement for unity of effort. To that end, sustained engagement, transparency, and clear norms governing domestic support roles are essential to maintaining public confidence in military professionalism and democratic oversight during crises and conflicts.

Ultimately, the future balance of power will be shaped not only by technological advances but also by societies' ability to organize themselves coherently, legitimately, and effectively under sustained pressure. The generation of whole-of-society resilience is the mechanism through which democratic systems translate values into strategic advantage. For the United States, investing in democratic resilience is not merely defensive; it is a proactive strategy to deter coercion, prevent the loss of escalation control, and sustain long-term strategic credibility in a contested global order.

Endnotes

[1] The authors are solely responsible for the views expressed in this publication, which do not necessarily represent the official policy or position of the Daniel K. Inouye Asia-Pacific Center for Security Studies, the U.S. Department of War, or the U.S. government.

[2] Hannah Arendt, *On Violence* (San Diego, CA: Harvest/HBJ, 1970), 44.

[3] Executive Order No. 14363, "Launching the Genesis Mission," Federal Register, November 24, 2025, https://www.federalregister.gov/documents/2025/11/28/2025-21665/launching-the-genesis-mission.

[4] North Atlantic Treaty Organization, "Deterrence and Defence," NATO What We Do, accessed January 2026, https://www.nato.int/en/what-we-do.

[5] Edward H. Christie and Kristine Berzina, *NATO and Societal Resilience: All Hands on Deck in an Age of War*, Policy Brief (The German Marshall Fund of the United States, July 2022), https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf; UK Government, *The Resilience Framework: 2023 Implementation Update*, (London, UK Government, December 4, 2023), https://www.gov.uk/government/publications/the-resilience-framework-2023-implementation-update.

[6] Kristin Eggeling, "Fieldnotes from the Bay: Why Are There Diplomatic Offices in Silicon Valley?" USC Center on Public Diplomacy, August 30, 2024, https://uscpublicdiplomacy.org/blog/fieldnotes-bay-why-are-there-diplomatic-offices-silicon-valley.

[7] Eggeling, "Fieldnotes from the Bay."

[8] Michael N. Schmitt and William Casey Biggerstaff. "Ukraine Symposium – Are Civilians Reporting with Cell Phones Directly Participating in Hostilities?" *Articles of War*, Lieber Institute, West Point, November 2, 2022, https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/.

[9] Joey Roulette, Cassell Bryan-Low, and Tom Balmforth. "Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia," *Reuters*, July 25, 2025, https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/; Sasha Vakulina, "Musk's SpaceX and Ukraine's Defence Ministry to Block Russia's Use of Starlink," *Euronews*, February 2, 2026,https://www.euronews.com/2026/02/02/musks-spacex-and-ukraines-defence-ministry-to-block-russias-use-of-starlink; Amritha Jayanti, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, March 9, 2023, https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

[10] G. Blair Kuplic and Jonathan Sawmiller, "Humanity on the Final Frontier: Challenges in Applying International Humanitarian Law to Modern Military Space Operations," *International Review of the Red Cross*, June 2025, https://international-review.icrc.org/articles/humanity-on-the-final-frontier-928.

[11] Edelman Trust Institute, *2025 Edelman Trust Barometer* (Edelman, January 2025), https://www.edelman.com/trust/2025/trust-barometer.

[12] Simi V. Sidalingaiah, *Operation Warp Speed Contracts for COVID-19 Vaccines and Ancillary Vaccination Materials*, Congressional Research Office, Insight, IN11560, updated March 1, 2021, https://www.congress.gov/crs_external_products/IN/PDF/IN11560/IN11560.6.pdf; U.S. Government Accountability Office, *Operation Warp Speed: Accelerating COVID-19 Vaccine Development Status and Efforts to Address Manufacturing Challenges*, GAO-21-319 (Washington, DC: GAO, February 2021), https://www.gao.gov/assets/gao-21-319.pdf.

[13] Jeffrey V. Lazarus et al., "A Global Survey of Potential Acceptance of a COVID-19 Vaccine." *Nature Medicine* 27 (2021): 225–228, https://doi.org/10.1038/s41591-020-1124-9.

