ANALYSIS

DIMET: RECONFIGURING GLOBAL POWER IN THE TECHNO-STRATEGIC AGE

Curtis McGiffin

Executive Summary

Today's fourth industrial revolution is characterized by artificial intelligence, automation, advanced manufacturing, and immersive technologies. As these innovations reshape societies and security environments, they have emerged as a core determinant of national power. No longer just an enabler of diplomacy, information, military, or economic power instruments, technology now serves as a fifth lever of power—changing the DIME framework of national power projection into the DIMET. It influences every aspect of statecraft, fueling economic competitiveness, military strength, geopolitical influence, and strategic resilience.

In this new era of "techno-strategic" power, technological sophistication both enhances and redefines a nation's ability to secure interests, project influence, and withstand strategic competition. "Technological States" that can leverage cutting-edge robotics, AI, biotechnology, quantum systems, space architecture, hypersonics, and advanced cyber capabilities will gain a military advantage, boost economic competitiveness, shape global governance, influence public opinion, and safeguard sovereignty. Technology also drives dependency and interconnectivity, making the ability to control, protect, and innovate critical systems a key measure of national resilience. Nations that proactively embrace, invest in, and strategically oversee forward-looking technological capabilities will define the future global order.

Technological power is now inseparable from strategic deterrence. It accelerates decision cycles, blurs the line between peace and conflict, and introduces new vulnerabilities across physical, digital, and biological domains. Technological power now decides whether nations can defend against cyberattacks, resist strategic coercion, and deter technologically sophisticated adversaries or face consequences from those who possess it. In this environment, mastery of cutting-edge technology has become the new strategic factor in shaping global order.

Introduction

The Information Age began in the mid-twentieth century with the invention of the transistor and the development of first-generation computers. The digital revolution accelerated in the 1970s, transforming society by the 1990s with the normalization of the internet. New inventions continue to disrupt the socio-economic landscape and enter the military-

This article expands on, Curtis McGiffin, "DIMET: Shaping the Age of 'Techno-Strategic' Power" *Information Series*, No. 637 (Fairfax, VA: National Institute Press, September 22, 2025).

industrial complex. Today, the world is in the midst of the fourth industrial revolution, advancing the digital age through machine learning, automation, digitalized manufacturing, and augmented reality.[1]

In the twenty-first century, the levers of national power have evolved beyond the traditional DIME framework—diplomacy, information, military, and economic strength—to include a fifth lever: technology. No longer merely a supporting function, technology has become embedded within all other instruments of power, acting simultaneously as an enabler, a multiplier, and a core indicator of national capability. Advances in robotics, artificial intelligence (AI), biotechnology, quantum computing, and related fields shape a nation's ability to secure its interests, project influence, and withstand strategic competition. As these technologies mature, they redefine both what power is and how it can be projected.

This new era of "techno-strategic" power deliberately integrates advanced technological capabilities with national strategy, fusing intelligent societies and innovative industries into a competitive engine of state power that blurs the boundaries between the physical, digital, and biological domains, reshaping how nations generate influence, project strength, and prepare for conflict.[2]

Explaining the Instruments of Power

For any country, geopolitical power is the ability to influence others' behavior to achieve desired outcomes, which are viewed as interests secured through the instruments of national power.[3] National power is central to determining a state's position, influence, and ability to exercise strategic options within the international system. Traditionally assessed by military strength, economic capacity, and diplomatic influence, national power is often viewed through the lenses of hard power (coercive methods to compel compliance) and soft power (persuasion or attraction to garner compliance).[4]

The projection of state power traditionally involves four main instruments: DIME (diplomatic, information, military, economic). These instruments of national power frequently overlap or connect to create synergies of influence or to maximize power. This framework helps strategists and policymakers to organize, formulate, and mobilize these power sources to meet their objectives:

---

[1] "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?," *McKinsey & Company*, Accessed July 9, 2025, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir.

[2] Leo Blanken, Doowan Lee, and Stephen Rodriguez, "The Imperative of Waging Techno-Strategic War: Looking Back at Technology Innovation," *Strategy Bridge*, August 17, 2018, https://thestrategybridge.org/the-bridge/2018/8/17/the-imperative-of-waging-techno-strategic-war-looking-back-at-technologyinnovation.

[3] Robert D. Worley, *Orchestrating the instruments of power: a critical examination of the U.S. national security system* (Potomac Books, an imprint of the University of Nebraska Press, 2015), p. 225.

[4] "Hard Power vs. Soft Power: How Nations Really Influence Each Other," *GovFacts*, November 24, 2025, https://govfacts.org/policy-security/hard-power-vs-soft-power-how-nations-really-influence-each-other/

- **D - Diplomatic**: This refers to using diplomacy, relationships, and negotiation to influence and achieve national goals. It involves persuasive engagement among states, including formal and informal discussions, treaties, and alliances.[5]
- **I - Informational**: This covers a nation's ability to gather, control, and manipulate information to achieve strategic, political, economic, or military goals. It uses information and communication strategies to influence foreign audiences, shape narratives, and promote national interests. Examples include public diplomacy, strategic communications, media engagement, cultural exchanges, cyber operations, combating disinformation, and information management security.[6]
- **M - Military**: This refers to the threat or use of armed force to achieve national objectives and further national interests. It includes deterrence, combat operations, security assistance, military training, multinational exercises, and humanitarian aid delivery.[7]
- **E - Economic**: This entails leveraging economic resources, access, and tools to influence other states. It encompasses international trade (access to goods, services, and resources), global finance (including investment, credit, and transaction access), and development assistance (grants, aid, and debt relief).[8] Economic statecraft includes "carrots," of aid, trade, and treaties, as well as "sticks," such as sanctions, tariffs, and export controls.[9]

Successful foreign policy often requires a "whole-of-government" approach in which diplomatic efforts are backed by credible military power, supported by information campaigns, and reinforced by economic incentives or disincentives.

