Introduction
Navigating Uncharted Territory in the Technological Era

Joseph S. Nye, Jr.
Co-Chair,
Aspen Strategy Group

Condoleezza Rice
Co-Chair,
Aspen Strategy Group

Nicholas Burns
Director,
Aspen Strategy Group

In August 2018, the nonpartisan Aspen Strategy Group (ASG) convened its thirty-fourth annual meeting in Aspen, Colorado. Over the course of three days, ASG members and invited experts from government, universities, think tanks, and the private sector debated the impact of dramatic technological change over the next decade on American national security. Our conversations covered a wide breadth of emerging technologies—artificial intelligence, machine learning, quantum computing, and biotechnology—and the challenges they pose to America's military, the intelligence community, U.S. economic power, and democratic institutions. Our group grappled with the central dilemma of how the U.S. government can harness these technologies—developed primarily in the private sector and research labs—to compete with China and other adversaries in the years ahead.

How do we reinvigorate America's innovation triangle of government, the private sector, and academia, which was so crucial in creating the country's global technological lead over the past half-century? How do we prepare the American workforce for the perpetual disruption of technology and the automation of a growing number of jobs? What steps must we take to modernize the U.S. defense apparatus and military to face future threats? How should the U.S. government respond to cyber and disinformation tactics perpetrated by foreign actors? Most critically, if the U.S. fails to respond to these dynamic changes, will it lose its place as the world's strongest military power in the years ahead?

These questions frame this book as they will our national debate on the future of America's power in the world. Our authors explore them further in the subsequent chapters. While these issues have been around for some time, the pace and scale of the change make it ever more urgent. Recognizing technology's tremendous influence on the key pillars of American power, we left Aspen with three overarching observations of how the U.S. government must respond to this transformative era.

I. The Necessity of Defense Modernization

One of the most pressing national security issues is military modernization and ensuring the U.S. defense structure is prepared for these dramatic future challenges. This modernization requires a unified, sustained vision that encompasses not only the U.S. Defense Department and military, but the Congressional leadership in both parties, the current and future Presidential administrations, and the private sector. The Administration must reevaluate the U.S. defense budget and procurement processes, rethink its human capital strategy, and face the looming ethical considerations of lethal autonomous weapons systems.

The U.S. Defense Budget and Procurement Process

In June 2018, the Senate approved one of the largest defense budgets in modern American history—nearly $716 billion. The major challenge for our country, however, is how to spend it wisely. The U.S. military continues to allocate much of its annual budget to building, operating, and maintaining large, manned, and expensive systems, while a minute percentage of the budget—less than 1 percent—is allocated toward science and technology research. Some of our participants argued that the defense budget must begin to reflect America's future military needs. Military modernization means shifting away from expensive, manned systems toward large quantities of smaller, dispersed systems that are unmanned, expendable, and as autonomous as possible. The Pentagon needs to incorporate emerging technologies, or it risks losing its advantage among near-peer competitors.

The defense procurement system must also be modernized to reflect the rapid pace of technological advancement. The U.S. cannot wait for years to acquire readily available technology in the private sector. The Pentagon must build a sustained partnership with the technology sector, including companies in Silicon Valley. Open dialogue is key to establishing trust between these two juxtaposed worlds. For the Defense Department, this relationship is imperative. The Pentagon must collaborate with industries to acquire the latest, most innovative cyber and artificial intelligence (AI) technologies.

The major tech firms in turn, must be willing to work with the Pentagon to ensure our military has the benefit of the most advanced technological break throughs in AI, quantum computing, and other areas.

Human Capital Strategy

The future needs of the U.S. military go beyond the procurement of advanced technology. The military does not yet have nearly enough technical specialists in its ranks to lead the Pentagon into the digital age.

The Defense Department must create pathways and incentives for young, talented technologists and engineers to join its ranks. The Defense Department could institute, for example, a talent exchange program with private sector technology firms, similar to the initiative former Secretary of Defense Ash Carter, one of our ASG members, proposed in 2016. This would give commercial sector technologists a sense of the Defense Department's mission and day-to-day operations.

This effort, ongoing in certain departments within the U.S. defense structure, must be urgent and widespread. The Defense Department needs to prepare its ranks to ensure the continued security of America's military personnel and the nation itself.

Ethical Considerations

The issue of maintaining a "human in the loop" is a more nuanced debate. The military already deploys systems with a high degree of autonomy. The Defense Department can and should work with private firms to ensure ethical considerations are embedded in the planning for unmanned systems. This process will be ongoing, and the U.S. government should continue to debate these ethical considerations as artificial intelligence and machine learning technologies advance and permeate every facet of America's defense structure.

II. The Future Character of Conflict

Our discussions in Aspen touched heavily on the nature of future conflict and the potential responses of the U.S. government to these emerging threats. Beyond the threat of cyberattacks from state rivals and non-state actors, the U.S. will continue to face an onslaught of devastating disinformation campaigns and hybrid warfare tactics of the type developed by the Russian government against the U.S. during the 2016 Presidential election and since then. The U.S. government should work with American allies and other international partners to counter information operations and cyber threats and defend against these multi-dimensional attacks.

Warfare in the Cyber Domain

To prepare for continued conflict in the cyber domain, the U.S. government must adopt a cyber strategy that includes both rules of engagement for offensive measures and strategies for defending the country's national security and critical infrastructure. This task is made more difficult by the rapid diffusion of technology. The U.S. must presume that whatever technology it develops will eventually become available to all, including less powerful nations, non-state actors, and even individuals.

As the prevalence of cyber conflict continues to surge, the U.S. must establish clear declaratory policies, which outline the country's measured response to cyberattacks and information operations, to deter aspirant cyber attackers.

