Bridging in the Valley: Technology, Politics, and Governance

A New Voices in National Security Workshop Report

Jane Darby Menton

Bridging the Gap Rapporteur

Research Scholar, UC Berkeley Risk and Security Lab

Executive Summary:

In November 2023, the New Voices in National Security Workshop sponsored by Bridging the Gap convened at Stanford University's Center for International Security and Cooperation in collaboration with the University of California, Berkeley's Risk and Security Laboratory to discuss technology, politics, and governance in an era of renewed great power competition. The workshop was convened by Andrew Reddie, Director, Bridging the Gap, and Associate Research Professor of Public Policy, UC Berkeley and Jim Goldgeier, Senior Adviser, Bridging the Gap, and Visiting Scholar, CISAC, Stanford University.

While previous workshops have focused on bridging the gap between academic research and government policy-making, this workshop—the first to be held in the Bay Area—brought the private sector to the table. Throughout the workshop, representatives from the university, government, and private industry shared their perspectives on the changing relationship between industry and government, the role of innovation as an arena for strategic competition, and the opportunities and challenges of both collaboration and regulation. The day concluded with a deep dive on artificial intelligence technologies. This memo synthesizes the day's discussions, noting key themes, areas of consensus and dissensus, and open questions that might be of interest to scholars and practitioners alike.

Notably, the relationship between government and private sector is shifting in the wake of strategic competition, with firms at the technological frontier continually engaging with government interlocutors to both shape—and take—regulation. At the same time, there are real challenges and questions associated with the externalities of government efforts to bolster

domestic industry—with impacts on the pace and price of innovation. Characterizing these challenges and associated costs and benefits represent clear places where scholarly work has a role to play.

New Voices in National Security is an initiative of Bridging the Gap, generously supported by the Raymond Frankel Foundation. This workshop was held at Encina Hall at Stanford University on November 3, 2023.

Introduction:

Strategic competition is bringing the government and the Valley closer together. In a recent workshop, held at Stanford University's Center for International Security and Cooperation, the Bridging the Gap New Voices Initiative convened a select group of academics, policymakers, and industry representatives to discuss issues related to technology and innovation in a period of renewed geopolitical competition. This day-long workshop explored the shifting relationship between Washington and Silicon Valley, the role of innovation in an era of strategic competition, and the importance of—and obstacles to—effective collaboration and technology governance.

Throughout the day, participants highlighted dynamics that are simultaneously reshaping industry-government relations. On the one hand, as tensions between states intensify, the United States is embracing tools of economic statecraft, in general, and industrial policy, in particular. This "securitization" of technology policy means that in more cases, interacting with the government is no longer a matter of choice for firms. As one participant put it, "even if you're a company that doesn't want to do national security, national security is being done to you." The PRC's preoccupation with technology as a critical domain of competition means that the United States cannot afford not to compete. In some cases, foreign actions, from IP theft to predatory trade practices are also bringing industry and government interests into closer alignment. At the same time, growing awareness of technological risks means that technology companies writ-large are facing heightened regulatory scrutiny at the national and international levels.

As export controls, technology governance regimes, and the changing policies of foreign states alter the pragmatic contours of industry-government relations, events are shifting perceptions of world politics. As many participants noted, Russia's invasion of Ukraine shattered the private sector's complacency about geopolitics, exemplified by past episodes such as private sector dissent in the wake of Project Maven, precipitating a cascade of voluntary commitments that directly implicated companies in U.S. foreign policy. Increased

awareness of the role of emerging technologies on the battlefield has also triggered an influx of money into the private sector.

At this point, it is unclear whether Ukraine will be seen as a precedent or an exception. Government and industry incentives may not align so neatly in future conflicts, and the haphazard nature of these engagements presents its own challenge. That said, the current conflict has already altered the way industry and government are relating to each other.

Given the breadth and immediacy of questions related to technology in an era of renewed geopolitical competition, conversations touched upon a wide range of issues, from Pentagon procurement policies to the challenges of AI governance. This memo summarizes the day's discussions, noting key themes that emerged from each session, as well as areas of potential inquiry going forward.

Risk and Emerging Technologies: A Silicon Valley Perspective

The workshop opened with a session showcasing industry perspectives on the state of engagement between Washington and Silicon Valley. Participants discussed the impact of strategic competition on the private sector and the successes and frustrations of public-private partnerships. Several themes emerged from these conversations:

Public-Private Partnerships (PPPs) are critical for strategic competition, but upscaling collaboration is not always easy. Workshop participants broadly agreed that the pace of innovation, coupled with the semi-sovereign control that private companies exercise over security-critical domains such as space, information, and cloud computing, means that the U.S. government will need to work with industry to maintain and wield its competitive edge in the technology sphere. For example, speakers argued that the only way the United States can build a sufficiently diversified and resilient space architecture in time to compete is by leveraging the commercial space sector.

Reflecting on the recent past, speakers posited that successful PPPs:

- *Connect the right people*. Multiple speakers highlighted the importance of human capital and the need to thicken the connective tissue linking Washington and Silicon Valley. Interpersonal connections played a key role during the early days of the Ukraine war, when companies such as Google and Microsoft stepped in to help protect Ukraine's information architecture and counter Russian disinformation campaigns. Participants also noted the importance of sending the right people to the right rooms, for example, connecting technical experts in government and the private sector.