Technology as an Instrument of National Power

In the early stages of the Cold War, the United States used technology in the form of nuclear weapons to offset or counterbalance the Soviet Union's non-nuclear military force advantages.[10]10 During the Second Offset (mid-1970s to late 1980s), Washington relied on leap-ahead technologies,[11] including precision munitions, stealth, persistent surveillance, and fourth-generation fighters, focusing on quality over quantity against the Warsaw Pact's numbers after the Vietnam War.[12] The Pentagon's 2015 Third Offset initiative emphasized

---

[5] Steven Heffington, Adam Oler, and David Tretler, *A National Security Strategy Primer*, (Washington, D.C.: National Defense University Press, 2019), pp. 24-25.

[6] Ibid., pp. 25-27

[7] Ibid., pp. 28-29

[8] Ibid., pp. 30-32

[9] Worley, *Orchestrating the Instruments of Power*, op. cit., p. 233.

[10] Gian Gentile, Michael Shurkin, Alexandra T. Evans, Michelle Grisé, Mark Hvizda, and Rebecca Jensen, *A History of the Third Offset,* 2014–2018 (Santa Monica, CA: RAND Corporation, 2021), https://www.rand.org/pubs/research_reports/RRA454-1.html.

[11] Rebecca Grant, "The Second Offset," *Air & Space Forces Magazine*, June 24, 2016, https://www.airandspaceforces.com/article/the-second-offset/.

[12] Gentile, Shurkin, et al., "A History of the Third Offset."

robotics, AI, cyber, unmanned systems, and machine learning, recognizing that adversaries were gaining or leading in technology.[13]

In her 2021 article, Maria Constantinescu from the National Defense University in Romania emphasized that the volatile, uncertain, and complex security environment necessitated a comprehensive approach that incorporates technology within a DIME-T framework across all security domains.[14] She noted that "technology will likely influence the operating environment of the future in direct and indirect ways," urging security strategies to reflect this.[15] Her clarion call to elevate technology beyond simply enabling improved national security was insightful; however, it did not fully explain how technology might be applied in context.

The term "technology" as an instrument of power emphasizes "high tech," involving significant investment in and use of advanced science and engineering methods or materials to perform complex functions. It shifts technology from an element of power to an instrument of power. While natural resources, population, and infrastructure form the elements of state strength, instruments like technology project power. Technological progress has accelerated and is now a key factor of power and influence, not just an element of national strength.[16]

Those who understand nuclear deterrence theory recognize that credibility is as important as capability. In current geopolitics, technological power not only projects real power, but it also shapes perceptions of power.

Projecting real power. Technology is already recognized as a key enhancer of DIME power, facilitating global communication, finance, navigation, and military force projection. However, projecting technological power is the deliberate use of advanced technology to influence other nations, achieve foreign policy objectives, bolster security, and enhance economic strength. It impacts terrestrial, maritime, aerial, space, and cyberspace domains, often crossing boundaries in nanoseconds by transmitting data via bits, pulses, and waves. Moreover, from drones and AI to satellites and quantum computing, technology is agnostic to civilian and military uses, often employing dual-use capabilities that permeate the commercial marketplace and the battlefield. Finally, the projection of technological power also occurs when dominance is paired with dependency—when others must rely on your systems to maintain their own functionality. Reliance on a nation's technological authority extends beyond mere possession of technology; it encompasses ongoing support and access to emerging technologies, which can stimulate allied interoperability, foster diplomatic connectivity, and enhance economic integration.

---

[13] Robert Work, Deputy Secretary of Defense, *The Third U.S. Offset Strategy and its Implications for Partners and Allies*, Speech Transcript, Washington, D.C., January 28, 2015, https://www.defense.gov/News/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/.

[14] Maria Constantinescu, "The National Security Strategy in the Current Environment: From Dime to a Dime-T Approach," *International Conference Knowledge-Based Organization*, Vol. 27, No. 1, June 2021.

[15] Ibid.

[16] Ibid.

Shaping perceptions of power. Generally, countries perceive the power of other nations through a combination of material production, observed actions, and future potential. They often assess military strength, economic performance, and technological sophistication to establish a baseline of objective power. Perceptions are further shaped by a nation's reputation for competence, its trajectory of innovation, and its capacity to generate future advantages. In today's digital world, the most influential nations lead in technology. Technology now defines how states compete, collaborate, and project sovereignty. Taiwan has leveraged its advanced semiconductor industry to attract Western investment and security guarantees, producing 90 percent of the world's most sophisticated microchips, which serve as a "silicon shield" to prompt a U.S. military response should they be attacked.[17] This highlights the risk of global disruption if China were to launch a military attack in pursuit of unification. Taiwan must strike a balance between collaborating with the United States and addressing concerns that relocating chip manufacturing could compromise its security. For Taiwan, its microchip industry is not just an economic asset; it is a perceived form of sovereign power that influences the behavior of other states.

