# US National Security in a New Era of Intense Global Competition

The Honorable Zachary J. Lemnios

STEPS: SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 6, 2022

STEPS (Print) ISSN 2158-3854 STEPS (Online) ISSN 2153-3679

STEPS (2022) 6:8-19





#### Copyright © 2022 by Potomac Institute for Policy Studies

STEPS: Science, Technology, Engineering, and Policy Studies is published by Potomac Institute Press of the Potomac Institute for Policy Studies.

**Disclaimers:** The Publisher, Institute and Editors cannot be held responsible for errors or any consequences arising from the use of information contained in this publication; the view and opinions expressed do not necessarily reflect those of the Publisher, Institute and Editors. The Potomac Institute is non-partisan and does not take part in partisan political agendas.

**Copyright Notice:** It is a condition of publication that articles submitted to this magazine have not been published and will not be simultaneously submitted or published elsewhere. By submitting an article, the authors agree that the copyright for their article is transferred to the Potomac Institute Press if and when the article is accepted for publication. The copyright covers the exclusive rights to reproduce and distribute the article, including reprints, photographic reproductions, microfilm, or any other reproductions of similar nature and translations.

Access to STEPS is available free online at: www.potomacinstitute.org/steps.

US National Security in a New Era of Intense Global Competition

The Honorable Zachary J. Lemnios Member Board of Regents, Potomac Institute for Policy Studies



# **Elements of Great Power Competition**



#### A New Era

The United States and China are in a great power competition that will have profound impact on the national security and economic security of both countries for decades. <sup>1,2</sup> This competition aligns across interdependent economic, military, and political vectors. At the core, this is a competition of ideals and governance. But unlike the 20th century Cold War competition with the Soviet Union, the competition with China involves new challenges. The resulting tension between the US and China has opened a new era requiring a new national security framework. <sup>3,4</sup>

In the past, the United States has confronted the need for a complete transformation in the national security environment. For example, after World War II and the proliferation of nuclear weapons capabilities, the nation undertook Project Solarium and the Project Charles Air Defense Study to define a new national security operating model to contain the Soviet Union.<sup>5</sup> The competition with China poses an equally significant challenge now.



## Made in China 2025

## LOCALIZE AND INDIGENIZE

Promotion of indigenous innovation to develop indigenous technologies, IP, and brands.

## **SUBSTITUTION**

Substitution by domestic production as a strategic imperative once dependence on foreign technology has been reduced.

### CAPTURE GLOBAL MARKET SHARE

Capture domestic and international market share across MIC2025 industries and technologies after developing or acquiring its own technology.

#### **KEY SECTORS**

- New information technology
- High-end numerically controlled machine tools and robots
- Aerospace equipment
- Ocean engineering equipment and high-end vessels
- High-end rail transportation equipment
- Energy-saving cars and new energy cars
- Electrical equipment
- Farming machines
- New materials, such as polymers
- Bio-medicine and highend medical equipment

Source: The People's Republic of China State Council, "Made in China 2025 Plan," May 19, 2015.

## **Economic Competition**

The United States and China are in a fierce rivalry spanning a broad range of global markets and complex global supply chains. In 2020, US goods imports of \$435 billion and exports of \$125 billion reflect a trade imbalance with China. Persistent trade imbalances of this magnitude are unsustainable. This is caused by a complex competition in which the playing field is skewed and can lead to global market instability. Our companies and supply chains are interrelated. We depend upon each other's markets and host each other's companies.

The "Made in China 2025" plan, published in 2015, is China's ten-year plan to reduce China's dependence on foreign technology and to promote China's technology position in the global marketplace.<sup>6</sup> China is focused on leading ten key high-tech industries (see the "Made in China 2025" figure above). Particular technology areas of competition with the US include information technology, robotics, new materials, and aerospace equipment. This plan is structured to raise the Chinese domestic content of core components and materials to 70% by 2025. The plan is the foundation of China's economic competition.

