JANUARY 2020

TWIN PILLARS

Upholding National Security and National Innovation in Emerging Technologies Governance

By Samuel J. Brannen,
Christian S. Haig,
Katherine Schmidt,
and Kathleen H. Hicks

Report of the
Global Security Forum

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JANUARY 2020

Twin Pillars

Upholding National Security and National Innovation in Emerging Technologies Governance

AUTHORS
Samuel J. Brannen
Christian S. Haig
Katherine Schmidt
Kathleen H. Hicks

A Report of the 2019 Global Security Forum

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Acknowledgments

This report is made possible by the generous support of Leonardo DRS. The authors extend special thanks to Dr. Jason Matheny for his expert guidance in helping to frame the day-long workshop underpinning this report. The authors also owe special gratitude to workshop moderators Rebecca Hersman, Suzanne Spaulding, Tom Karako, Todd Harrison, and Stephanie Segal.

Contents

Acknowledgments III
Executive Summary VI
Foreword VII
I. Importance of Emerging Technologies Governance 1
Modernizing Governance 1
The China Challenge 3
II. Key Themes 6
Leading Across Emerging Technologies 6
Public-Private Partnerships 8
Innovation and Security 12
Emerging Technologies Workforce 12
Board, Sustained Diplomatic Engagement 13
Prepare for Inevitable Frictions and Crises 14
Conclusion 16
About the Authors 18
Appendix A: 2019 Global Security Forum Experts' Workshop Participants 19
Appendix B: 2019 Global Security Forum Scenarios 20
Scenario 1 Outline – Patient Zero 21
Scenario 2 Outline – AI(n)stability 23
Scenario 3 Outline – IoTerror 26
Appendix C: 2019 Global Security Forum Pre-discussion Questions 31

Executive Summary

In an era of global technological competition and diffusion of innovation, the United States must uphold the twin pillars of national security and national innovation. The overall success of the U.S. federal government in emerging technologies governance is at best a mixed case and is overall inadequate to the scale and stakes of the challenges and opportunities ahead.

At the 2019 Global Security Forum, national security and technology experts identified five findings to inform a more effective U.S. federal government approach to emerging technologies.

1. Expertise in emerging technologies increasingly resides outside the U.S. government. Yet, government retains its vital responsibility to recognize and respond to the greatest security, economic, and social risks presented by emerging technologies.

2. Current U.S. emerging technologies governance is uneven and highly decentralized, with some success cases but many gaps.

3. It is often impossible to forecast end-use cases for emerging technologies, placing a premium on threat detection and information sharing between the private and public sectors.

4. Tensions between governments and technology companies worldwide are rising, with increasing protectionism, localization requirements, and regulatory disharmony between the United States and even its closest allies.

5. In a globally competitive environment, restrictive export controls may slow others down temporarily but are unlikely to prevent the ultimate acquisition of any given technology. Such restrictions instead may cede market share and leverage in standards and norms setting.

Participants proposed six actions to enhance U.S. emerging technologies governance.

1. On an evergreen basis, the U.S. government should identify those “must win” technologies where primacy or parity with competitors is vital to national security. This will allow the U.S. government to more effectively concentrate efforts and resources across federal departments and agencies and operate in concert with the private sector.

2. The United States should undertake broad, sustained diplomatic engagement to advance collaboration on emerging technologies, norms, and standards setting. This will require clearer articulation of U.S. policies and standards on multiple issues.

3. To gather the understanding necessary to effectively govern emerging technologies, the U.S. government should experiment with new models and incentives for public-private partnership that create trust and enable information sharing.

4. The U.S. government should increase attention to the human dimensions of emerging technologies, from ethical questions to impacts on the workforce. This affects policy spanning K-12 education, immigration, government recruitment, vetting of non-government workers with access to powerful technologies, and much more.

5. The U.S. government should assess how best to deploy existing resources to spur innovation, such as making more usable data sets publicly available (e.g., properly "cleaned" data) and targeting research funding to address gaps (e.g., in existing Internet of Things (IoT) security) and solve hard problems beyond a commercial scope.

6. Finally, the U.S. government should prepare for the inevitable future security challenges and crises presented by emerging technologies. This includes building trust, cooperation, and resilience now, with the public, with allies and partners, and even with competitors on select issues.

Foreword

Geopolitical competition in the decades ahead will be increasingly defined by economic and technological power. Those countries that set the rules and standards in emerging technologies will reinforce and spread their political, economic, and societal values globally. They will thus be advantaged in developing the international institutions and rules that reinforce their preferences, with compounding returns.

Recently, autocratic governments have appeared more adept at positioning themselves for this competition. Autocratic countries may create environments less favorable to producing technological innovation, but they are able to exert greater central control over technologies and then direct technological developments to advance their geopolitical interests. Through this central control, they manage or avoid frictions between the public and private sector, and between military and civilian uses. They are also less bound by ethical considerations than governments in open societies. They can move forward rapidly to experiment and field technologies that threaten our security.

In response to progress by competitors, incumbent powers like the United States may be tempted to maintain their technological edge by locking down, as through restrictive immigration policy, and preventing the spread of their sensitive technologies, as through highly constrained export policies. But such approaches ignore the long-term advantages of the United States in incentivizing our dynamic private sector to innovate and recruiting the best talent from around the globe. Instead, we should leverage our unique leadership and alliances to reinforce values of fairness and competition globally. The United States should focus on responsibly accelerating its own technological progress, not simply obstructing potential adversaries. Over time, the benefits of this approach will outweigh any perceived benefits of pure protectionism, just as was the case during the Cold War.

In parallel with efforts to spur a broad U.S. innovation economy, the U.S. government should focus on a few priority areas. As government departments and agencies continue to invest in research, they should be resourced to promote the highest national priorities and fill gaps in security considerations that the private sector has insufficient incentives to address. And finally, those parts of government that are responsible for enabling innovation, such as the National Institutes of Standards and Technology and the National Science Foundation, should be protected from the increasingly partisan politics and funding uncertainty that has come to characterize this era. These quiet, effective bureaucracies are the vanguard for future U.S. global leadership in technology and our national security.

John Hamre
President & CEO

I. Importance of Emerging Technologies Governance

There is broad agreement among national security policymakers that emerging technologies will be decisive in determining future U.S. national competitiveness and security. There is also growing concern that the U.S. government may not be capable of optimizing such potential while also guarding against risks.

On October 2, 2019, CSIS brought together a bipartisan group of leading experts on defense technology, international law, and trade policy to consider these challenges and identify actionable insights and solutions to preserve or restore U.S. and allied advantage. These insights, along with a series of semi-structured interviews and discussions over the past year with technology leaders conducted by the report authors, inform the findings presented here.

Modernizing Governance

Concerns about the future direction of emerging technologies governance by the U.S. federal government are driven by three considerations.[1] First, the speed at which emerging technologies are developing and coming into widescale use is accelerating.[2] There is less time for policymakers to both understand the potential end uses and implications of any given new technology and to institute sufficient governance around those unknown future cases. The fear is that government risks either overregulating or underregulating technologies, creating suboptimal outcomes that directly affect national security, innovation, and global commercial competitiveness and market share.[3] Second, global commercial industry beyond traditional defense companies increasingly drives the creation of new technologies, including those

1. The term "governance" as used in this paper encompasses the strategies, processes, resources, laws, regulations, institutions, bureaucracies, and international cooperation and agreements that affect government engagement with and oversight of emerging technologies.
2. The acceleration of progress is evident in the continuation of Moore's Law (the number of transistors on a microchip doubles every two years and the cost of processing is halved) and the Carlson Curve (speed and cost reduction of genetic sequencing, much faster than Moore's Law). See also Max Roser and Hannah Ritchie, "Technological Progress," Our World In Data, 2019, https://ourworldindata.org/technological-progress.
3. Collingridge wrote, "The social consequences of a technology cannot be predicted early in the life of the technology. By the time undesirable consequences are discovered, however, the technology is often so much part of the whole economics and social fabric that its control is extremely difficult." See David Collingridge, The Social Control of Technology (New York, NY: Palgrave Macmillan, 1980), 11.

technologies with military applications.[4] The expanded use of commercial off-the-shelf technology in military and other national systems means that the private sector plays a more significant role in traditional defense and national security systems. Moreover, the United States' ability to dominate critical technologies is weakening in a globally integrated economy with more highly distributed innovation hubs and talent bases. And third, the risks posed to U.S. democracy and security, as well as to allies and international institutions, by emerging technologies—including through new and novel uses—are increasing. The weaponization of social media and rise of digital surveillance are but two examples of unintentional consequences of such new and novel end uses.

U.S. federal government efforts to address emerging technologies are increasing in scale and focus. The concept of a "National Security Innovation Base" was introduced in the 2017 National Security Strategy and the 2018 National Defense Strategy. As part of the Fiscal Year 2018 National Defense Authorization Act, Congress signed into law the Foreign Investment Risk Review Modernization Act and Export Control Reform Act to strengthen controls around sensitive U.S. technologies. There are also multiple efforts across government related to artificial intelligence, quantum computing, and advanced manufacturing, with billions in new investments concentrated in these areas. Efforts within existing bureaucracies in executive branch agencies and departments, and within Congress and supporting offices, have also intensified. Parallel to this activity, there is increased communication and consultation between government and the private sector on emerging technologies, including the creation of new bodies for information exchange and collaboration.