Technology is a tool of national power that both drives and is driven by other instruments, leveraging multiple domains and serving various functions.[18] Within the DIME framework, diplomacy seeks to achieve agreement, information disseminates knowledge, the military employs coercion, and economics strives for prosperity; technology facilitates the exquisite execution of these instruments of power. However, technology today is not merely an enabler; it constitutes a decisive strategic domain. It shapes the balance of power, determines the character of war, pervades the media, and energizes the global marketplace. Technology enables nations to project power and influence on an expanded scale, extending well beyond their borders. Thus, adding technology as a fifth instrument of national power would necessarily change the acronym from DIME to DIMET (pronounced "Dye-Met"). Therefore, including the "T - Technology" in the DIME framework descriptions would be as follows:

- **T - Technology**: This pertains to the pragmatic utilization of scientific knowledge and engineering expertise, as well as the invention, deployment, and exploitation of devices and methods to enhance human performance, while concurrently reducing the impact of time, distance, and volume.[19]

In this world, no country is entirely devoid of technology. There exist "states with technology," "technological states," and "technologically marginal" states. The difference

---

[17] Matthew Shea, "Taiwan's chip dominance becomes global security, economic flashpoint," *United Press International* (June 12, 2025), https://www.upi.com/Top_News/World-News/2025/06/12/taiwan-semiconductors-world-economy/1961749741666/.

[18] Zachary Kallenborn, "National Security Needs Both Futurists and Traditionalists," *War on the Rocks*, April 1, 2021, https://warontherocks.com/2021/04/national-security-needs-both-futurists-and-traditionalists/.

[19] Description informed by: James Andrew Lewis, "Technology and Power," *Center for Strategic and International Studies*, March 30, 2022, https://www.csis.org/analysis/technology-and-power#:~:text=This%20series%20of%20short%20essays%20will%20examine%20key,they%20can%20be%20used%20to%20gain%20national%20advantage.

between a state with technology and a technological state pertains to the extent to which technology is integrated into the fabric of that state's national power and strategic goals.

A State with Technology is a country that has or uses technology, but technology is not central to its national identity, power, or strategic actions. It relies on commercially available off-the-shelf technology for internet access, communication, and military strength, but may lack significant local investment, innovation, or research and development capabilities.

A Technological State is a country where technology underpins its identity, policy, and power. It invests heavily in science, innovation, and emerging technologies to boost its military and global stature; utilizes technology to shape international norms and geopolitics; and leverages technology for sovereignty, deterrence, and competitiveness. It also has a robust state-tech-industrial complex, like military-tech partnerships, digital governance, cyber capabilities, and strong local innovation.

A Technologically Marginal State is a country with only basic or antiquated technology, and is often fragile, isolated, or failed. It has minimal infrastructure, suppresses innovation, lacks governance or access to technology, or may outright reject it. Generally, these states do not develop technology, lack control over it, are unable to weaponize it, and remain susceptible to those who possess such capabilities.

"States with technology" utilize it to maintain a modern, connected society in the global landscape. However, "technological states" leverage technology as a core part of their power and identity, boosting their military and economic influence. A technologically advanced state is often perceived as forward-looking, resilient, wealthy, and powerful. In a world where perception matches actual performance, technological strength is the new strategic currency. Whether stabilizing or disruptive, only a "technological state" can develop and exploit high-tech tools to impact global markets, influence governments, and deter or defend militarily with high-tech capabilities.[20]

Technological power lies not only in scale, but also in control and purpose. It serves as a powerful tool that can impact a technologically advanced nation across six distinct categories. These six categories can both overlap and inform one another.

1. Military Dominance Through Technological Superiority

Technology's role as a national power is most visible in military capabilities. From the bow and arrow to drones and satellites, technological advances have shaped the character of warfare.[21] Today, disruptive technologies like autonomous weapons, hypersonic missiles, AI decision-making, and directed energy are driving a paradigm shift in military preparation. High-tech militaries tend to embrace the transition from evolutionary to revolutionary

[20] Christopher F. Chyba, "New Technology & Strategic Stability," *Daedalus* 149, No. 2, Spring 2020, pp. 150-170, https://direct.mit.edu/daed/article/149/2/150/27321/New-Technologies-amp-Strategic-Stability.

[21] "Emerging and disruptive technologies," *NATO*, June 25, 2025, Accessed November 22, 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies.

capabilities, strategies, and organizations.[22] Modern high-tech militaries depend on information dominance rather than mass production, tend to prioritize network-centric operations over platform-centric approaches, and are potentially shifting from human intuition and cognition to AI autonomy and rapid processing.[23] Modern militaries now rely on advanced technology for precision strikes, missile defense, and battlefield awareness. America maintains its global influence and threats through its advanced long-range stealth aircraft, cyber capabilities, and satellite networks, underscoring its leadership in technology. When it comes to American technology and its impact on military capability, it is as much about the engineers as it is about the generals.[24]

While Russia's nuclear weapons technology has largely matured over the past half-century, nearly every category of its conventional, electronic, and space warfare capabilities has experienced notable technological advancement. Despite prolonged economic and technical sanctions, Russia's adoption of emerging technologies—including AI, unmanned systems, and hypersonic weapons—signals a significant shift in its defense strategy and provides competitive advantages in select domains. In 2017, President Putin asserted that "the one who becomes the leader in this [AI] sphere will be the ruler of the world."[25] Moscow's progress in hypersonic glide vehicles and cruise missiles, advanced air and missile defenses, and its pursuit of AI-enabled and nuclear-powered autonomous systems now challenge existing arms-control frameworks, exploiting gaps that heighten geopolitical tensions and undermine global stability.[26]