The initial salvo for strategic industry leadership began with 5G wireless-telecommunications, as part of the "new information technology" sector. This is the entry point to the global digital and cyber-physical infrastructure with the opportunity to control the network infrastructure. This is also the path to position China as a "first mover" in training artificial intelligence (AI) algorithms on massive global data, driving AI to the network edge and accelerating digital transformation across many industries.<sup>7</sup>

As a result, China is driving the development of technologies in the 5G telecommunications sector, led by its private sector companies Baidu, Alibaba, Tencent, Huawei, and ZTE (Zhongxing Telecommunications Company Ltd.). While there are over 200 Chinese companies listed on US stock exchanges with a total market capitalization in excess of \$2.2 trillion, Huawei and ZTE have been the subject of special scrutiny.8 In late 2019, the Wall Street Journal reported that Huawei had access to as much as \$75 billion in support from the China state government.9 In July 2020, the US government officially designated Huawei and ZTE as threats to US national security, because of their close ties to the Chinese Communist Party and China's military apparatus and their legal obligation to cooperate with China's intelligence services. More recently, White House Executive Order 13959 identified 59 Chinese entities for which US investments are banned by the Treasury Department. 10

The "new information technology" sector of the "Made in China 2025" plan also depends on advanced semiconductor technology. State-of-the-art-microelectronics requires a complex supply chain with specialized technical talent and massive capital investments. Manufacturing facilities (fabs) are benchmarked by semiconductor wafer size (measured in millimeter in diameter), manufacturing volume (wafers/ month) and smallest printed geometric feature (nanometers). Today's state-of-the-art products are manufactured on 300mm wafers at 5nm geometries. At the end of 2018 there were 112 production-class fabs globally utilizing 300mm wafers.<sup>11</sup> The global industry is projected to add at least 38 new 300mm fabs by 2024. Of these, Taiwan is expected to add 11 large-volume fabs, and China will add 8 to account for half of the global 300mm large-volume fabs by 2024. To support this, the China state government has established an investment fund of \$150 billion to finance mergers and acquisitions for companies and technologies in the semiconductor industry.12

As a result, China is poised to successfully compete in the semiconductor sector. China is making significant investments and now has 13% of the global fabless market, up from 5% in 2010.<sup>13</sup> The Chinese semiconductor manufacturing sector has seen an average compound growth rate of nearly 25% since 2014.<sup>14</sup> Design of semiconductors is also making significant progress in China. In 2019, China's semiconductor design sector reached a level that surpassed Taiwan, making China the second-largest design industry cluster after the United States globally. China's share of semiconductor design grew from 3.6% in 2004 to nearly 43% in 2019.<sup>15</sup> Leadership in semiconductor design and manufacturing implies leadership in new information technology, which is but one sector of emphasis of the "Made in China 2025" plan for economic competition.

The US has begun to recognize the criticality of America's supply chains and the economic security and national security challenge posed by foreign disruption. The recent White House review on this topic launched a comprehensive whole-of-government effort to strengthen domestic competitiveness and supply chain resilience across four critical sectors: (1) semiconductor manufacturing and advanced packaging, (2) large capacity batteries, (3) critical minerals and materials, and (4) pharmaceuticals and active pharmaceutical ingredients.<sup>16</sup>

To answer the challenge of economic competition, the US will need to greatly improve its ability to understand the national security implications of foreign economic developments and to provide better security for its own developments. New technologies can assist in addressing the national security implications of economic competition. Pursuit and integration of these directions into a comprehensive national defense apparatus might require new agencies and resources. Technology concepts, adapted from the commercial sector, could open new approaches to respond to economic challenges. These include the following.

 Development and utilization of real-time national financial models to provide early warning indicators of critical supply chain disruptions, on both sides, thereby playing long-term offense and defense. Statistical models applied to open-source financial and industry data are being used today by companies to optimize global supply chain efficiencies and costs. With additional data, these could be used at a national level to preemptively forecast supply chain risks and economic impact and to make decisions to secure critical supplies for national needs.