Despite these developments, the U.S. government is not effectively positioned to uphold the twin pillars of national security and national innovation. Over the course of the workshop discussion, experts expressed the opinion that U.S. policymakers should continually expand and refine their thinking on technology as a national security imperative. Discussants broadly agreed that there will need to be additional, formalized cross-government policy planning to focus on key themes and issues related to the physical security, third-party transfer, and nonproliferation implications of emerging technologies. Workshop discussion also made clear that there is no "one-size-fits-all" governance approach to the set of emerging technologies that exist today, let alone for novel end uses of existing technologies or the unknown technologies ahead. An evolving set of tailored policies, actions, and new modes of organization will be necessary. The U.S. government will need to strengthen technology expertise across agencies and departments, as a customer, user, and regulator. Moreover, there will need to be new approaches to collaboration between the public and private sectors at the national and international levels.

At the federal level, the executive branch should lead on emerging technologies policy. This will require knowledge capacity and authority at the White House to coordinate oversight of issues that cut across national security and national science and technology innovation. The existing Office of Science and Technology Policy (OSTP) was created in 1976 to advise on research and development (R&D) priorities,

4. Multiple factors account for this trend, including reduced government R&D spending both as a percentage of total GDP and total national R&D spending, the growth of global supply chains, the rise of multinational corporations serving multiple markets, the growing number of STEM-educated workers worldwide, and more.

but it has never had budgetary authority. While OSTP's importance has risen over recent decades, its influence has remained limited. At the same time, departments and agencies throughout the federal government as well as the U.S. Congress must demonstrate facility with emerging technologies issues that intersect with economic and security priorities. Overall U.S. government engagement on new technologies has also been uneven over this period; large-scale bureaucracies have targeted issues such as cybersecurity, but technologies such as synthetic biology are overseen by relatively limited teams, despite such technologies' enormous strategic importance. In contrast, the U.S. Defense Advanced Research Project Agency (DARPA) has proven a remarkably successful body in bridging the divide between public and private sectors, in staying on the cutting edge of emerging technologies, and in concentrating resources to achieve critical breakthroughs in national security and national innovation. Whether there is a scalable or exportable "DARPA model" for the broader government is a question that deserves separate evaluation.

The China Challenge

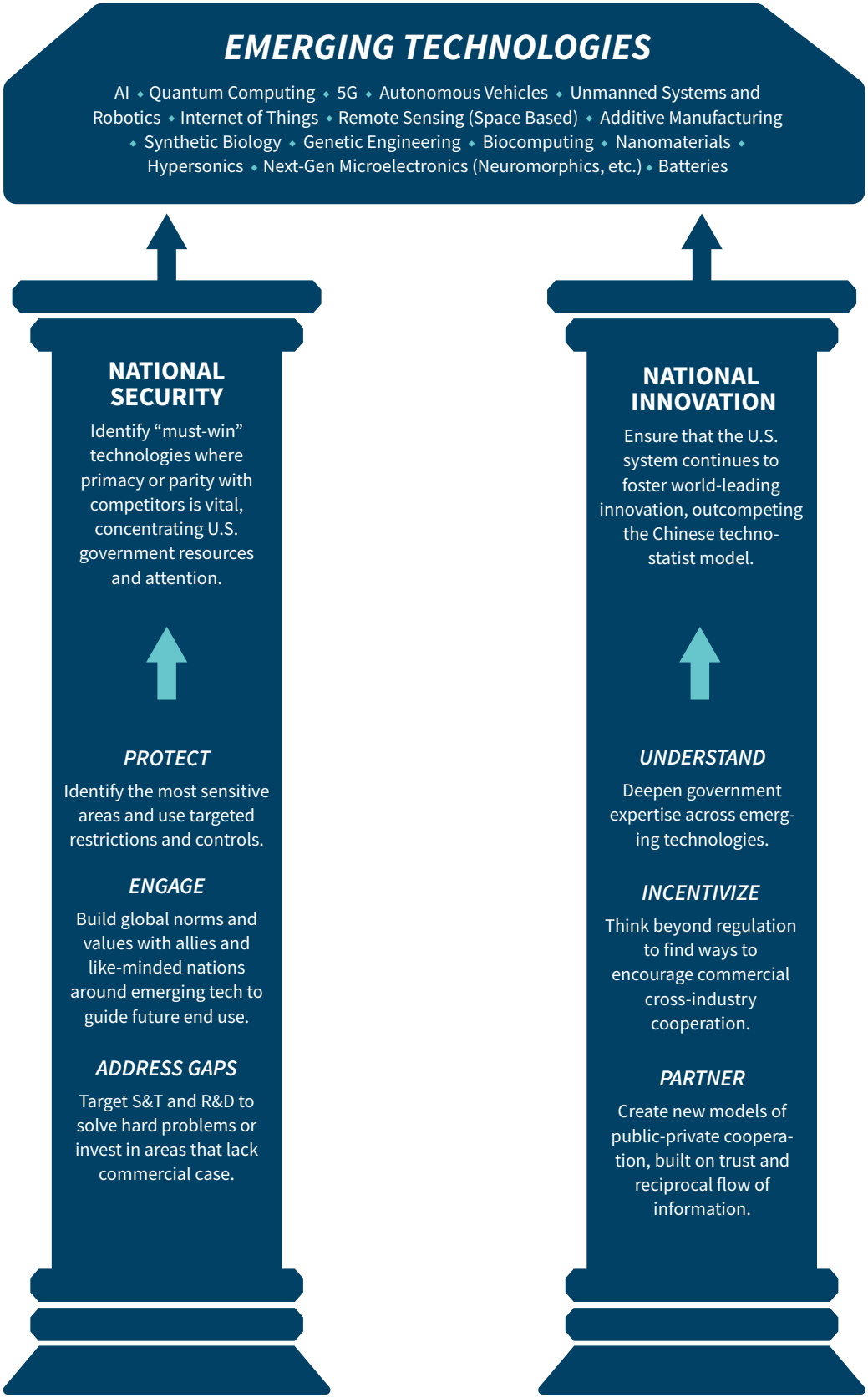
China seeks to leverage emerging technologies to its national advantage in a way that disadvantages other nations. Its tools to achieve that end include massive state subsidization and direction of industry, forced technology transfer and intellectual property theft from foreign companies, and other state-led industrial policies. The Chinese model of state-directed capitalism and military-civil fusion afford it unique advantages to concentrate resources on specific emerging technologies via private industry, researchers, academia, and the military. Rather than balancing national security and national innovation, it has combined them into a top-down enterprise. It is, in effect, an ambitious bet by China's leadership that the state can pioneer a new approach to innovation in the same way it engineered its most recent era of economic development.

While statistics on China's R&D spending and direct quotes from political doctrine show a significant increase in inputs into emerging technologies, many workshop participants observed that measuring outputs or outcomes from the Chinese system remains difficult. While it is unclear how effective or efficient Chinese investment is, it is clear that Chinese activity is significant. It is highly likely that China will emerge as a leader in certain emerging technology sectors, joining the ranks of incumbent technological powers, such as the United States, Europe, and Japan. Given China's track record in growing its national power over the past three decades, the United States should take seriously China's intention to subsume global technological innovation and supply chains, as stated in the Made in China 2025 strategy and elsewhere.[5] The global technology landscape will become more fragmented as a result, and it is less certain that the United States will always be able to reap advantages, nor will it likely dominate across all technologies.

Another distinguishing element of the Chinese approach to emerging technologies is its ability to rapidly gain market access and market share using its global array

5. Wayne M. Morrison, "The Made in China 2025 Initiative: Economic Implications for the United States," Congressional Research Service, April 12, 2019, https://fas.org/sgp/crs/row/IF10964.pdf.

Figure 1: The Twin Pillars of Emerging Technologies Governance



of bilateral agreements and the global commercial and political network, such as it has done under its Belt and Road Initiative and the corollary Digital Silk Road. State subsidization and guaranteed market share could allow Chinese firms to stifle competition from U.S. and other foreign firms and give the Chinese state significant intelligence gathering tools. Already, China seeks to set standards that favor its companies and interests in areas such as 5G wireless technology and autonomous vehicles, seeking to create vertically integrated systems wherever possible to maximize central control, especially of data. The data those companies collect is in turn used to advance Chinese national interests. Furthermore, guaranteed market share allows Chinese entities to set the global parameters of emerging technologies use, which affects norms related to citizen rights, data privacy, and fair governance. For instance, its move into the "safe cities" technology market creates an opportunity to export its authoritarian model of citizen surveillance. This could advantage undemocratic regimes seeking to control their populations and undermine the individual expression and peaceful political dissent of citizens.

If the United States fails to maintain global market share in key emerging technologies, it loses its ability to engage with like-minded countries to explicitly reinforce shared values of human rights and freedoms. The United States must therefore walk a fine line between preventing Chinese abuses, such as espionage and intellectual property theft, and creating a self-fulfilling prophecy of decline by closing U.S. companies off to Chinese and other markets through wide-scale U.S.-China decoupling. To that end, U.S. thinking on technology must acknowledge the dangers posed by China without adopting a purely threat-driven approach to national security and national innovation.