China pursues a campaign to dominate critical advanced technology sectors and its military is rapidly integrating emerging technologies to strengthen its forces and deploy disruptive military capabilities.[27] China's rapid militarization of AI, space systems, hypersonic weapons, and quantum communications underscores its strategic goal of achieving military parity with the US or dominance. China's 2021 test of a new orbital bombardment system showcased a significant technological breakthrough, with a 40,000 km flight in under 100 minutes. This unprecedented development disrupted the military balance and was likened to a "Sputnik-like moment" by then-Chairman of the Joint Chiefs of Staff, General Mark Milley.[28] Technological surprises typically result from a state's deliberate

---

[22] "The Transformative Effects of Military Revolutions on Warfare," *Total Military Insight*, July 15, 2024, https://totalmilitaryinsight.com/military-revolutions-and-their-impacts/.

[23] Michael Bennett, "Artificial intelligence vs. human intelligence: Differences explained," *TechTarget.com*, October 7, 2024, https://www.techtarget.com/searchEnterpriseAI/tip/Artificial-intelligence-vs-human-intelligence-How-are-they-different.

[24] Benjamin Jensen, Yasir Atalan, Can Mutlu, and Jose M. Macias III, *Competition in the Shadow of Technology* (Washington, D.C.: Center for Strategic & International Studies, 2024), p. 1.

[25] *Putin: Leader in artificial intelligence will rule world*, *Associated Press*, September 1, 2017, https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4.

[26] Defense Intelligence Agency, *2025 Annual Threat Assessment*, Washington, DC: May 11, 2025.

[27] Ibid., p. 7.

[28] Emma Helfrich, Tyler Rogoway, "More Details On China's Exotic Orbital Hypersonic Weapon Come To Light: An official report on Chinese military power revealed additional details about its hypersonic weapon test that made headlines in July

effort to disrupt the status quo, especially when involving the military capabilities of a rival state.

Weaponizable technological advancements that surprise the world can be destabilizing unless they are balanced or countered. While evolutionary technological improvements boost military effectiveness, revolutionary high-tech forces create greater fear and influence than ever before.

Cyber warfare opens a new domain of conflict where nations can exert power without traditional kinetic methods. Cyberattacks can disable critical infrastructure, steal secrets, and disrupt command-and-control networks. Smaller rogue powers like North Korea and Iran employ cyber tools to confront Western powers. Combining and leveraging technology with military and intelligence operations now allows smaller nations to showcase their strength in ways previously not possible.

2. Economic Competitiveness and the Technological Edge

Technology fuels economic growth, productivity, and global influence. It is much more than just access to the internet and mobile phones. Nations leading in technology excel in specialized industries, attract top talent, and set global standards. Currently, economic leaders such as the United States, China, Germany, Japan, Taiwan, and South Korea have achieved their status through continuous research and development, high-tech manufacturing, and advancements in fields including AI, biotech, robotics, telecommunications, and advanced materials.

Technology now drives economic security, which merges national security and economics.[29] Semiconductor supply chains, rare earth elements, 5G infrastructure, and microchips are not just commercial items; they are strategic assets. The 2022 global semiconductor shortage showed how access to critical technologies can affect everything from vehicle manufacturing to national defense systems. Recognizing this, countries are adopting "techno-nationalism," focusing on domestic innovation, securing supply chains, and restricting exports of critical technologies to competitors. China's "Made in China 2025" plan and the U.S. CHIPS and Science Act exemplify how nations embed technology into grand strategies, employing the DIME framework to further the "T," to help sustained or improve their respective power positions.

Technological states are not just wealthy; they also dominate the global market share. The economies of the world's five most technologically advanced nations—Japan, the Republic of Korea, China, the United States, and Germany—constitute 52 percent of the global gross domestic product.[30] Moreover, the United States, China, and Japan account for

---

2021," *The War Zone*, November 30, 2022, https://www.twz.com/more-details-on-chinas-exotic-orbital-hypersonic-weapon-come-to-light.

[29] Justin G. Muzinich, Gina M. Raimondo, James D. Taiclet, Jonathan E. Hillman, Anya Schmemann, "U.S. Economic Security: Winning the Race for Tomorrow's Technologies," *Council on Foreign Relations*, New York, November 13, 2025.

[30] "Most Technologically Advanced Countries 2025," *World Population Review*, August 10, 2025. https://worldpopulationreview.com/country-rankings/most-technologically-advanced-countries.

nearly 65 percent of the global stock market capitalization.[31] For example, "Apple's market cap alone ($3.56 trillion) is nearly equal to the entire stock market valuation of the United Kingdom ($3.7 trillion), while "Nvidia ($3.21 trillion) is almost as big as the combined stock markets of Canada and India."[32] These comparisons highlight the dominance of just two American high-tech companies and select technological states on the global stage.