- Development and utilization of macroeconomic models to forecast foreign government involvements across global markets, and to provide early indicators of potential disruptive activities. For example, modeling mainland China's potential economic futures with Taiwan would help to better understand and shape the region to thwart conflicts. Monte Carlo simulation techniques exist today to model thousands of scenarios and alert on early warnings and emerging scenarios, and to game threats and optimize responses. Analysts today monitor military threats; future analysts will use tools to analyze economic threats.
- Utilization of blockchain, watermarking, design partitioning, and hardware obfuscation security approaches. Such approaches, emerging for use in commercial venues, can mitigate risks of counterfeiting, intellectual property theft, and tampering. A national approach is needed to integrate in-line data from millions of sensors across complex global supply chains with comprehensive analysis of the data to model and deploy strategies to defend the economic homeland.

### Military Competition

Military strength and resiliency comprise a second element of competition. China's strategy of "Military-Civil Fusion" poses significant challenges for the US and our allies. China's Military-Civil Fusion development strategy has leveraged a whole-of-government approach to achieving parity with the United States in several military areas, including air defense systems, land-based conventional ballistic and cruise missiles, and shipbuilding.<sup>17</sup> The prospect of China developing and fielding advanced military capabilities by integrating research across its commercial sector with its military and defense industrial sectors, is a key element of this great power competition.

The Communist Party of China (CPC) Central Committee has established the goal of building a "fully modern military" by 2027, with the capability to defend national sovereignty, safeguard against security threats in the western pacific region, and protect overseas development interests as China's global economic presence grows.<sup>18</sup> These plans include accelerating its integrated development in "mechanization," "informatization," and "intelligentization," comprehensively strengthening military training and preparation. A recent report outlines the pace and impact of China's military modernization, with a focus on the People's Liberation Army's (PLA's) strategy to use science and technology for military purposes.<sup>19</sup>

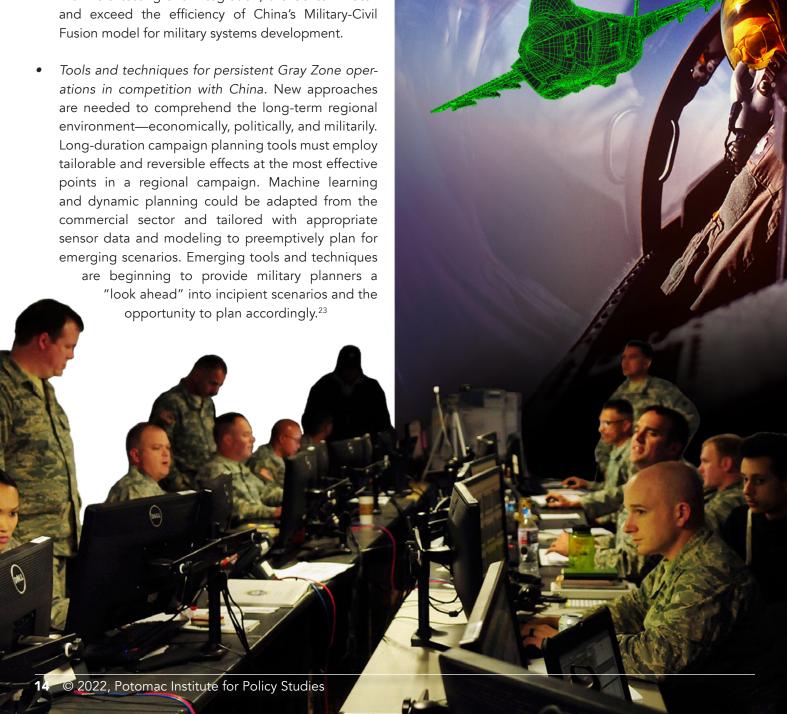
Over the past decade, China has made significant progress in key technical areas including radio frequency systems, electronic warfare, hypersonics, and more recently quantum computing. As an example, Chinese researchers recently published an approach to network hypersonic weapons into a smart swarm for coordinated attacks.<sup>20</sup> The concept opens the alarming prospect of a saturation attack that would be difficult to counter, even with future air defense systems. Particularly alarming are the references that the Beijing Institute of Technology authors cited, including the Raytheon Tomahawk Cruise Missile (RGM/UGM-109) Technical Manual and System Description.