II. Key Themes

Through scenario-based and seminar-style discussions, workshop participants considered a highly varied set of emerging technologies. Special focus was given to artificial intelligence, robotics, social media, cybersecurity, and genetic engineering. Less discussion occurred around hypersonics, quantum computing, next-generation microchips, biocomputing, computer-brain interface, nanomaterials, and other topics.

Leading Across Emerging Technologies

The term "emerging technologies" refers to a broad range of very different technologies that are most usefully considered separately, despite a bias among the national security community to discuss them in monolithic terms.

The United States is unlikely to be dominant across the varied domains of emerging technologies. Both U.S. allies and adversaries can and will be first movers as they pursue their own technology and innovation strategies in line with their own future economic competitiveness and national security strategies. The United States should therefore take the following steps to optimize its own strategy regarding emerging technologies innovation.

- *Cultivate expert understanding of emerging technologies at a technology-specific level.* Each given technology—from artificial intelligence to synthetic biology—is a complex field unto itself. Any one person is unlikely to be an expert across multiple technologies, particularly when it is a secondary specialty or sub-interest, as it is for many in government. While it is true that there are growing intersections and important interactions between technologies, each technology remains driven by a distinct expert community, and each necessitates specific subject-matter expertise in government. Ensuring "coverage" across emerging technologies is important, including a gap analysis of where attention or understanding may be insufficient. Taking a generalist approach to governing emerging technologies, however, would lead to suboptimal outcomes in innovation and national security risk management.
- *Identify those technologies in which success is imperative for national security*. Certain emerging technologies, such as artificial intelligence, could prove a decisive advantage for first movers, rapidly tipping the balance of power. The U.S. government should identify and prioritize resources and energies for these technologies. The current

U.S. federal approach involves a co-signed memorandum from the Office of Science and Technology Policy and the Office of Management and Budget for the heads of executive departments and agencies on FY 2020 Administration Research and Development Budget Priorities.[6] While a step in the right direction, the guidance lacks an implementation plan and associated formal governance structure.

- *Prepare to be a fast follower*. In an increasingly competitive global technology landscape, the United States should develop plans to be a "fast follower" in those areas where others may be first to innovate. The U.S. intelligence community has an increasingly important role to play in monitoring and assessing foreign technology capabilities. To continue to avoid destabilizing strategic technological surprises, the U.S. intelligence community should further invest in predictive research and indicator tracking and communicate regularly with the rest of government regarding those fields that are difficult to track.

- *Balance defense and offense* (*fences and gates)*. The United States has continued to strengthen measures to monitor foreign access to and transfer of sensitive technologies. Strengthened export and investment controls are both necessary and effective. However, overuse of defensive tools risks stifling U.S. innovation while simply pushing would-be adversaries elsewhere in the global market, ultimately undercutting U.S. leverage to set norms and standards.

- *Fund basic research*. While private-sector R&D continues to rise as a share of total R&D, federally funded basic research is critical to addressing items the private sector is not incentivized to pursue. That includes long-term R&D efforts on difficult challenges, especially relating to security, that lack market rationale. U.S. research institutes, centers of excellence, defense agencies, mixed programs, and grants are all vehicles to deliver on this type of R&D. U.S. federal laboratories ("the national labs") also represent an underutilized source of innovation. Under current laws, these laboratories are not rewarded for their role in specific technology innovation transferred to the private sector—that is, their budget share does not increase as a result of revenues they generate back to the U.S. Treasury. Changing this simple incentive could further motivate their cooperation with the private sector in technology transfer and facilitate greater outcomes from current federal R&D spending.

- *Operationalize new technologies in government*. The United States, and Department of Defense in particular, should focus on developing new operational concepts to take advantage of emerging technologies. Beyond the defense sector, government departments and agencies should be intentional about experimentation with new technologies to improve both day-to-day and complex processes. This should include more flexible R&D budgets to facilitate experimental process innovation (versus "bulk buy" systems). The Internal Revenue Service, for example, lacks the procurement authority to test even basic operational automation and must thus make large-scale, cross-agency procurements. Learning should be shared across federal departments

6. Kelvin K. Droegemeier and Russell T Vought, "Memorandum For The Heads Of Executive Departments and Agencies," Excecutive Office of the President, https://www.whitehouse.gov/wp-content/uploads/2019/08/FY-21-RD-Budget-Priorities.pdf.

and agencies, identifying ongoing initiatives, current proficiencies, and where potential weaknesses exist.

Public-Private Partnership

While government will continue to play a vital role in setting the conditions for national innovation and managing the national security risks of emerging technologies, the private sector will drive U.S. emerging technologies innovation. Unfortunately, public-private relations are increasingly tense, operating more in the mode of a prisoner's dilemma than productive collaboration. New models of public-private partnership are necessary, which should begin with clearer communication and greater incentives to exchange information and ideas. To maximize the effectiveness of such partnerships, policymakers should consider some of the following recommendations.

- *Embrace new models for public-private partnership*. The U.S. government and private sector should do more to jointly develop innovation priorities, collaborate on basic research, create joint ventures, utilize new grants and competitions, and increase opportunities for experts to move between sectors. The federal government can do more to play a convening role in issues of national importance. The Financial Services Information Sharing and Analysis Center (FSIAC) is an example of how a public-private consortium can be used to respond to a larger issue (in this case, cyber risk in the financial system). The FSIAC leverages its intelligence platform and a peer-to-peer network of experts to respond to cyber threats. However, it is worth noting that the trust and cooperation that exists in the banking sector is the result of decades of strong federal oversight and regulation and will take time to build in other sectors.

- *Build trust between public and private sectors*. There is broad need for confidence building between the public and private sectors. The relationship between technology companies and Congress has become particularly charged as rhetoric around technology has become more politicized and partisan. This is particularly true in congressional oversight. There is a need for broad information exchange to build shared understanding of technology, terminology, and even culture between government and the private sector. The use of track two and track 1.5 dialogues, drawing from lessons of confidence-building measures between countries in the context of conflict resolution and arms control may be the right set of case studies to draw inspiration from.

- *Develop new models of transparency for sharing information and data.* The current relationship between the public and private sectors on data is still relatively one sided. Private companies collect data that the government later requests, often based on national security requirements and against the wishes of the companies. Private companies also take on increasing risks as they collect potentially sensitive national security data that makes citizens/consumers uncomfortable and creates liabilities. The dynamic could be improved through a more regularized, reciprocal exchange of data and a clearer regulatory role for government. This could in turn reduce liability and public concern with the self-policing powers of private companies. This applies to all companies that collect personal data on users, which include a growing number of businesses outside the traditional technology sector.

- *Open more government data sets to the public and make them easier to use*. While the government has improved data publication in recent years, much of it is still poorly labeled. Furthermore, the federal government still controls massive amounts of unpublished data, which represent a critical input for machine learning and artificial intelligence. Opening datasets, while protecting personal information and privacy, allows for a range of potential entrepreneurs to experiment and innovate. The United States can also harness the power of its own data for efficiencies and even military advantage. For example, the Department of Defense collects significant data on its personnel and platforms that it has only leveraged heretofore in narrow applications. With the right AI application, such data could yield everything from significantly higher military readiness to medical breakthroughs.

Innovation and Security

Building on the above point, close collaboration between the public and private sectors is necessary to achieve the twin objectives of preserving national security and the continued global innovative competitiveness of the U.S. private sector. Collaboration is far easier for government and business to achieve with existing technologies than with emerging technologies for the simple reason that industry and government are learning as they go with the latter. Governments tend toward inertia, while companies must move quickly to achieve scale and profitability in a competitive market. While this tension is in some ways natural and unsolvable, there are steps that can be taken to reduce risk while maintaining open innovation.

- *Revisit industrial policy*. National industrial policy played an important part in maintaining U.S. technological progress throughout the Cold War. The United States maintains a form of national industrial policy through today in the defense acquisition process. Alongside grants, defense acquisition gives the government tools to create incentives for the private sector to provide solutions in exchange for market access and guaranteed public-sector customers. Industrial policies are not readymade solutions but will need to be combined with other incentives to stoke innovation. These policies can also be market-based in principle, using tax incentives and multiple other forms of government assistance and technology transfer approaches to promote certain U.S. industries. Rising protectionism and technology industry intervention by U.S. adversaries and commercial competitors may also necessitate response by the U.S. government to help re-level the playing field for U.S. companies, which must remain viable at scale for national security purposes.