3. Geopolitical Influence Through Technological Diplomacy

Technology is increasingly shaping global influence and alliances. Technological states are increasingly adopting technological diplomacy, a practice rooted in the power of innovation—the ability to create, regulate, and control transformative technologies. This approach often includes aspects of digital diplomacy, which relies on information power to shape narratives and influence audiences through digital platforms and social media. In contemporary international relations, however, significant state influence more often comes from guiding technological development and managing high-tech innovation ecosystems rather than solely relying on digital communication. While digital diplomacy mainly seeks to influence through communication, often using widely available digital and social media platforms, technological diplomacy exerts influence by developing, managing, and governing those platforms, capabilities, and standards that support the global technological framework.[33]

Leading countries in technological innovation set rules, regulate data, establish standards, and guide governance models. The competition over 5G networks between the United States and China exemplifies the intertwined economic and military rivalry. Washington's attempt to keep China's telecom systems out of the allied infrastructure was more than corporate rivalry; it was a strategic effort to prevent Beijing from embedding surveillance, gaining control over global networks, or conducting espionage in allied territories.

Similarly, nations are leveraging technology to advance diplomacy and cultivate strategic partnerships. For example, the European Union (EU) utilizes its regulatory influence—the so-called "Brussels Effect"—to shape global standards on data privacy. The United States, through its "tech companies," shapes much of the digital infrastructure and services used worldwide. Meanwhile, China exports surveillance technologies to autocratic regimes under the guise of "smart cities," thereby spreading its model of digital authoritarianism.

---

[31] Harshita Tyagi, "US commands half of Global Stock Market! Apple, Nvidia, Tesla and other top 10 giants hold 32% of it," *IND Money*, February 14, 2025, https://www.indmoney.com/blog/us-stocks/us-commands-half-of-global-stock-market-apple-nvidia-tesla-and-other-top-10-giants-hold-32-of-it.

[32] Ibid.

[33] "Digital Diplomacy vs. Tech Diplomacy: Understanding the Difference," *Tech Diplomacy Institute*, accessed 11/22/2025, https://tech-diplomacy.com/digital-vs-tech-diplomacy-navigating-the-new-frontiers-of-international-relations/#:~:text=Tech%20diplomacy%2C%20conversely%2C%20centers%20on,within%20diplomatic%20and%20governance%20frameworks.

Strategic partnerships, such as AUKUS (comprising Australia, the United Kingdom, and the United States) and the Quadrilateral Security Dialogue or the "Quad" (comprising the United States, India, Japan, and Australia), focus on technological cooperation in defense (nuclear-powered submarines), cybersecurity, and supply chain resilience. Technology now influences international norms, rules, and institutions, while connecting Western democracies. These democracies are becoming more integrated through shared digital infrastructure, cybersecurity standards, and common ethical frameworks.

4. Cyber Power and Manipulation

Cyber capabilities represent a new and powerful means of national power. They now shape markets, supply chains, and corporate governance as profoundly as they affect modern military operations. At the same time, digital influence campaigns reshape public opinion and alter political dynamics in ways once reserved for traditional statecraft or advertisement. As these trends converge, economic competition, military readiness, and information dominance become inseparable pillars of national power.

Cyberattacks can sabotage nuclear centrifuges, infiltrate critical infrastructures, or paralyze financial systems, thereby achieving strategic effects. Attacks on utilities, government facilities, and pipelines pose a significant threat to life and can have cascading effects for consumers. The difficulty in attribution and deniability makes cyber operations attractive to both state and non-state actors. Ransomware costs victims over $810 million in 2024, down from $1.25 billion in 2023.[34] The United Nations reports North Korea has stolen $3 billion in cryptocurrency to fund its nuclear weapons program.[35]

Cyber power extends beyond hacking to include information warfare, influence operations, and digital coercion. Russia's disinformation campaigns seek to weaken democracy, polarize societies, and erode trust in the United States and Western Europe. "Russian disinformation campaigns effectively exploit societal vulnerabilities, reshaping public opinion and geopolitical dynamics."[36] Similarly, the use of bots, trolls, and deepfakes adds a new dimension to strategic competition, where truth itself is now a contested domain. China spreads authoritarian AI worldwide, with models like DeepSeek's R1 and Alibaba's Qwen 2.5 rewriting history, censoring abuses, and suppressing topics to control online

[34] Bill Toulas, "Ransomware payments fell by 35% in 2024, totaling $813,550,000," *Bleeping Computer*, February 5, 2025, https://www.bleepingcomputer.com/news/security/ransomware-payments-fell-by-35-percent-in-2024-totalling-813-550-000/.

[35] Patrick Martin, "North Korea is behind cyberattacks worth $US3 billion and is stealing cryptocurrency to fund weapons programs, UN report finds," *Australian Broadcasting Corporation*, March 21, 2014, https://www.abc.net.au/news/2024-03-22/north-korea-stealing-cryptocurrency-to-fund-nuclear-weapons/103618152.

[36] Kateryna Odarchenko, "The Fight Against Disinformation: A Persistent Challenge for Democracy," *Foreign Policy Research Institute*, January 24, 2025, https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/.

discourse. China floods the market with 'free' open-source models that contain censorship while investing heavily in proprietary AI to achieve strategic dominance.[37]

Cyber operations and influence are now a staple in this global digital society and its militaries. Ubiquitous cyber technology enables malware, denial-of-service attacks, and social engineering to disrupt, damage, or infiltrate enemy systems, as seen in the 1982 Soviet pipeline sabotage, the 2007 cyberattacks on Estonia, the 2010 malware attack on Iran's centrifuges, and the 2015 network attack on Ukraine's power grid.[38] Defensive strategies focus on protecting infrastructure through firewalls, intrusion detection systems, digital encryption, and incident response plans, which are now necessary and responsible technical reactions. As digital connectivity deepens, adapting to future trends—such as the expanding and sophisticated influence of the Internet of Things, cyber-enabled surveillance, and AI-infused cyber operations—is essential for national resilience and global stability.