In the field of quantum technologies, the Intelligent Perception Technology Laboratory of the 14th Institute of China Electronics Technology Group Corporation (CETC) announced China's first quantum radar system in 2016 and displayed a mockup at the Zhuhai Airshow in 2018.<sup>21,22</sup> More recently, China opened the world's largest quantum research center to push the frontier of quantum computing. The National Laboratory for Quantum Information Sciences, a \$10 billion four-million square foot facility, has programs in quantum sensing, self-contained navigation, quantum computing, and quantum communications.

The United States has relied upon US technology leadership, unmatched engineering talent, and highly trained military personnel to build, deploy, and operate the world's most technologically advanced military. With the development and availability of key advanced technologies from the commercial sector, nation state competitors and non-state actors now have equivalent access, eroding the technology overmatch to which our nation has grown accustomed. To recover and maintain technology superiority for military systems, new emphasis needs to be placed on defense technologies, involving new research

and development agencies and approaches. Some concepts that should be explored prior to establishing such centers include the following.

• Faster movement toward reinvigorating US technology development demonstrating and fielding advanced technology in key areas. The Department of Defense can do so by expanding its Federally Funded Research and Development Centers (FFRDCs) and Department Laboratories, or instituting new ones, in partnership with US industry. By using new partnership models to engage in a campaign of continuous development with field testing and integration, the US can match and exceed the efficiency of China's Military-Civil Fusion model for military systems development.



A new deterrence strategy to address a combined Nuclear, Chemical, Biological, Cyber (NCBC) threat, expanding the range of highest priority threats requiring national capabilities. New deterrence, detection, and countermeasure techniques are needed considering that any combination of NCBC employment could present an existential threat to the United States. Natural or man-made, the COVID-19 pandemic resulted in millions of deaths and crippled the world's economy for many months. Fielding a global NCBC early warning capability is essential as engineered pathogens could have a similar impact. Deploying such a capability globally with allies and partner nations requires US global leadership.

### Political Competition

Political strength is the third, and perhaps most challenging, element of the great power competition between the United States and China. China has harnessed its political and military strength in the South China Sea on a Gray Zone strategy. This has become an operati-onal domain characterized by a long campaign of low threshold actions to achieve long-term strategic objectives without crossing the threshold of military confrontation.<sup>24</sup> It includes elements of Hybrid Warfare<sup>25</sup> and Soft Power.<sup>26</sup>

China and Russia are increasingly using Gray Zone means to achieve their objectives without direct military engagement and below the level of war.<sup>27</sup> The Gray Zone is growing rapidly in the South China Sea, where China is using coercion, intimidation, propaganda, and manipulation to expand its position in the region.<sup>28</sup> China has built an artificial island chain, reclaimed disputed land, militarized islands, and is using legal arguments and diplomatic influence to expand its position.

In early 2020, China's State Council established two new districts in Sansha City, a prefecture-level city headquartered on Woody Island which governs the bulk of China's territorial claims in the South China Sea. This development will expand China's control over the region and further complicate political and diplomatic dynamics.

While military deterrence is essential, the United States and our allies need a set of new technical and operational capabilities to operate in a persistent and multidomain Gray Zone.29,30

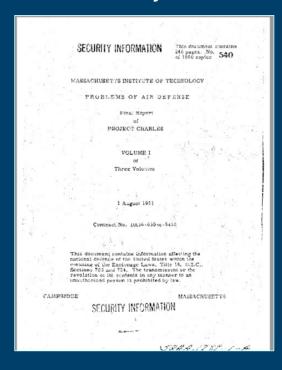
Prevailing in a prolonged political competition with China requires the United States to develop and implement a whole-of-government approach to integrate economic, political, and military signatures, indications, and warnings. The following technical approaches should be explored and deployed.