- *Create voluntary standards.* Introduced at the right time, with the right message, and in the right forum, voluntary standards can create natural networks for information sharing and best practices. For example, the Leadership in Energy and Environmental Design (LEED) is the most widely used green building rating system in the world and provides a successful potential template for voluntary private-sector standard setting. This certification concept could be copied for other innovation types, such as a certification for IoT security or for a standard of care. The concept could be taken more broadly to address, for instance, issues such as platform content, where. voluntary standards related to shared values could be introduced that companies would then seek to uphold in content moderation. The 1975 Asilomar Conference on Recombinant DNA represents another example of voluntary standards and guideline

Figure 2: Examples of Successful Governance Organizations or Processes

Organization/Process	Description
U.S. Defense Advanced Research Project Agency (DARPA)	DARPA, founded in 1958, creates a bridge between government and private companies through special hiring and funding authorities to create technological breakthroughs.
The Financial Services Information Sharing and Analysis Center (FSIAC)	FSIAC, founded in 1999, is a knowledge-sharing industry consortium dedicated to reducing cyber-risk in the global financial system.
Leadership in Energy and Environmental Design (LEED)	LEED, founded in 1993, is the most widely used green building rating system in the world.
Asilomar Conference on Recombinant DNA	The 1975 conference was highly influential in regulating potential biohazards related to biotechnology, while dramatically increasing public understanding of the technology.
Global Internet Forum to Counter Terrorism (GIFCT)	GIFCT, formally established in 2017, is an independent organization that sustains and deepens industry collaboration while incorporating civil society and government to further the goal of disrupting terrorist abuse of platforms.
Critical Infrastructure Partnership Advisory Council	This DHS-convened forum was established in 2013 to foster collaboration between government and private sector companies on critical infrastructure security and resilience.
National Institutes of Standards and Technology (NIST)	NIST, founded in 1901, works closely with commercial industry to develop global commercial standards of metrology.
Global Health Security Agenda (GHSA)	The GHSA, launched in 2014, is a collection of nations, international organizations, and civil society that aims to accelerate progress toward making the world safe from disease threats.
Civil Reserve Air Fleet	The Civil Reserve Air Fleet, launched in 1951, is a cooperative, voluntary program involving the DOT, DOD and the U.S. civil air carrier industry in a partnership to augment DOD aircraft capability during a crisis.

setting. In addition to addressing the public health and safety challenges of an emerging technology, the conference greatly expanded public understanding of the topic and created trust in future dialogue.

- *Encourage industry-led consortia on specific challenges*. Among the clearest cases of success to date in emerging technologies governance is the industry-led Global Internet Forum to Counter Terrorism (GIFCT). The forum has emerged as a premiere venue to share best practices, understand emerging threats, and jointly tackle shared technical challenges in preventing and responding to the use of digital platforms by terrorists and violent extremists. It has also provided a format in which participants can meet with government policymakers behind closed doors to

discuss sensitive matters in a way that relieves any individual company of the risks of that exchange.

- *Underwrite basic security in critical technologies.* The federal government may need to foot the bill for creating a baseline level of security in some technologies, especially where there are not incentives or broad enough purview for private industry itself to develop and coordinate baseline security standards. Government can do this in coordination with industry, such as was the case in addressing computer BIOS security through the Department of Homeland Security-convened Enduring Security Forum in 2010.[7]

- *Attach strings to federal contracts [requests for proposal (RFP)].* Federal contracting could set new standards regarding basic security guarantees. Those requirements could have broader positive spillover impacts as the federal government leverages its position as a major customer to raise the bar industry wide.[8] Recognizing that, for example, Department of Homeland Security grants have largely focused on physical security (e.g., first responder equipment or hardening certain facilities from attack), there is an opportunity for the federal government to redefine how it views national critical infrastructure. By redefining critical infrastructure, the U.S. government could reapportion funds to address a broader set of vulnerabilities and better manage the risks of emerging technologies.

- *Build in liability clauses where individuals are responsible for company security*. To date, the cost of major cyber breaches has been in the form of financial penalties at the company level. This may not be sufficient incentive for due diligence and attention from senior leaders, suggesting that personal liability could be a potential solution.

- *Bring in state and local governments.* Hundreds of individual cities and municipalities will be responsible for the implementation and support of smart city infrastructure and security, taking on new risks they are largely unprepared for. This means that while the federal government certainly has a role in creating certain standards and policies, it should support local government capacity to innovate while cultivating proper understanding of risks. The recent rash of ransomware attacks on municipalities demonstrates the growing vulnerabilities of subnational governments.

- *Approach emerging technologies issues flexibly and dynamically.* The rapid pace of change has made clear the need for flexible new approaches. For example, the United States could issue more dynamic Federal Select Agent rules and export control lists, which historically have helped stop the proliferation of hazardous substances. To avoid stifling innovation, rule-making processes and experts will need to be highly specialized, with participation from external subject matter advisers and the private sector. Such mechanisms could be made faster and be retooled to govern particularly critical technologies, including by limiting access by non-state actors.

Emerging Technologies Workforce

The human dimension of the workforce is an often-overlooked factor in emerging technologies discussions. Three main objectives stand out. The first is to grow the overall base of qualified workers in the United States across the public and private sectors. The second is a need to strengthen standards for who has access to sensitive emerging

technologies. And the third is to determine how to encourage interest among tech experts to work within and in support of the U.S. government on national security challenges. Participant proposals to foster an innovative U.S. workforce include:

- *Improve personnel vetting and standards for safety and conduct.* Beyond protecting and hardening technologies, it is also vital to U.S. national security to monitor both the people who work in certain high-risk fields and the physical security of their worksites. The U.S. regime for handling insider threats, such as potential domestic terrorists, is inadequate in light of increasingly dangerous technologies. The fast-growing biotech economy, for example, might need to explore the concept of licensed and bonded researchers, with the federal government providing resources to support screening critical research facilities. Additionally, the sector would benefit from confidential reporting mechanisms through which researchers could report possible insider threats as well as severe violations of ethical and safety standards.

- *Reform the federal workplace.* The government should make the public sector more attractive to STEM professionals by modernizing and adjusting their institutional culture to allow for fast-paced innovation and to welcome ideas from lower-level employees. The government could also utilize project-based employment cycles that allow private-sector subject matter experts to temporarily work on critical national technology projects. Additionally, the government should make greater use of government tech fellowships and grants, which allow movement to different states and departments and permit fluidity between the public and private sectors. This in turn would promote subject expertise and appeal to a workforce that increasingly values change.

- *Improve K-12 and STEM education.* The United States increasingly faces a lack of qualified STEM workers. Facilitating greater access to undergraduate STEM education would help the U.S. workforce better prepare for the future needs of a high-tech economy. The United States could use such access, through conditional education grant programs and revamped STEM fellowships, to channel new talent to meet critical national requirements. Additionally, both K-12 schools and higher education institutions should be given the resources to improve and standardize their STEM curricula. Promoting tech education and skills training in military education could also benefit U.S. security interests while simultaneously benefitting the U.S. private-sector workforce by equipping veterans with increasingly desirable skills for a high-tech economy.

- *Attract and maintain global talent*. The United States has historically thrived on welcoming the talent of immigrants. Immigration policy should aim to complement efforts to make the United States welcoming to foreigners, with the goal to promote a creative and tech- and science-positive society. The United States should reform its immigration policies to allow all PhD graduates from foreign countries to apply for a green card and to permit easy transfer of research grants and licenses from one state to another. This would disincentivize brain drain or return migration and enhance the pool of talent from which the private and public sectors draw.

Broad, Sustained Diplomatic Engagement

Emerging technologies are central to U.S. interests. As such, they should be central to U.S. diplomatic engagement globally. Diplomacy will be necessary in the realm of emerging technologies; the United States should prepare for potential friction with even the closest allies but also allow room for cooperation with even the most adversarial countries. U.S. values and core interests should drive principled engagement that seeks common ground around critical issues and aims to set the rules of the road for years to come. But to realize this agenda, the United States should clearly articulate those values and interests and position them as an alternative—or, in some cases, a complement to—China's increasingly assertive efforts to lead on emerging technologies globally. A principled engagement strategy could be structured as follows.

- *Support the efforts of allies and partners.* The U.S. alliance structure provides a unique opportunity to ensure an innovation edge through collaboration and distribution of efforts between countries. The United States should coordinate technology strategy with allies and should encourage partners to mitigate the risks of an adversary dominating a particular field in which the United States does not have a clear advantage. For example, in the case of 5G cellular technology, the United States does not have a direct competitor firm to China's Huawei, but the European Union is home to Nokia and Ericsson, both comparable producers of key 5G infrastructure. The United States should strive to learn from other countries and lead by fostering a science-friendly climate. This includes creating "playgrounds" for collaboration with stakeholders from other countries. Formal or informal "technology alliances"—setting joint technological standards and rules with friendly and like-minded countries—could serve as force multipliers supporting the adoption of U.S. technological preferences.

- *Articulate clear positions on specific end uses.* The United States should set priorities not only for research but also for ethical decisions on issues including gene therapy, human experimentation, and surveillance. In the digital governance space, the United States should decide its position on privacy and data flows. As these technologies rapidly evolve, the United States should accelerate efforts to establish its position and ensure the compatibility of these developments with the country's democratic values. The U.S. National Institutes of Standards and Technology (NIST) and the National Science Foundations will continue to play important roles in informing and leading these efforts. NIST has been especially effective in working closely with industry to develop global commercial standards of metrology that mirror U.S. values of safety, effectiveness, openness, and transparency.

- *Emphasize norm building, particularly with support from the Global South*. The United States should engage the global community to promote its version of technological and scientific development. LEED certification, the Global Health Security Agenda, Paris Climate Agreement, and (now defunct) Transpacific Partnership are all examples of how norms can be built with multilateral and multi-stakeholder support. Participants noted that powerful norms are frequently integrated with national laws, indicating the importance of such efforts. While the United States should work to build norms with historical allies, it should also aim to engage and compromise with historically marginalized countries, particularly those in the Global South, to create global frameworks. The cost of entry is low for a number of emerging technologies, meaning

that strategic geographic areas outside of developed economies can become major global technology players with influence over data centers and software development. Countries such as Vietnam, India, Brazil, and Indonesia are emerging as important and, in some cases, problematic actors in emerging technologies governance issues, demanding greater U.S. engagement. The United States should facilitate greater market connection with such countries to foster collaboration.