Emerging cyber-fused technologies are transforming both boardrooms and battlefields, reshaping how leaders assess risk, allocate resources, and compete for advantage—especially within the man-made environment of cyberspace. States capable of integrating AI with advanced cyber capabilities may process vast volumes of data at speed, extract predictive and actionable insights, and convert information superiority into decisive strategic advantage.[39]

Meanwhile, international laws, ethical considerations, and collaborative defense efforts seek to regulate behavior and enhance collective security. Countries and global corporations alike are now developing both offensive and defensive cyber strategies, investing in cyber commands, and viewing cyberspace as a frontier for economic, military, and diplomatic goals. The concepts of "persistent engagement" and "defend forward" in U.S. cyber strategy show that cyber operations are no longer just reactive—they are now a proactive, integrated part of national power.[40]

5. Strategic Resilience and Technological Sovereignty

Navigating a complex and uncertain world requires strategic resilience and technological sovereignty to maximize technology's influence against great power competitors. The rapid development or deployment of new or novel technologies can lead to strategic surprises, catching nations unprepared at the strategic level. Countries with a mutually reinforcing

---

[37] Doug Kelly, "America Must Act Now to Secure Tech Leadership, New Study Finds," *American Edge Project*, March 25, 2025, https://americanedgeproject.org/america-must-act-now-to-secure-tech-leadership-new-study-finds//

[38] Harry Atkins, "The Biggest Cyberattacks in History," *History Hit.com*, March 24, 2022, https://www.historyhit.com/the-biggest-cyberattacks-in-history/.

[39] Rakibul Hasan Chowdhury, Nayem Uddin Prince, Salman Mohammad Abdullah, and Labonno Akter Mim "The role of predictive analytics in cybersecurity: Detecting and preventing threats" *World Journal of Advanced Research and Reviews*, 2024, 23 (02), pp. 1615-1623, https://wjarr.com/sites/default/files/WJARR-2024-2494.pdf

[40] Department of Defense, *2023 Cyber Strategy Summary* (Washington, D.C.: U.S. Department of Defense, 2023), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

foundation rooted in resilience and sovereignty can lessen the possible impact of disruptive technologies that may exploit weaknesses and escalate risks.

Strategic resilience is a country's ability to anticipate, endure, and recover from disruptions that threaten its core military, economic, or technological functions, independence, or direction.[41] Technological sovereignty is a nation's capacity to develop, acquire, control, and safeguard its critical technologies and digital infrastructure.[42] When used together, resilience and sovereignty enable greater freedom of action by fostering increased technical agility and redundancy, as well as more control over data and supply chains amid interdependence, global competition, and systemic risks.

High-tech nations must protect critical infrastructure and data sovereignty, and foster resilient technological ecosystems. The recent pandemic and the war in Ukraine have revealed vulnerabilities in global supply chains,[43] an overdependence on adversaries' technology, and the need for resilient domestic capacity. Efforts such as Europe's GAIA-X cloud infrastructure,[44] India's push for "digital sovereignty,"[45] and the U.S. reshoring of semiconductor production[46] all seek to secure autonomy, reduce adversaries' leverage, and bolster strategic independence.

Another example of technological sovereignty is space-based navigation. Countries like Russia, China, and those within the EU have developed their own satellite systems for positioning, navigation, and timing (PNT), thereby reducing their reliance on the United States' Global Positioning System. Russia's Global Navigation Satellite System, with approximately 30 satellites, China's BeiDou with 35, and the EU's Galileo with 28, all have achieved global coverage. Japan and India are also developing regional space-based PNT. These efforts demonstrate how nations strive for digital and navigational sovereignty, showcase their technological capabilities, and enhance their global prestige.

The struggle to sustain and control sovereign and resilient technology is driven by the need to secure it against adversarial competitors and vulnerable supply chains. Technology is politically neutral and cannot always align with democratic values, Western ethical standards, or international security protocols. Nevertheless, a nation's control over its high-tech is vital to its strategic survival amid great-power rivalry.

---

[41] Department of Defense, *National Defense Strategy* (Washington, D.C.: Department of Defense, 2022), p. 8.

[42] GP Acharya, "Tech Sovereignty: National Power Capability to [sic] Threat to Humanity," *Nepal Foreign Affairs*, May 18, 2022, https://nepalforeignaffairs.com/tech-sovereignty-national-power-capability-to-threat-to-humanity/.

[43] 24/7 Staff, "The 13 Biggest Supply Chain Disruptions Since 2000," *Supply Chain 24/7.com*, May 20, 2025, https://www.supplychain247.com/article/the-biggest-supply-chain-disruptions-since-2000.

[44] "About Gaia-X," *Gaia-X* (website), last modified 2023, https://gaia-x.eu/about/.

[45] Shuborno Chakroborty, "AI, Digital Sovereignty, and Geopolitics: India's Strategic Positioning Between the U.S. and China." *Impact and Policy Research Institute*, May 2, 2025, https://www.impriindia.com/insights/ai-digital-geopolitic-indias-strategic/.

[46] Bill Conerly, "U.S. Manufacturers Reshoring, But It Will Take A Long Time," *Forbes*, August 19, 2023, https://www.forbes.com/sites/billconerly/2023/08/19/us-manufacturers-reshoring-but-it-will-take-a-long-time/.