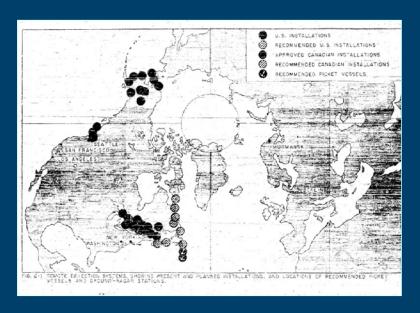
- Intelligence, advanced forecasting, and decision support capabilities to detect, tailor, and preemptively plan economic, political, and military actions. Political actions can involve influence operations, marketing, competitive assistance, as well as tariffs and sanctions. Techniques can be adapted from the commercial sector to process live-stream data and alert on emergent behavior.
- Whole-of-government synchronous strategic messaging and information operations using approaches from the commercial sector. Social media has opened a new strategic communication channel for enabling red teaming against a range of simulated actions and responses from China. The development of multi-domain models could open the prospects of predictive risk assessment to extend our economic, political, and military options.
- New technical approaches to detect and protect government, enterprise, and private information that are increasingly entangled and increasingly vulnerable. Developing an effective layered information defense system is a daunting challenge. In addition to protecting critical infrastructure, effective capabilities would position the United States as a leader in information security, countering China's cybersecurity laws that permit the government to obtain any information that they deem has an impact on Chinese security.

## Peer-level Challenges of the Past

The US has faced peer-level national challenges in the past. Our peer-level competition with China on the economic, military, and political levels is no less daunting than the confrontation with the Soviet Union some 70 years ago.

# Project Charles Early Warning Architecture





The Soviet Union detonated its first atomic bomb in September 1949, and by 1951, the Korean War had begun as a proxy war with the Soviet Union. With growing geopolitical tension between the United States and the Soviet Union, the US confronted the possibility of a devastating surprise attack.

In response, the US completely revamped the defense system in the 1950s and beyond. A strategy of containing the Soviet Union was devised, and more importantly, enacted. For example, the Project Charles Air Defense Study, begun in 1951, was more than a study, but a four-month effort to design short- and long-term development of an early warning system for attacks that might emanate from the Soviet Union.<sup>31</sup> It led to the formation of MIT Lincoln Laboratory,<sup>32</sup> and engaged scientists and engineers from across industry and academia, and military liaisons, to outline many of the principles of today's air defense systems. They focused on early warning target detection and discrimination, threat interception, and command and control. Project Charles working groups were briefed on Soviet strategic capabilities and visited military operational field sites. They evaluated approaches to detect a small number of threat aircraft buried in a large constellation of commercial aircraft, and the importance of field testing a prototype system comprised of a network of small radars connected to a central computer at a command center.

With urgency to quickly counter the Soviet threat, the Project Charles Study outlined a development program that included short-term extensions of current technologies and longer-term plans to leverage an "electronic high-speed digital computer...and the revolution that the transistor will bring about in electronics to open up quite new possibilities in aircraft and weapon control."<sup>33</sup> These options were available because the United States led the world in radar, electronic warfare, communications, electronics, display, and other key technologies needed to deploy an initial early warning system.<sup>34</sup>

Resulting contracts and development, called "Project Lincoln," led to the Semi-Automatic Ground Environment (SAGE) system and the Distant Early Warning system. Rand Corporation, another Federal Contract Research Center, was involved in developing the programming for the sophisticated mainframe computer, and MITRE was founded in 1958 to operate and expand the system.<sup>35</sup> SAGE protected the United States into the 1980s.<sup>36,37</sup>

The use of federally funded research and development centers (FFRDCs) was established for challenges that cannot be met solely through the commercial sector. As national security threats evolved from bombers to intercontinental ballistic missiles, FFRDCs focused their efforts on a major initiative in ballistic missile defense. This began in the late 1950s, expanded in the 1960s and grew significantly in the 1980s with President Reagan's establishment of the Strategic Defense Initiative.<sup>38</sup> This work was critical to US national security and led to software and hardware concepts which are in use today, including collection and analysis of test data, high fidelity simulations, critical discrimination techniques, and design of new radar and infrared sensors.