- *Engage through multilateral institutions.* Participants highlighted the necessity of multilateral institutions, including the United Nations, G20, G7, World Health Organization, and various standards-setting consortiums, to bring order to emerging technologies on a global basis. Best practices will likely take a patchwork approach, depending on the health of existing institutions and major gaps or differences that need to be addressed. Close cooperation with like-minded countries will be necessary to maintain U.S. influence in such bodies, which are vital to establishing universal norms. Engagement in credible multilateral institutions also allows the United States to seek common ground with countries such as Russia and China.

- *Consider new vehicles/agreements (vs. entire organizations) to push emerging technology priorities.* For example, the United States could incorporate security standards, from cybersecurity to biosafety, into trade agreements. It may in other cases wish to pursue single-purpose memoranda of understanding.

Prepare for Inevitable Frictions and Crises

History shows that surprise derived from emerging technologies is inevitable. Designing approaches to governance that account for rapid response capability are essential. Expert dialogues, gaming, and simulation can be useful in exploring the possibility space of what challenges emerging technology could pose, exposing senior decisionmakers to the possibility of these risks before they manifest. These could include some range of the following actions.

- *Educate Congress, the White House, and the judiciary*. Congress cannot appropriately legislate regarding emerging technologies without basic understanding of rapid developments. Expert advice is therefore a vital input for members of Congress. The most obvious "win" would be the restoration of an Office of Technology Assessment for Congress. It might be beneficial to have a Council of Technology Advisors for the White House additional to existing advisory structures. The judiciary also must be considered. U.S. judges may fail to understand liability relating to cybersecurity and critical technologies governance without advice on potential "domino effects" that a lapse in security can bring to the wider ecosystem.

- *Hold public hearings on technologies governance*. Expertise to inform governance and the public on such subjects can be found across multiple disciplines, including from technical and scientific experts, international relations scholars, economists, and more. Broadly, exploratory public hearings, including an interdisciplinary pool of technology experts, would helpfully broaden the dialogue on critical issues.

- *Develop a secure platform for emergency information*. With the rise of misinformation and information operations, the government requires a trusted platform or mechanism

citizens can turn to in a crisis. Mass panic can lead to increased damage and casualties. Other countries have information centers or government offices dedicated to the dissemination of accurate and timely knowledge to the public that could serve as potential models. For example, the National Tsunami Warning Centres are designated to serve as a trusted source to coordinate international tsunami warning and mitigation activities globally.

- *Establish pre-crisis partnerships*. A massive cyberattack or global pandemic could incapacitate digital and physical infrastructure, as well as cause massive disruption across society, including erosion of trust in core institutions. Anticipating such risks, the U.S. government should assemble a list of cyber, biology, and medical experts willing and able to assist in the event of a debilitating crisis. Furthermore, the government could even prequalify companies willing to share information or resources in times of emergency. One model to keep in mind is the Civil Reserve Air Fleet, which enables the military to use partnered companies' aircraft in times of war in exchange for higher chances of securing an Air Force contract. Such incentives could also help provide the federal government access to cyber and other professionals in the event of crisis.

- *Develop emergency response education and procedures*. It is essential to educate the public on emergency procedures, including on how to fall back on analog systems. The U.S. public—especially younger generations—has grown increasingly dependent on digital connectivity and should be prepared to act without it in times of crisis. Preparedness and resilience also require redundancy. The United States should develop backup systems in the event that primary digital systems are disabled. This includes building reserves of medical, energy, and food supplies and in some cases developing analog systems for day-to-day services such as water and waste management.

Conclusion

The overall success of the U.S. federal government in emerging technologies governance is at best a mixed case and is overall inadequate to the scale and stakes of the challenges and opportunities ahead. It is impossible to fully anticipate future governance requirements, just as policymakers will not arrive at a gold standard of governance scalable across all current and next generation technologies. The United States should therefore experiment broadly with its approach to governance, encouraging innovation and accepting inevitable setbacks along the way. The greatest danger is inaction or resignation to "business as usual" amid an age of technological hyper-expansion and global competition. There is a clear need for greater cooperation and engagement on the challenges within government; between federal, state, and local levels; between governments; and between the public and private sectors. By recognizing its own comparative strengths and weaknesses, the U.S. federal government can take measured steps that increase its chances of success and guard against risks. The United States should carefully balance defensive and offensive measures. The stakes are high: setting fences too high risks stunting domestic innovation, setting them too low risks exposure to potentially calamitous downsides of unknown emerging technologies.

Government should fundamentally reimagine its role and embrace a networked approach. Good ideas, along with dangers, will flow from many nodes, many of them outside government. Governance is increasingly a shared responsibility and enterprise, where new hybrid models are necessary. Absent such a shift in mentality, the U.S. government will perpetually lag in understanding ongoing changes. Government needs to shift from top-down control to develop new horizontal modes of information sharing and cooperation external to its vertical structures. That said, there is also need for renewed White House-directed leadership in emerging technologies governance. This should be an issue at the top of the agenda for any president and cabinet. Government cannot deliberate endlessly and should err on the side of permission and action. Global progress on emerging technologies will move on with or without its approval.

And finally, there are critical considerations when it comes to areas where failure by government would be catastrophic. In these cases, the United States should be steadfast in creating and enforcing security. The U.S. government should hold purview and agency over the overall question of U.S. technological competition with China and others. The U.S. federal government should continue to help clarify the risks associated with foreign technology domestically and with our allies and partners. Additionally, it should articulate and plan for the

social, labor, environmental, and other external impacts of technology developments to come. As technology plays an increasingly dominant role in human affairs, the fate of nations rests on the ability of governments, companies, and citizens to uphold the twin pillars of national security and national innovation.

About the Authors

Samuel J. Brannen leads the Risk and Foresight Group at CSIS and is a senior fellow in the International Security Program. He has previously served as a long-range strategic planner and adviser to senior leaders in government and business. The newly established Risk and Foresight Group is charged with providing decisionmakers with insights into the forces of change reshaping the global environment, from shifting demographics to emerging technologies.

Christian Stirling Haig is a research assistant in the International Security Program at CSIS. In this position, he provides research and program support for the Risk and Foresight Group. Prior to working at CSIS, he was a Scoville International Peace Fellow researching and writing on Department of Defense vulnerabilities to climate impacts at the Natural Resources Defense Council. He holds a BA in political science and peace, war, and defense from the University of North Carolina at Chapel Hill.

Katherine Schmidt is a research intern with the Risk and Foresight Group at CSIS. She holds a BS in Science, Technology, and International Affairs from Georgetown University's School of Foreign Service and researches the topics of China, Azerbaijan, and cyber policy.

Kathleen H. Hicks is senior vice president, Henry A. Kissinger Chair, and director of the International Security Program at CSIS. With over fifty resident staff and an extensive network of non-resident affiliates, the International Security Program undertakes one of the most ambitious research and policy agendas in the security field. Dr. Hicks is a frequent writer and lecturer on geopolitics, national security, and defense matters. She served in the Obama Administration as the principal deputy under secretary of defense for policy and the deputy under secretary of defense for strategy, plans, and forces. She led the development of the 2012 Defense Strategic Guidance and the 2010 Quadrennial Defense Review. She also oversaw Department of Defense contingency and theater campaign planning. From 2006 to 2009, Dr. Hicks was a senior fellow in CSIS's international security program. Prior to that, she spent almost thirteen years as a career official in the Office of the Secretary of Defense, rising from Presidential Management Intern to the Senior Executive Service.

Appendix A: 2019 Global Security Forum Experts' Workshop Participants

The 2019 GSF Experts' Workshop was conducted on a not-for-attribution basis. Participants' insights and the dialogue among them was foundational to developing this report. Nevertheless, the summary of the proceedings contained herein do not necessarily reflect the views of any individual participant.