6. Technology and Strategic Deterrence

Finally, technology is redefining deterrence in fundamental ways. In the Cold War era, U.S.-Soviet strategic deterrence was about mutually assured destruction and clear signaling. In the digital era, deterrence becomes more complex and ambiguous. Attribution is more difficult, escalation is uncertain, and the lines between war and peace, as well as between civilian and military, are increasingly blurred.

War remains primarily a political act, not just driven by advanced technological capabilities. Yet, greater risks emerge when autocratic nations combine strong geopolitical ambitions with highly effective militaries equipped with technologically sophisticated weapons that have intercontinental reach across all domains. The implications for strategic deterrence may be significant. A recent RAND study noted that "collections of emerging technologies—especially in the realms of information aggression and manipulation, automation [AI], hypersonic systems, and unmanned systems—hold dramatic implications for both the effectiveness and stability of deterrence." Moreover, strategic deterrence becomes significantly more difficult to maintain when adversaries threaten to employ integrated, multi-technology strategies that can simultaneously strike numerous points across diverse attack surfaces and vectors. Such convergence enables the prospect of "society-wide paralytic attacks," potentially eroding deterrence by giving an aggressor confidence that it can disable or delay a defender's response long enough to achieve its objectives.[47]

The pursuit of nuclear weapons has not diminished since the conclusion of the Cold War; rather, it has transformed into a new arena of strategic competition. For North Korea, Iran, and Pakistan, the aspiration for nuclear armament extends beyond mere sovereign security; it now represents a symbol of national pride and technical ability. In October 1965, shortly after losing the Indo-Pakistani War of that year, Pakistan's Foreign Minister Zulfikar Ali Bhutto declared, "If India builds the [atom] bomb, Pakistan will eat grass or leaves, even go hungry, but we will get one of our own."[48] This statement became a cornerstone of Pakistan's nuclear policy and served as a North Star for decades to come. Moreover, North Korea has

[47] Mazarr, Michael J., Ashley L. Rhoades, Nathan Beauchamp-Mustafaga, Alexis A. Blanc, Derek Eaton, Katie Feistel, Edward Geist, Timothy R. Heath, Christian Johnson, Krista Langeland, Jasmin Léveillé, Dara Massicot, Samantha McBirney, Stephanie Pezard, Clint Reach, Padmaja Vedula, and Emily Yoder, *Disrupting Deterrence: Examining the Effects of Technologies on Strategic Deterrence in the 21st Century* (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA595-1.html.

[48] Khushwant Singh, "Foreign Affairs Pakistan, India and The Bomb," The New York Times, p. 21, July 1, 1979, https://www.nytimes.com/1979/07/01/archives/foreign-affairs-pakistan-india-and-the-bomb.html.

employed technology in its pursuit of a substantial nuclear arsenal to coerce its neighbors[49] and prevent domination by the United States.[50]

For decades, technological progress has enhanced both offensive and defensive capabilities, thereby reinforcing strategic deterrence. The development of intercontinental ballistic missiles, dual phenomenology, and variable-yield nuclear warheads exemplifies the significant impact that technological advancements have had on the deterrence strategies employed by major powers. Currently, the emergence of AI-enabled weaponry, hypersonic capabilities, and space-based attack vectors may reduce warning and decision times, thereby generating unpredictable dynamics that could potentially lead to escalation.[51] Quantum technologies may one day render today's encryption or stealth obsolete, upending information security and jeopardizing long-range strike abilities. Moreover, biotechnology may enable the development of new forms of genetically engineered bioweapons that will be more difficult to detect, attribute, and deter.[52]

However, according to President Trump, "The threat of attack by ballistic, hypersonic, and cruise missiles, and other advanced aerial attacks, remains the most catastrophic threat facing the United States."[53] While ballistic missile defense offers countries the ability to "deter—and defend its citizens and critical infrastructure against—any foreign aerial attack on the Homeland,"[54] it may also enhance the state's ability to control escalation. Some experts posit that technological innovation now exists to create a "Golden Dome," a practical effort that will enhance deterrence and counter Russian and Chinese regional "theories of victory."[55] Others, however, argue that the Russians and Chinese are "going to build better offenses so they can overcome these defenses," perhaps igniting a new kind of arms race.[56]

---

[49] National Intelligence Council, "North Korea: Scenarios for Leveraging Nuclear Weapons Through 2030," *NIE 2023-00262-B* (Washington, D.C.: National Intelligence Council, January 2023), https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-NIE-North-Korea-Scenarios-For-Leveraging-Nuclear-Weapons-June2023.pdf.

[50] Doug Bandow, "North Korea Needs the Bomb to Protect Itself from America," *Cato Institute*, July 7, 2021, https://www.cato.org/commentary/north-korea-needs-bomb-protect-itself-america.

[51] Adam Lowther and Curtis McGiffin, "America Needs a 'Dead Hand'," *War on the Rocks*, August 16, 2019, https://warontherocks.com/2019/08/america-needs-a-dead-hand/.

[52] Yelena Biberman, "Deterrence in the Age of Weaponizable Biotechnology," *Georgetown Journal of International Affairs*, June 4, 2025, https://gjia.georgetown.edu/2025/06/04/deterrence-in-the-age-of-weaponizable-biotechnology/.