## Lessons Learned from the Cold War Competition

We can learn from the competition between the United States and the Soviet Union in the second half of the 20th century. The Cold War was a competition between liberal democracies and communism, just as we now confront a competition with a different form of government. The Soviet Union's self-proclaimed world power centered on its massive number of ballistic missiles with nuclear munitions. Without its ballistic missiles, the Soviet Union could not project power very far beyond its regional boundaries.

In our current confrontation, the protagonists are, as before, very careful not to engage with each other in direct military confrontation. Just as the Cold War lasted about 40 years, the current competition is likely to last for multiple decades. The United States, with superior technology, won the Cold War. The US competed with the Soviet Union in a technology race to directly challenge their missile force with developments such as the Strategic Defense Initiative. The Soviet Union was in no position to engage and thus, conceded defeat when President Yeltsin dissolved the Soviet Union on December 8, 1991.39

## Interdependent Elements of this Great Power Competition

While military, economic, and political interdependencies are not new, we are now in competition with a peer nation where military strength alone is not sufficient to succeed.

In a similar manner, new technical capabilities and operational concepts are needed to prevail in a long-term great power competition with China, which may also last for decades. In each element of great power competition, there are possible solutions, involving technology, policies, and investments in research and development.

But in developing solutions, we must recognize the interdependencies and interoperability of these capabilities. Responses in one area will affect other areas, and to prevail, we must respond in all areas. Each of these domains-economic, military and political-have unique signatures and can be competitively modeled. But it is the interplay between domains that is critical. The challenge is to decompose this into a cross-domain model, fed by live-stream data to provide insight for preemptive courses of action. This is a messy, loosely structured, data-rich environment with a host of potential threats and ambiguities. It is also the environment we must understand and in which we must prevail.

#### A Call to Action

The United States and China are in a protracted great power competition that will have profound impact on the national security and economic security of both countries for decades. The complex and interdependent economic, military, and diplomatic tension between the US and China has opened a new era of national security challenges. Just as superior technology allowed the United States to prevail against the Soviet Union, technology solutions will be the deciding factor in our current competition.

And yet, our current structures for acquiring and applying technologies are inadequate for the challenges posed by the new great power competition. The Defense Industrial Base designs and builds weapon systems with advanced technology. The commercial sector is remarkably effective at developing high technology commercial goods. Private industry, often with government help, invests in technologies for health care, transportation, energy, space, materials, and manufacturing. Basic research capabilities and advancements are strong. What is lacking, however, is an integrated approach to addressing the interlocking economic, military, and political competition with those who have developed their own capabilities and technological progress.

## Interdependent Cross-Domain Capabilities are Essential Supply Chain Forecasting Macroeconomic **Economic** & Red Teaming Forecasting Strength Nuclear, Chemical, Scenario Projection Biological, Cyber (NCBC) Military **Political Red Teaming** Deterrence Strength Strength Information Security Gray – Zone Operations Technology Leadership Strategic Messaging and Information Operations

A focused executive commission is urgently needed to frame this multi-domain challenge, to include talent from across industry, academia, government, and the military. Like Project Solarium and Project Charles, the study needs to involve the most senior, trusted, and intellectual experts in the nation. The study's "Terms of Reference" should be succinct and blunt: How can the United Stated prevail in the great power competition with China? What new capabilities do we need? What are the operational models and how are these integrated across whole-of-government? Bold ideas merit exploration.

This will not be a study typically conducted by agencies today. This commission needs to have an impact. Both short-term and long-term recommendations must lead to action, both executive and legislative.

The results are certain to support a restructuring of our technology development enterprise. Near-term fixes will be proposed to leverage novel technologies. But long-term developments will also be needed. New long-term institutions

are likely to be proposed, including new FFRDCs and new government laboratories. These might be carved from existing institutions, but they also might require new centers to support evolving needs. A pipeline of human capital and infrastructure resources will be necessary. Support to the military's combatant command at United States Indo-Pacific Command (USINDIOPACOM) will be critical to develop and validate cohesive econometric/military/political models that can be integrated through operations. Other combatant commands and collaboration with allies will be equally important. New weapon systems for deterrence will be but one aspect of fortifying a great power competition in the economic, military, and political domains.