Scenario Moderators

Rebecca Hersman
Thomas Karako
Suzanne Spaulding

Seminar Moderator

Todd Harrison
Kathleen Hicks
Stephanie Segal

Participants

Eric Brewer
William Carter
Rocco Casagrande
Daniel Chenok
Richard Chin
Drew Colliatie
Melissa Dalton
Jennifer Daskal
Mary DeRosa
Morgan Dwyer
Eric Edelman
Matthew Goodman
Sharaelle Grzesiak
Todd Harrison
Rebecca Hersman
Kathleen Hicks
Andrew Hunter
Jason Gresh
Jay Farrar
Thomas Karako
Scott Kennedy
Meg King
Bhavya Lal
Jonathan Lee
Ryan Lewis
Ed Loughran
Doug Loverro
Tom Mahnken
Jason Matheny
Jamie Morin
Steve Morrison
Adam Mount
Kent Myers
Michael O'Hanlon
Cindy Reed Paska
Radha Iyengar Plumb
Kingston Reif
Bill Reinsch
Sokwoo Rhee
Stephen Del Rosso
Lisa Sawyer
Kelley Sayler
Adam Segal
Stephanie Segal
Lindsey Sheppard
Jordana Siegel
Erin Sikorsky
Ian Simon
Jeremy Spaulding
Suzanne Spaulding
Helen Toner
Paul Triolo
Ian Wallace
Leigh Warner
Christine Wormuth
Birian Wynne
Erol Yayboke

Appendix B: 2019 Global Security Forum Scenarios

The interactive workshop began with three concurrent scenario-based discussions. The scenarios set in the mid-to-late 2020s were designed to stress-test assumptions about governance around different types of emerging technologies, comparing and contrasting necessary approaches. "Patient Zero" envisioned a pandemic linked to a humanmade pathogen, laying clear the potential consequences of a rapidly expanding and weakly governed global bioeconomy. "AI(n)stability" considered a wildcard of Chinese development and fielding of artificial general intelligence (AGI) in its battle management system, providing a qualitative military edge in the Indo-Pacific region. "IoTerror" posited a large-scale cyberattack on U.S. smart cities infrastructure and home Internet of Things (IoT) systems, paired with a concerted information operations campaign by a malign foreign actor (or actors). These scenarios were not predictions of the future, nor was any probability assigned to their occurrence.[9]

Insights from the scenario discussions informed a second phase of the workshop, during which participants considered in a seminar format four issues: (1) the right balance of proactive and defensive measures in sustaining the U.S. innovation base; (2) the assessment of gaps in current governance structure; (3) the international context for emerging technologies governance; and (4) models for public-private collaboration in governance (see appendix C).

This proceedings document distills insights and recommendations from the workshop. The intellectual content is derived from participant contributions, though specific attribution is withheld according to the Chatham House rule under which the event was convened. The GSF workshop aimed to advance a conversation and action plan to help the United States navigate the impact of emerging technology on the economy, national security, and geopolitics. The paper organizes findings and recommendations first by describing

9. Rather, the scenarios were meant to help participants imagine a distressing future that they should want to avoid. Discussants were asked to "backcast" events to the present, identifying potential changes they could make today to foster a better future. Backcasting is a qualitative foresight technique in which a specific future trajectory, desirable or undesirable, is described as if it has already occurred. Then, events that allowed for the manifestation of that future are identified, and actions taken or not taken are identified that could either increase or decrease the likelihood that such a future would ultimately come to pass.

the importance of emerging technologies governance, then by identifying key themes and recommendations, and lastly by recommending U.S. federal government priorities for action.

Scenario 1 Outline – Patient Zero

- A modified pathogen from a European bioresearch lab has caused a global pandemic.
- It has not been firmly established whether the pathogen was released as a result of lax biosecurity or intentionally with terrorist intent.
- The event raises broader questions about biosecurity, biosafety, and expanding global research involving modified pathogens.

The World Health Organization declared a Public Health Emergency of International Concern (PHEIC) on January 4, 2025 as infection rates of a SARS/MERS-like coronavirus reached 800 million globally, killing 25 million to date (about 3.125 percent of those infected).[10] The United States, Europe, Northeast Asia, and the Middle East have been particularly hard hit by the illness.

Few countries have been left unaffected by the outbreak, and the global economy has dipped into recession. Though against World Health Organization and World Trade Organization agreements, widespread travel bans have been enacted between multiple countries. The International Monetary Fund has dramatically increased non-concessional lending and has directed member countries to exercise monetary expansion and fiscal stimulus measures to offset slowing economies globally.

The virus has been identified as humanmade, linked to a research strain from a laboratory in Berlin, Germany. The modified pathogen was a coronavirus like the one responsible for sudden-acute respiratory syndrome (SARS) and Middle East respiratory syndrome (MERS), and it was designed and replicated for research into treatment that might have application for future disease outbreaks. The incident further raises concerns of laboratory biosecurity and biosafety, which have been significantly underinvested in and understudied amid a revolution and dramatic global expansion in bioscience research related to microbe manipulation.[11]

The outbreak rapidly spread from its primary case at Berlin Tegel Airport to a range of connecting international destinations. It has not been established whether the release of the

10. In comparison, the Spanish flu of 1918-1919 infected about 500 million people worldwide (about one-third of global population) and killed 20-50 million (4-10 percent of those infected).
11. Rocco Casagrande, "Federal Funding for Biosafety Research is Critically Needed," CSIS, CSIS Brief, August 6, 2019, https://www.csis.org/analysis/federal-funding-biosafety-research-critically-needed.

pathogen was purposeful or accidental. The release of the virus has been claimed by multiple terrorist groups as a deliberate act of violence, but following an inquiry by U.S. health agencies and the intelligence community, the surgeon general of the United States announced that none of these groups possess the skill and access to materials necessary to have created it or to have acquired the specific strain. A state-sponsored attack has also been ruled out.

Two leading theories on the origin of the virus are now under close examination, both centered on a laboratory employee who is believed to have been the index case ("patient zero"). The first theory is that the pathogen was intentionally smuggled out and then released by the laboratory-employed person of interest. The individual had access to the pathogen, had academic background in infectious disease transmission, and had espoused extreme views on climate change and human overpopulation online. The second theory is that the release of the virus may have been inadvertent and the result of poor biosecurity at the facility. The laboratory has been closed for the past three months, following its established connection to the pathogen. In this time, multiple safety and security issues have been identified that could have led to inadvertent infection of the person of interest.

The person of interest was infected with the strain either unintentionally or in an attempt to or in the course of infecting others at Tegel Airport. He boarded a flight from Tegel for what he claimed was a planned personal vacation to New York, where he transited through John F. Kennedy International Airport and the virus further spread. The patient was hospitalized a day after his arrival in New York City and quickly quarantined, but not before spreading the infection in five key locations in downtown Manhattan, from which it rapidly spread to New Jersey, Connecticut, and to other U.S. and global cities via contact during his transit through JFK Airport. The person of interest recovered from the illness and was released to German authorities and returned to Berlin. He committed suicide last week while under house arrest and after his identity was revealed in German media, which was quickly picked up as headline news globally. He maintained his innocence and blamed poor biosecurity practices at the laboratory for the release. He expressed great guilt at having been patient zero.

In the three months since its release, the virus spread rapidly across Europe, North America, Northeast Asia, and the Middle East. The disease is transmissible during the prodromal period, during which carriers show only mild and, in some cases, unnoticeable symptoms. The novel nature of the pathogen means very low immunity across the population. There is no known existing treatment or prevention method (vaccine or medicine). The virus is highly transmissible via direct, person-to-person contact, and the fatality rate is significant (around 3 percent). Global drug manufacturers working in collaboration with national biodefense researchers in countries around the globe are surging to develop a treatment and vaccine, but they are months away from a workable trial.

The Chinese and Russian governments have announced ongoing experimentation with somatic therapies to create coronavirus resistance in human subjects using CRISPR gene editing.[12] The World Health Organization has warned against these

12. CRISPR—an acronym for "clustered regularly interspaced short palindromic repeats"—is essentially a cut-and-paste

efforts, pointing to a governance framework to manage norms and principles around the emerging technology—a first in its 61-year history—that discourages any broad-scale use of somatic therapies making modifications to the human genome when little is fully understood about the multiple role of the genes being edited. Chinese laboratories are also believed to be experimenting with germline editing related to coronavirus resistance.

Scenario 2 Outline – AI(n)stability

- In a technological and geopolitical shock, China developed artificial general intelligence (AGI) well before other nations and has successfully integrated AGI with its sensor networks, including air and missile defense systems.
- U.S. forces are now at a significant operational disadvantage throughout the Western Pacific region, leading the Pentagon and U.S. regional allies alike to conclude that the United States may no longer be able to defeat China in a regional conflict.
- There is additional concern that the same model of rapid innovation that allowed China to field AGI may also lead it to be first in quantum computing and other emerging technologies with military applications.

Two months ago, the Secretary of Defense and Chairman of the Joint Chiefs of Staff briefed a special National Security Council (NSC) meeting chaired by the president with detailed analysis showing that the U.S. military may no longer be able to defeat China in wartime conditions in the Western Pacific region. The assessment was spurred by a series of U.S. intelligence community (IC) findings over the last year. At the outset of the briefing, the Chairman of the Joint Chiefs informed the president and NSC members:

> This technological breakthrough has afforded China a qualitative military edge that undermines U.S. regional deterrence. Our forces deployed throughout the region, though formidable, are now held at significantly increased risk, as are those of our allies and partners. I do not have confidence in our ability to execute against operational plans.

The IC has assessed with high certainty that the Chinese People's Liberation Army (PLA) had made a breakthrough in the development of AGI. The development comes a decade or more ahead of the consensus view on when this threshold would be crossed. Unlike all existing AI to date—so-called artificial "narrow" intelligence—AGI is capable of human-like cognition at the speed of the world's fastest computers and with the ability to fuse information from an almost unlimited number of sensors and systems.

With the approval of the Chinese Communist Party (CCP), the PLA had integrated AGI into its strategic situational awareness capabilities, including radar and satellite systems, dramatically increasing the speed with which it can now process, exploit, and disseminate intelligence, surveillance, and reconnaissance data. This in turn provides the PLA significantly improved battlespace awareness and allows the PLA to find, fix, and finish targets with dramatically increased speed and precision out to the second

---

function for DNA and RNA editing in organisms from viruses to humans

island chain. Notably, CCP leadership maintains human control over China's offensive strike and nuclear forces.