[53] Donald J. Trump, Executive Order 14186 of January 27, 2025, "The Iron Dome for America," *Code of Federal Regulations,* Title 3 (2025), p. 8767, https://www.federalregister.gov/documents/2025/02/03/2025-02182/the-iron-dome-for-america#page-.

[54] Hannah D. Dennis, "The Golden Dome (Iron Dome) for America: Overview and Issues for Congressional Consideration," Congressional Research Service (CRS) Insight, No. IN12544 (Washington, D.C.: Congressional Research Service, April 16, 2025), p. 1, https://www.congress.gov/crs_external_products/IN/PDF/IN12544/IN12544.1.pdf.

[55] Keith B. Payne, "Why Does America Need Golden Dome?," *Information Series,* No. 628 (Fairfax, VA: National Institute Press, June 18, 2025), https://nipp.org/information_series/keith-b-payne-why-does-america-need-golden-dome-no-628-june-18-2025/.

[56] Christy Lee, "Analysts: American Iron Dome reduces nuclear coercion but drives arms race," *Voice of America*, February 04, 2025), https://www.voanews.com/a/analysts-american-iron-dome-reduces-nuclear-coercion-but-drives-arms-race/7963461.html.

When it comes to deterrence, technology has been and will continue to be both a sword and a shield.

Future deterrence strategies and force postures must consider not only the destructive potential of high-tech weapons but also the strategic ambiguity, scientific surprises, and cross-domain threats posed by emerging technologies. As rapid innovation blurs traditional boundaries between nuclear and non-nuclear kinetic, cyber, space, and informational domains, adversaries gain new opportunities to exploit uncertainty, achieve asymmetric advantages, and complicate attribution. Technologies such as artificial intelligence, autonomous systems, hypersonics, quantum capabilities, and nuclear expansion introduce new risks that can outpace existing warning systems, threaten command-and-control structures, challenge political will, and undermine confidence in deterrence stability.

In this environment, integrating advanced technologies into strategic deterrence is crucial. Such integration can boost military strength, improve resilience, and help maintain the ability to anticipate, absorb, and counter emerging threats or follow-on attacks. Effectively using innovative technologies to oppose emerging technologies is likely to become a key principle of future deterrence. Countries that can master, exploit, and coordinate one or the other will be better equipped to defend national interests and protect their homeland in an era of rapidly advancing technology.

Conclusion

Technology is no longer merely a support mechanism for the traditional instruments of national power, the DIME; it has become a form of national power in its own right. It influences every aspect of statecraft, including military dominance, economic performance, diplomatic influence, cyber operations, strategic resilience, and deterrence. Nations that proactively embrace, invest in, and strategically oversee their technological capabilities will define the future global order. In his 2022 National Security Strategy, President Biden admitted the dominant role technology has in America's grand strategy: "Technology is central to today's geopolitical competition and to the future of our national security, economy, and democracy. U.S. and allied leadership in technology and innovation has long underpinned our economic prosperity and military strength. In the next decade, critical and emerging technologies are poised to retool economies, transform militaries, and reshape the world."[57]

Technological leadership acts as a "power amplifier," boosting military strength and driving economic growth through innovation, automation, and data control, while also expanding global influence and diplomatic power, and strengthening national resilience, prestige, and attractiveness. Countries leading in advanced technology hold greater influence by controlling key modern drivers: information, communication, defense, and manufacturing. In the digital world, high-tech dominance provides a strategic advantage, becoming a new form of international power.

[57] Joseph R. Biden, *National Security Strategy* (Washington, D.C.: The White House, October 2022), p. 32.

Countries possessing advanced technology and the willingness to deploy it will wield greater national power than those that lag behind or lack either one. Technology, as a fundamental instrument of national power, can both unify and augment the DIME framework comprehensively. Nevertheless, technology must also be directed towards advancing national objectives directly, functioning as its own instrument, supported by the DIME, thus evolving the framework to the DIMET.

As the world enters the era of "techno-strategic" power, technology has become a decisive instrument of national power, essential for shaping geopolitical relationships and the global economy. "Winners in the tech race will shape the international order, while losers will sit on the sidelines, unable to ensure their survival, let alone their prosperity."[58] As great power competition intensifies, nations must actively harness technology as a strategic power asset––an instrument to wield in its own right. State leaders in innovation will shape the international order, while laggards risk marginalization and dependence. Technological dominance is now the core foundation on which all other tools of national power rely. It influences the pace, authority, and information advantage, transforming the efficacy of diplomacy, the value of economics, and the effectiveness of military potency.[59] Technology, once a mere element of the DIME framework, now stands as a pillar of national power, marking the era of DIMET, where technological dominance shapes prosperity and preeminence on the global stage.

Colonel Curtis McGiffin (U.S. Air Force, Ret.) is currently a Visiting Professor at Missouri State University's School of Defense and Strategic Studies Graduate Program in Washington, D.C. He is also the Vice President for education at the National Institute for Deterrence Studies. He has 30 years of total service in the USAF. The views expressed in this article are those of the author only and do not necessarily reflect the views of Missouri State University or any other organization with which the author may be affiliated, past or present.

[58] Caitlin Lee, "Winning the Tech Cold War," RAND Commentary, August 17, 2023, https://www.rand.org/pubs/commentary/2023/08/winning-the-tech-cold-war.html.

[59] Zachary S. Ford, Session 4 Paper Review, Missouri State University, DSS 715 course, October 16, 2025.