The United States has risen to grand challenges in the past, but only by taking bold and decisive steps. Those actions served to prevail in the past, but only after commitments that lasted decades. Today's challenges require similar kinds of commitments. It is time to frame the problem, propose approaches, and make those commitments.

#### **Endnotes**

- Anthony H. Cordesman, Chinese Strategy and Military Forces in 2021, Center for Strategic International Studies June 7, 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210607\_Cordesman\_Chinese\_Strategy. pdf?fG7hUZdWUVJgaJzyC4E9Qj1m3w13SfjQ.
- National Defense University Press, PRISM 8 (4) June 2020, https://ndupress. ndu.edu/Portals/68/Documents/prism/prism\_8-4/prism\_8-4.pdf.
- 3 The Policy Planning Staff, Office of the Secretary of State, The Elements of the China Challenge, December 2020, https://www.state.gov/wp-content/up-loads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf.
- 4 F.W. Loomis, Problems of Air Defense: Final Report of Project Charles, Contract Number DA36-0039sc-5450, August 1, 1951, http://www.bitsavers.org/pdf/ mit/lincolnLaboratory/project\_charles/A800165\_Final\_Report\_of\_Project\_ Charles\_Vol\_1\_Aug1951.pdf.
- Department of State Office of the Historian, Foreign Relations of the United States, 1952-1954, National Security Affairs, Volume II, Part 1, "Paper Prepared by the Directing Panel of Project Solarium," https://history.state.gov/historicaldocuments/frus1952-54v02p1/d69.
- 6 The People's Republic of China State Council, Made in China 2025 Plan May 19, 2015, http://english.www.gov.cn/policies/latest\_releases/2015/05/19/content\_281475110703534.htm.
- 7 State Council Notice on the Issuance of the New Generation Artificial Intelligence Development Plan, A New Generation Artificial Intelligence Development Plan, July 20, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/ blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.
- 8 U.S.-China Economic and Security Review Commission, Chinese Companies Listed on Major U.S. Stock Exchanges, https://www.uscc.gov/research/chinese-companies-listed-major-us-stock-exchanges.
- 9 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," Wall Street Journal, December 25, 2019.
- US Department of the Treasury, Issuance of Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China & Related FAQs; Introduction of Non-SDN Chinese Military-Industrial Complex Companies List, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210603.
- 11 Semi, 300mm Fab Spending to Boom through 2023 with Two Record Highs, November 3, 2020, https://www.semi.org/en/news-media-press/semi-press-re-leases/300mm-fab-outlook.
- 12 U.S. Chamber of Commerce, Made in China 2025: Global Ambitions Built on Local Projections, 2017, https://www.uschamber.com/assets/archived/images/ final\_made\_in\_china\_2025\_report\_full.pdf.
- Antonio Varas, Raj Varadatajan, "How Restrictions to Trade with China Could End US Leadership in Semiconductors", Boston Consulting Group, March 2020, https://www.bcg.com/en-us/publications/2020/restricting-trade-with-china-could-end-united-states-semiconductor-leadership.
- 14 Paul Triolo, "The Future of China's Semiconductor Industry, American Affairs Spring 2021 5 (1), https://americanaffairsjournal.org/2021/02/the-future-of-chinas-semiconductor-industry.
- 15 US Department of the Treasury, Issuance of Executive Order Addressing the Threat from Securities Investments, https://home.treasury.gov/policy-issues/ financial-sanctions/recent-actions/20210603.
- 16 The White House, 100-Day Reviews under Executive Order 14017. June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.
- Office of the Secretary of Defense, Military and Security Developments involving the People's Republic of China 2020, Annual Report to Congress, August 21, 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL-PDF.
- 18 Communiqué of the Fifth Plenary Session of the 19th CPC Central Committee, October 30, 2020, http://english.www.gov.cn/news/topnews/202010/30/content\_WS5f9b6f64c6d0f7257693ea0a.html.