Japan and the Republic of Korea are also aware of China's breakthrough and are alarmed at increasingly aggressive behavior on the part of China over the past year, which aligns with the AGI capability coming online. Two weeks ago, China moved irregular maritime forces to surround the Senkaku Islands, which have remained in place, with reports of Chinese supply ships previously associated with Chinese island base-building activities. Unlike responses to past incursions, Japan did not send Coast Guard or Maritime Self-Defense Forces in response or consult with Washington on the issue. Instead, Tokyo requested urgent high-level direct talks with Beijing. The Japanese Ministry of Foreign Affairs has relayed through multiple channels to U.S. counterparts that Tokyo is seeking to renegotiate its relations with China in a way that may necessitate the withdrawal of most or all U.S. forces from Japan. In a phone call initiated by the president last week, the Japanese prime minister said, "For the future of my country, we must acknowledge China's new role in the world. We must make decisions that are difficult but necessary to secure peace and ensure stability."

Chinese investments and strategy to develop its national AI base, outlined in its 2017 AI Development Strategy, resulted in the country achieving its stated goal three years ahead of schedule: to become the world's leading AI power by 2030. China's ability to grow globally dominant, military-fieldable innovation came in part from investment in "national champion" technology firms. These companies became globally competitive in fields including robotics, networked devices, AI sensors, and machine learning programs, fueled by the vast trove of data acquired from the Chinese market and nearly 2 billion other users on Chinese digital infrastructure around the world. China also succeeded beyond expectations in creating its own innovation ecosystem around AI research parks, AI research academies, AI-related university programs, oversight-free innovation zones, and industry-academic collaboration. Beijing also offered significant subsidies to overseas Chinese and foreign AI experts, as well as foreign technology companies, to set up research offices in China. Integration of AI by the PLA has been expedited by Beijing's "military-civilian fusion" strategy, modeled after the United States' own national research and development strategy from the Cold War. China sought to eliminate barriers between its academic institutions, industry, and military entities to facilitate increased innovation and deployment of novel technologies. Notably successful was the Beijing Institute of Technologies' academic program for elite students to develop AI weapons systems and Tsinghua University's military-civil fusion lab.

In October 2024, Beijing deployed an advanced, automated air and missile defense system using a growing system of ground-based, airborne, and space-based sensors. As of January 2027, China's air defense systems had been deployed to both the Chinese mainland and to South China Sea naval and air force installations on Chinese-claimed islands, which continued to grow in size and sophistication. This system also includes newly developed maneuverable, hypersonic missiles and narrow AI-enabled missile swarms deployed in batteries along the Chinese coastline and on South China Sea naval installations. Combined and aided in detection and targeting by AGI sensor fusion, these systems pose a significant threat to U.S. carrier groups out to the second island

chain. The United States had successfully fielded disruptive cyber tools, advanced electronic warfare systems, and sophisticated railgun and energy-based defensive countermeasures. But in its assessment the Pentagon warned that China's increasingly potent AI missile swarms could possibly overwhelm all U.S. defenses. AGI allows China to hold at risk a significant number of U.S. platforms simultaneously through extremely effective targeting and allocation of PLA resources. China has also fielded new undersea capabilities, including a new class of People's Liberation Army Navy (PLAN) Chinese submarines and the Underwater Great Wall, a network of seabed sensors, unmanned surface vessels (USVs), and unmanned underwater vehicles (UUVs) under development since 2016 and formally activated in 2023. These systems are integrated by and reliant on AI for autonomous operation. These PLAN capabilities have proven highly effective at tracking both U.S. submarines and the United States' own UUVs.

While China's AI strategy moved at an accelerating clip over the past decade, the U.S. approach flatlined. Tightening U.S. immigration restrictions increasingly pushed international AI talent to Canada, Europe, and China, in addition to encouraging Chinese talent to remain at home. And even as U.S. companies continued to retreat from the Chinese market with continued trade and economic tensions over the past decade, Japanese, Korean and European businesses continued to seek access to the Chinese market and comply with Chinese technology-sharing requirements. Simultaneously, China continued to support its military and AI development programs through widespread industrial cyberespionage.

The U.S. approach to AI development has suffered from two principal shortcomings. First, the federal funding, development, and acquisition approaches have been insufficient. Over the past decade, U.S. federal investment in AI development, in addition to being dwarfed by Chinese spending, has been hampered by a lack of consistent funding. The authorization and appropriation processes have proven slow and cumbersome, and congressional budget battles have led to multiple government shutdowns resulting in suspended contractor work and furloughed AI developers. Simultaneously, while the U.S. military devoted greater resources to AI development since the introduction of Third Offset Strategy in 2014, the majority of the services' resources continued to be directed to acquiring current-generation capabilities. Finally, the federal government pursued a largely decentralized approach to funding basic science and technology research, failing to meaningfully concentrate resources on priority areas.

The federal government, and the Department of Defense in particular, struggled to strengthen ties with the U.S. tech sector. In 2018, Google ended its work with the Pentagon on Project Maven to develop a drone AI imaging and target acquisition program, following protests from thousands of employees, including mass resignations. Then, in 2019, the U.S. Army called to build an Advanced Targeting and Lethality Automated System (ATLAS) to facilitate target acquisition, identification, and engagement faster than manual human processes. The clumsy announcement of this program blindsided the Pentagon's Joint AI Center (JAIC), which was designed to synchronize AI work across the military and burned many of the bridges outside government that the center had carefully built. In 2021, 30,000 U.S. AI developers signed a petition against militarized AI deployments, and most major U.S. tech companies and many academic research

institutions had ended their work with the U.S. military. In addition to tech worker reluctance to work on military-applicable AI projects, U.S. private sector investment in AI focused increasingly on commercially viable, short-horizon subsets of AI, such as social media and business software applications.

At the conclusion of the NSC meeting, the Director of National Intelligence warned the president and other principals present that it could get much worse. "China has similar efforts ongoing related to other emerging technologies including quantum computing and encryption," he said. "Our most sensitive human intelligence suggests that they may be years or even a decade ahead of us in some areas, and the region is taking note."

Scenario 3 Outline – IoTerror

- The United States has been crippled by a large-scale cyberattack targeting Internet of Things (IoT) devices, 5G wireless networks, autonomous vehicles, and infrastructure.
- The immediate effects of the attack were significantly worsened by an accompanying information operation across online platforms meant to sow public fear and mistrust of government response.
- The inability to attribute the attack and respond has shaken Americans' belief in the safety and security of digital infrastructure and disrupted operations across a range of commercial sectors and industries.

In the past week, the United States fell victim to a crippling attack on U.S infrastructure and households that exploited vulnerabilities in 5G networks, IoT devices, and legacy supervisory control and data acquisition (SCADA), as well as newer-generation smart infrastructure. The immediate effects of those attacks were significantly worsened by a coordinated information operation across social media platforms meant to sow maximum fear and panic through the deliberate spread of false information related to the scale and severity of the attack and U.S. response efforts. The attacks and panic surrounding them directly resulted in dozens of deaths, hundreds of injuries, riots and looting in several U.S. cities, the largest single-day drop in the U.S. stock market ever recorded, and a run on banks. In an address to the nation yesterday, the president said, "This was an attack on our very values and freedom—our trust in our safety in our communities and our homes. This is a new way of war, but make no mistake, we are at war and we will protect and defend this country."

The U.S. intelligence community (IC) finds with high confidence that the scale and organization of the attack mean state sponsorship, but at this time the IC lacks sufficient forensic evidence for specific attribution. Russia, China, North Korea, and Iran are all suspects, but each has carefully denied involvement and offered assistance both in identifying the attacker and in assisting U.S. recovery. The most destructive cyber tools involved in the attack came from non-government sources, including dark web marketplaces and an Israeli private intelligence firm breached by an external hacker collective several years ago.

Prior to the attack, the United States was by all accounts leading the world in successful integration of a range of new technologies. By 2021, working closely with federal, state,

and municipal governments, the private telecommunications industry had rolled out 5G networks across much of the United States. This was a major achievement, keeping the United States on track in the global competition around the Fourth Industrial Revolution by putting into place the critical digital infrastructure necessary to move forward on several fronts. In 2022, the White House released a much-admired National Smart Cities and Counties Plan and worked with Congress to increase funding to NASA, the Department of Defense, the Department of Energy, the Department of Agriculture, and the National Science Foundation to create programs for a range of sectors and industries to take full advantage of 5G technology. The effort was greeted on a bipartisan basis as a visionary step forward for the country, putting partisan politics aside for the good of the nation. Supporting technologies, such as edge computing, spread across the country to process the large quantity of data produced by a growing number of IoT devices and smart systems riding on the 5G network. IoT devices were adopted at breakneck pace in households and businesses around the country as they proved increasingly useful to personal and professional productivity and to organizing an increasingly complex world of digital-physical convergence. Penetration of IoT devices was particularly high in the health and agriculture sectors.