[14] Alex Stone and Peter Wood. "China's Military-Civil Fusion Strategy," China Aerospace Studies Institute, June 15, 2020, https://www.airuniversity.af.edu/CASI/Display/Article/2217101/chinas-military-civil-fusion-strategy/.

[15] Tai Ming Cheung, "National Strategic Integration: How China is Building Its Strategic Power," IGCC/MERICS, October 2023, https://ucigcc.org/wp-content/uploads/2023/10/Cheung-National-Strategic-Integration-and-Building-of-Chinas-Strategic-Power-2.26.24.pdf.

[16] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: DOD, December 2025), 46, https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

[17] Chris Buckley, Agnes Chang, and Amy Chang Chien, "Thousands of Chinese Fishing Boats Quietly Form Vast Sea Barriers," *The New York Times*, January 16, 2026, https://www.nytimes.com/interactive/2026/01/16/world/asia/china-ships-fishing-militia-blockade.html.

[18] Paul W. Rhode, James M. Snyder Jr., and Koleman Strumpf, "The Arsenal of Democracy: Production and Politics During WWII," *Journal of Public*

Economics 166 (2018): 145 – 61, https://users.wfu.edu/strumpks/papers/JPubE_2018.pdf.

19 National Security Act of 1947, Pub. L. No 80–253, 61 Stat. 496 (1947), as amended through Pub. L. 119–60, December 18, 2025, https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.

20 Laurie Harris, *The National Science Foundation (NSF): FY2026 Appropriations and Funding History*, Congressional Research Services, Report R48783, https://www.congress.gov/crs-product/R48783.

21 U.S. National Academy of Sciences Committee on Criteria for Federal Support of Research and Development, "Supplement 1: The Evolution and Impact of Federal Government Support for R&D in Broad Outline," in *Allocating Federal Funds for Science and Technology* (Washington, DC: National Academies Press, 1995), https://www.ncbi.nlm.nih.gov/books/NBK45556/.

22 Defense Advanced Research Projects Agency, "About DARPA," DARPA, accessed January 2026, https://www.darpa.mil/about; Marcy E. Gallo, *Federally Funded Research and Development Centers (FFRDCs): Background and Issues for Congress*, Congressional Research Services, Report R44629, updated August 27, 2021, https://www.congress.gov/crs-product/R44629.

23 Defense Advanced Research Projects Agency, *Program Information Package for Defense Technology Conversion, Reinvestment, and Transition Assistance,* Technology Reinvestment Project (Washington, DC: DARPA, March 10, 1993), https://acquisitioninnovation.darpa.mil/docs/DARPA%20OT%20Programs/Technology%20Reinvestment%20Project.pdf.

24 U.S. Department of Homeland Security, "Creation of the Department of Homeland Security," last modified May 8, 2023, https://www.dhs.gov/creation-department-homeland-security.

25 U.S. Government Accountability Office, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236 (Washington, DC: GAO, March 10, 2021), https://www.gao.gov/assets/gao-21-236.pdf.

26 GAO, *Operation Warp Speed*.

27 U.S. Army Public Affairs. "Army Launches Detachment 201: Executive Innovation Corps to Drive Tech Transformation," June 13, 2025, https://www.army.mil/article/286317/army_launches_detachment_201_executive_innovation_corps_to_drive_tech_transformation.

[28] Exec. Order No. 14363, "Launching the Genesis Mission."

[29] Kwan Nok Chan, "Public Administration in Authoritarian Regimes: Proposition for Comparative Research," *Asia Pacific Journal of Public Administration* 46, no. 3 (2024): 214–19, 224–25, https://doi.org/10.1080/23276665.2024.2306554.

[30] Recorded Future, "China's Militia Forces Train to 'Get Strong' in the New Era," October 30, 2025, https://www.recordedfuture.com/research/chinas-militia-forces-train-to-get-strong-in-the-new-era.

[31] State Council Information Office of the People's Republic of China, *Xin shidai de Zhongguo guojia anquan* [National Security in China's New Era] (Beijing: Foreign Languages Press, May 2025), http://www.scio.gov.cn/zfbps/zfbps_2279/202505/t20250512_894771.html.

[32] National Security Commission on Emerging Biotechnology, *Charting the Future of Biotechnology* (Washington, DC: NSCEB, April 2025), 70, https://www.biotech.senate.gov/final-report/chapters/.