- 19 The National Institute for Defense Studies, NIDS China Security Report 2021: China's Military Strategy in the New Era, Nov 2020, http://www.nids.mod.go.jp/publication/chinareport/pdf/china\_report\_EN\_web\_2021\_A01.pdf.
- 20 Shixun Luo, Zhongshan Zhang, Shuai Wang, et al., "Network for Hypersonic UCAV Swarms" Science China Information Sciences 63, Article Number 140311 (2020), https://doi.org/10.1007/s11432-019-2765-7.
- 21 CETC 14th Research Institute, https://www.globalsecurity.org/military/world/china/cetc-14.htm.
- 22 "China Shows off First Quantum Radar Prototype," *Aviation Week Network* November 5, 2018, https://aviationweek.com/defense-space/china-shows-first-quantum-radar-prototype.
- 23 Chris Nott, Stephen Gordon, and Leendert van Bochoven, IBM Defense Simulation Analytical Service, December 10, 2021, https://www.ibm.com/blogs/think/uk-en/defense-simulation-analytical-service/.
- 24 George Popp, Sarah Canna, The Characterization and Conditions of the Gray Zone, NSI. Inc, Winter 2016.
- 25 Frank Hoffman, Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges National Defense University PRISM 7(4) November 2018.
- 26 Joseph Nye, "Soft Power" Foreign Policy No. 80, Twentieth Anniversary (Autumn, 1990), pp. 153-171.
- 27 Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, et al., Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War. Santa Monica, CA: RAND Corporation, 2019, https:// www.rand.org/pubs/research\_reports/RR2942.html.
- Oriana Skylar Mastro, Military Confrontation in the South China Sea, Council on Foreign Relations, May 21, 2020, https://www.cfr.org/report/military-confrontation-south-china-sea.
- 29 Defense Science Board, Summer Study on Capabilities for Constrained Military Operations, December 28, 2016, https://dsb.cto.mil/reports/2010s/DSBSS16\_ CMO.pdf.
- 30 Defense Science Board, Task Force on 21st Century Multi-Domain Effects, September 2020, https://dsb.cto.mil/reports/2020s/FINALMDEExecutiveSummary.pdf.
- 31 F.W. Loomis, Problems of Air Defense: Final Report of Project Charles, Contract Number DA36-0039sc-5450, August 1, 1951, http://www.bitsavers.org/pdf/mit/lincolnLaboratory/project\_charles/A800165\_Final\_Report\_of\_Project\_Charles\_Vol\_1\_Aug1951.pdf.
- 32 Alan A. Grometstein, MIT Lincoln Laboratory: Technology in Support of National Security (MA: Lincoln Laboratory MIT) 2011, http://www.ll.mit.edu/sites/default/ files/other/doc/2018-04/MIT\_Lincoln\_Laboratory\_history\_book.pdf.
- 33 SAGE: The First National Air Defense Network, IBM100 Icons of Progress, https://www.ibm.com/ibm/history/ibm100/us/en/icons/sage/.
- 34 SAGE: The First National Air Defense Network.
- 35 SAGE: Semi-Automatic Ground Environment, https://sage.mitre.org/.
- 36 Kenneth Shield, The Emerging Shield: The Air Force and the Evolution of Continental Air Defense, 1945–1960 (Washington, DC: Office of the Air Force History) 1991, https://archive.org/details/TheEmergingShield/page/n23/mode/2up.
- G.O. Ekstedt, The DEW Line Story (Western Electric Company), https://www.beatriceco.com/bti/porticus/bell/pdf/dewline.pdf.
- 38 President Ronald Reagan, Address to the Nation on Defense and National Security March 23, 1983, https://www.reaganlibrary.gov/archives/speech/address-nation-defense-and-national-security.
- 39 Michael Dobbs, "Slavic Republics Declare Soviet Union Liquidated," Washington Post Foreign Service December 9, 1991, Page A01, https://www.washingtonpost. com/archive/politics/1991/12/09/slavic-republics-declare-soviet-union-liquidated/c15d0d5d-7e03-42c6-b1a1-6eb0568a8c80/.