Two U.S.-based companies, Company Y and Company U, were the first to bring level-five (fully) autonomous vehicles (AVs) to market, and they have maintained a commanding domestic and international market share as adoption increases. Alongside these, electric vehicles (EVs) with varying levels of autonomy were broadly adopted in coastal cities, including as ride-pooling and sharing vehicles under the control of U.S. tech firms, concentrated in urban areas.

The stock market boomed on the strength of telecommunications and tech stocks, with many other industries riding along in the excitement over growing efficiencies and new business opportunities enabled by 5G technology. But security measures proved inadequately considered across this increasingly connected U.S. landscape.

The first phase of the attack occurred on July 4, 2025.[13] A breach in the physical security of the office building housing the hypervisor that controlled the IT infrastructure used by the two largest cloud service providers led to the introduction of malicious code into the source code. The intruder was caught after these events, but she was a hired hand paid in cryptocurrency to undertake the attack and did not know any specific details regarding the larger attack or the malicious actor. Using the digital access enabled by the physical penetration of the network, unknown hackers then modified the hypervisor code to create a permanent backdoor to access remotely at their whim.[14] When the attackers struck, they dealt an immediate blow to U.S. confidence in digital infrastructure and affected 60 percent of all cloud services, including the organizations' cloud DNS web services. Additionally, two major banking clients utilized the cloud service providers to store

13. During this first phase, CYBERCOM received incorrect intelligence that the attacks most likely were sponsored by Russia. In response, CYBERCOM launched a covert attack against Russia's internet, shutting down government websites and online banking systems for 10 hours. Further intelligence revealed that Russia is among a host of suspects, including China and other non-state actors.

14. A hypervisor creates a virtual platform on the host computer and is one of the key components of the cloud. This hypervisor scenario is modeled on fictional scenario from Lloyd's, Counting the cost: Cyber exposure decoded (London: 2017), p. 27, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost.

customer data. The hackers zeroed out approximately 120,000 accounts and the integrity of customer data for nearly one million accounts was compromised.

That same day, July 4, the same hackers are believed to have simultaneously organized an attack that hit 5G-based systems nationwide. Combined with exploiting known vulnerabilities in edge computing devices, these 5G penetrations allowed the attackers to target routing infrastructure to effectively take down websites and impact a broad range of applications.

With most Americans home on that July 4 holiday, the attacker also used a malware that targeted IoT devices like IP cameras, home routers, and smart baby monitors, successfully infecting devices that did not encrypt data, change default admin passwords, or were designed to be unpatchable but hosted known vulnerabilities. Consumers' smart microwaves started fires as all programmed cook times were overridden and set to 90 minutes. Baby monitors played loops of disturbing sound clips from movies. Smart fridges locked or turned off unexpectedly. In hospitals, various IoT devices malfunctioned, including automated care systems, certain pacemaker brands, and remote surgical devices. These incidents led to botched surgeries, improper care, and casualties. In some hospitals, workers failed to recognize the scope of the misfunctioning hardware until they heard about the attacks on the news.

Those attacks persisted for several days, and just as they seemed contained, hackers targeted AVs in several ways. First, they deployed AI-enhanced malware targeting common architecture in the two most widely deployed models of AVs, giving the attackers root access to implement a one percent correction in direction. Second, a backdoor in Chinese-manufactured chips broadly used across level-five AVs and below was created, allowing hackers to gain control of tens of thousands of vehicles, disabling some and crashing others. Responses from passengers and drivers ranged from shutting down operations, to failure to notice the subtle changes to vehicle behavior, to overcorrections that led to traffic pileups and pedestrian casualties. There was a lag between the first instance of this hack and media warnings to stop using AVs. This instance, combined with the malfunctioning of smart transit systems that automate traffic for efficiency, was responsible for the majority of casualties.

Accompanying these attacks was a nearly simultaneous online information operation from dozens of fake social media accounts that were rapidly picked up by mainstream media and amplified by social networks. The information campaign sought to blame a fake terrorist group with claims that the group also had gained control of U.S. nuclear command and control systems and military networks. Hackers simultaneously leaked what were proven to be fake audio recordings of a conversation between the president and chairman of the joint chiefs of staff on the situation in which both sounded panicked and confused. Generative adversarial network-created (AI) fake images and videos of the meltdown of a nuclear plant and of airplane crashes in several major cities were also leaked. This led to the cancellation of school classes, early dismissal of employees from work, and traffic and transportation chaos in cities around the country. Riots and looting occurred in Chicago and Los Angeles. This episode of panic and distrust was so severe that local aid stations were often unvisited, and it was hard for emergency responders to help victims. Additionally, there was a drop in the

number of volunteer responders, as most people wanted to stay with their families, isolated from crowds and others.

The second phase of attack occurred two days later. While the first phase appeared to target individuals, the second phase targeted infrastructure. There were no demands or communication before the second phase; as such, it seems like the actor's intent was to rip apart all aspects of public and private life in the United States. The attacker targeted the power grid systems in New York, Washington, D.C, and Portland, Oregon.[15] Forensics indicate that hackers attempted to use 5G linkages connecting various cities' smart grid systems and the power grid at large; however, the main outages resulted from successful phishing attacks that gave the attackers control over operational technology (OT) systems and the ability to disable alarms. In order to improve efficiencies and meet changing demands, power plant operators have been integrating IT with OT systems, which exposes the power grid to higher cyber risk and means that a breach in the IT system could carry over into the OT system. These attacks resulted in fires and caused a sustained blackout that lasted around 24 hours in New York and Washington, D.C. and created rolling blackouts and brownouts throughout the East Coast. Portland's power was back online in 12 hours, supplemented by other cities on the West Coast. The attacks on the East Coast proved to be more damaging, shutting down the New York Stock Exchange and causing a surge in fatalities as backup systems failed in the intense summer heat. Communication lines were compromised and this lack of connectivity between family members and friends, the public and first responders, and individuals in government caused significant delay in responding to emergencies and working to rebuild after the events.

Hackers also compromised municipal water SCADA systems in Portland, Oregon, Washington, D.C., and New York connected to the hacked smart grid systems and decreased the quantity of chemicals used to treat the water while simultaneously disarming safety mechanisms. It took utility providers one week to realize the extent of this manipulation. In the meantime, illness cropped up in certain neighborhoods due to untreated water. Once the issue was exposed in the media, an online information operation claimed that the problem was sweeping in scope across the United States and water was no longer fit to drink anywhere. This led again to public panic, leading to the need for public leaders across the country to conduct water quality tests and reassure the public in various ways.

As markets reopened following a weeklong shutdown, stocks recovered somewhat from their historic plunge. Polling indicates a sharp loss of confidence in core institutions, from government to media and corporations. Long-term effects are still being revealed and neither the government nor the American public know what may happen next. The IC believes that electronic health records, biometric data, and additional banking information was also compromised during the attacks and could be gradually leaked or used in malicious ways in the future. In various cities, officials have begun to weigh the benefits of returning to 4G infrastructure due to

15. With the introduction of smart grid technology that utilizes IoT devices for functions such as sensing and measuring, the vectors of attack have increased.

the compromise of edge computing devices. There is an increase in suspicion of foreign technology, which is being blamed for the disaster in some pockets of the country. There is also a growing backlash against adopting new technologies, with a government-ordered stop on all new AV sales and calls for a voluntary disabling of AV features until the systems can be patched against attack. The reaction from the public continues to be one of fear, as every aspect of their lives–from private to public–was affected. Some continue to sleep outside or cut power off to their homes at night for fear of attack.

Appendix C: 2019 Global Security Forum Pre-discussion Questions

The four questions listed blow served to guide the discussions during the seminar portion of the event. The questions were based on our initial understanding of the state of emerging technologies governance and policy conversation surrounding it.

What is the right balance of proactive and defensive protection efforts to gain/sustain a U.S. edge in innovation (the U.S. "innovation base")?

- What is the appropriate role for the U.S. federal government in actively steering innovation through direct fiscal spending, tax incentives, and other levers?
- Where should export controls be focused, and where are they ineffective or counterproductive?
- How open should U.S. research education and employment be to all foreign nationals?
- How can and should the United States work with allies on emerging technologies governance?

What institutional gaps exist in current U.S. governance of emerging technologies?

- How can we deepen senior decisionmakers' understanding of emerging technologies?
- Should we design and assign a taxonomy to emerging technologies to better understand and govern them? Are there economies of scale and speed to be achieved through such an approach?
- Who in government should lead on emerging technologies governance?
- Are changes in interagency structure or process on emerging technologies governance necessary?

What gaps exist in international organizations, standards, and legal frameworks governing emerging technologies?

- How best should the United States work within existing constructs?
- What new constructs are necessary?
- What role should the international science and research community play?

What is the proper model for collaboration between the public and private sectors on emerging technologies governance?

- How do we strike the right balance between overregulation and under-regulation (address the Collingridge dilemma)?[16]
- What public-private partnership models could be most effective, and are these portable across emerging technologies, including those with research universities?
- Where do public and private interests diverge, and what can be done to productively navigate those gaps?

16. David Collingridge wrote in The Social Control of Technology (1980), "The social consequences of a technology cannot be predicted early in the life of the technology. By the time undesirable consequences are discovered, however, the technology is often so much part of the whole economics and social fabric that its control is extremely difficult."

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org