China has stated its intent to be the leader in A.I. in the near future. Washington should adopt an ambitious program to respond to China's digital aspirations. Tensions between the two nations will endure, and America cannot afford complacency. The U.S. must establish a clear, long-term vision for AI and cyber development—a response to China's "Made in China 2025" strategic plan. This vision should encompass not only the Defense Department and military, but commercial technology firms and research institutions as well.

Collaborating with International Partners

To adapt and thrive in this challenging new environment, the U.S. must rely on its wealth of international partners and allies. By cooperating and sharing data, the U.S. and its allies can begin to learn from and counter cyberattacks perpetrated against them. The U.S. should lead NATO in developing strategies for deterring cyber and information operations, ensuring not only its own security, but also the security of its allies. NATO must ensure that each member country fulfills the objectives set out in Article III—that all nations will "maintain and develop their individual and collective capacity to resist armed attack." This resilience must include the threat of cyberattacks and hybrid warfare tactics.

NATO allies should also continue to discuss the Article V threshold in the cyber realm. At what point will NATO member countries consider a cyber attack against one of them to be an attack against all of them? These questions are not theoretical. Hybrid warfare, executed by countries such as Russia and China, will continue to evolve and advance, pushing the limits and boundaries established by NATO member countries.

III. Reinvigorating the Innovation Triangle

Walter Isaacson's chapter in this book outlines the history and strength of America's innovation triangle. This alliance of government, universities, and the private sector was essential to the country's technological advancement since World War Two. In the midst of dramatic technological shifts, America must rely once more on this whole-of-nation approach.

Why is this triangle not functioning as it has in the past? The problem is not a lack of innovation in the U.S., but a failure of meaningful and sustained collaboration among the three pillars of the triangle. Deep mistrust permeates the relationship between Washington and Silicon Valley. The first step is to bridge these two disparate worlds. The second step is reinvigorating federal funding for research and development. The government must increase federal funding for university research labs to ensure continued American innovation and basic science research. Third, and most critically, the U.S. government must propose a strategic vision for cyber and emerging technologies that encompasses the other two pillars of the triangular alliance. This vision should include input and ideas from government officials, Congressional leaders, leading commercial sector technologists, academics, and researchers. A whole-of-nation approach requires a whole-of-nation strategy.

Future of Work

The innovation triangle is also pivotal in preparing the American workforce for continued economic disruptions caused by technology and automation. An increasing number of jobs will be subjected to automation, and Washington must work with the private sector and research institutions to help Americans adapt and thrive in this evolving workforce. Retraining workers for the digitized economy is vital, and must be vigorously endorsed by federal and state governments and widely implemented by employers. This long-term challenge goes far beyond just the economic ramifications—it poses a threat to the health and security of our civil society. An alliance of government, the private sector, and research institutions is necessary to prepare the country and its workforce for this future.

Maintaining America's Edge

This is still the dawn of the digital era. While cyber technology and artificial intelligence are in full public view, they are merely examples of what is to come. It is imperative that the U.S. government respond to the changing nature of military

technology. Military modernization must be a priority, and the defense budget must reflect the military needs of the future, both in equipment and personnel. This sustained challenge was summarized by Chairman of the Joint Chiefs of Staff Joseph Dunford, who warned Congress: "In just a few years, if we do not change our trajectory, we will lose our qualitative and quantitative competitive advantage."

In the essays that follow, technologists, career government officials, private sector leaders, and scholars dive deep into these critically urgent issues. While each chapter touches on a unique piece of the technological revolution, the central message is clear: to maintain America's technological edge for the future, we must act now.

Ash Carter's Ernest May Memorial Lecture opens this volume with historical examples of disruptive technological change, before exploring possible solutions to the dilemmas we face today.

Jason Matheny and Jack Clark's essays introduce specific digital and biological technologies that are shaping important instruments of American power and the capabilities and risks associated with these perpetually evolving landscapes.

While we strive to create the environment for successful technological innovations, we also need to understand how our home front must adapt to resolve the problems innovation creates as digitization, machine learning, and A.I. affect American lives. Diana Farrell, Edward Alden, and Penny Pritzker dedicate their pieces to understanding how these changes are affecting the Future of Work so that we can create inclusive economic growth and a sustainable labor market.

John Dowdy and Chandru Krishnamurthy delve into the future nature of conflict and how emerging technologies are fundamentally altering core defense missions and challenging existing thinking on autonomous systems. They argue for urgent modernization of our defense procurement system and a more effective partnership between the private sector and the Federal government.

Beyond the battlefield, technologies also pose serious threats to democracies and institutions around the globe. Malicious cyber and disinformation campaigns are creating a new level of hybrid warfare and "digital war zones" that we must also tackle, as Jared Cohen outlines in his chapter. Laura Rosenberger, Eric Rosenbach, and Katherine Mansted offer their proposals on the best ways for democracies to counter and survive this age of disinformation.

It is necessary to look at the larger context of the global balance of power when discussing America maintaining its technological edge. John Deutch's chapter

examines America's greatest competitor in this space—China, with its well-funded, cohesive, and long-term innovation strategy *China2025*. His chapter offers insights on how the U.S. should reimagine a clear, multifaceted innovation plan to remain competitive without undercutting our own openness and values.

Finally, Walter Isaacson argues that the underpinnings of our new strategic long-term innovation policy can be found by remembering how America first achieved its technological edge—through strong working relationships between the U.S. government, universities, and the private sector. His chapter reminds us that for the U.S. to remain on the forefront of technological developments, it must prioritize significant investments in the ground-breaking research that this requires.

Our hope is that the ideas and policy recommendations presented in this book will amplify the lessons we learned during our time in Aspen, moving them beyond our seminar table and into the classrooms, labs, offices, and homes of those dedicated to maintaining America's national security technological edge. Our future depends on it.