- *Insulate security-critical capabilities and relationships from the whims of individuals*. Although many PPPs during the Ukraine war emerged organically, several participants noted the importance of locking in key partnerships with contracts.
- *Help companies balance innovation and safety*. Companies at the technological cutting edge can work with the government to ensure that emerging capabilities are used in a safe and responsible manner.
- *Articulate a clear problem statement*. Both sides need to be able to understand the purpose and objectives of the partnership. Companies without government experience cannot always parse what the government is asking for.

There are, however, dynamics that complicate industry-government collaboration.

- *The government is not a great customer.* Byzantine appropriations, procurement, and certification processes make it harder for policymakers to partner with industry. Lengthy and opaque budgeting processes in particular undermine attempts to inject competitiveness into the defense industrial base and make it harder for the government to leverage and wield capabilities that are commercially available. Approximately two-thirds of procurement dollars still go to only six vendors, and Congress has been reluctant to offer the Pentagon more expansive and flexible authorities.[1] Speakers also noted that the Services remain somewhat skeptical of emerging technologies.
- *U.S. tech companies are beholden to multiple national stakeholders*. Many American companies serve global customer bases, rely on globalized supply chains, solicit foreign capital, and are subject to increasingly fragmented regulatory standards. To maintain market access, industry must navigate the demands and constraints of multiple national governments. Going forward, companies like Google may find it harder to balance their national and multinational identities and commitments.
- *Successful PPPs can trigger backlash*. These partnerships can be weaponized by parties seeking to disassemble collaborative efforts. For example, Russian disinformation campaigns have targeted cooperative initiatives designed to mitigate them. There is an endogeneity in some of these threats that impacts solutions.

The Valley is not a monolith. Roughly speaking, technology companies can be distributed along two axes. The first is *scale*. At one extreme are actors like Google, Microsoft, and Meta, which possess capabilities and resources that rival those of many nation-states. The other end of the spectrum is populated by early-stage startups, with limited resources and personnel. Companies also differ in terms of *scope*. Some entities, such as Anduril and Palantir are

[1]For example, projects like the DoD's Replicator Initiative have not been formally allocated funding, although policymakers are trying to work around this by drawing from already-funded programs.

conscious participants in the defense ecosystems, and certain sectors such as commercial space have obvious security relevance; however other companies may be ignorant of their strategic significance. Although industry-government interactions are increasing across the board, different types of companies have different concerns, priorities, and capabilities, which drive patterns of engagement on both sides.

- *Some companies are better positioned to work with the government than others*. For example, bigger players are more resilient to erratic payment cycles than small startups because their viability does not depend upon government contracts alone. Other enablers of collaboration include prior connections to the government, experience navigating the procurement ecosystem (or access to those who can advise), and clear alignment between commercial products and government priorities.
- *While some companies are trying to work with the government to shape the policies and regulations to which they are subjected, others, especially smaller startups, are more concerned about mitigating their exposure to political risks*. The revival of strategic industrial policy impacts companies that are not directly interfacing with the government by disrupting supply chains and input costs and increasing regulatory exposure.
- *Private companies are not always aware of their relevance to national security*. One example that participants raised is biotechnology. Although China is prioritizing leadership in this arena, many American biotech startups do not see themselves as integral to national security. In such cases, the government might need to assume a more active role in evaluating the strategic importance of emerging technologies, supporting critical industries, and elucidating the security implications of business decisions.[2]

Silicon Valley and Great Power Competition

In the second session, a mixed panel, drawing from government, academia, and industry addressed the role of innovation in an era of renewed strategic competition. Building off of the morning's conversation, this session focused on the increasingly complex relationship between industry, government, and the academy, given the resurgence of economic statecraft and the emergence of various initiatives to govern and mitigate technological risks. A few takeaways emerged from this session.

[2] Participants raised the example of biotechnology startups that build their own models but rely on contractors to manufacture molecules. This is a potential security concern that may not be immediately obvious to companies that are optimizing for efficiency and product quality.

The tension between innovation and national security is real, and it is playing out in the regulatory space. The "Wild West" days of unfettered innovation are over. National governments and international bodies alike increasingly perceive risks that pertain to emerged and emerging capabilities, and they are actively seeking to govern them. Rather than debating whether or not regulation is desirable, participants focused on how to regulate, where to regulate, and who is—and should be—at the table. Several themes emerged:

- *Regulatory standards are becoming balkanized*. Simultaneous initiatives at the international, regional, national, and even local levels are creating an increasingly fragmented governance ecosystem.
- *Technology governance has cross-border implications*. For example, when the EU mandates that companies report certain kinds of harm, they are obligated to comply regardless of where they are operating. More broadly, there is a first-mover advantage when it comes to tech sector regulation. External strictures can trigger proactive self-regulation, shaping how companies approach and evaluate risks going forward.
- *Although intergovernmental processes have limitations, companies struggling to navigate an increasingly complex business and geopolitical ecosystem might benefit from more systematic and sustained engagement with existing forums.* This includes various UN processes, multilateral export control regimes, and Internet governance organizations such as ICANN, the International Telecommunication Union (ITU), and the Internet Governance Forum (IGF). Participants also noted that the dearth of U.S. leadership has created space for authoritarian states to co-opt various multi-stakeholder governance frameworks.

Industry, Academia, and Government face distinct hurdles when it comes to bridging the gap in an era of strategic competition.

- The government is interested in emerging technologies, but it lacks capacity and expertise in many core areas. The gap is particularly acute outside of the Pentagon, in other parts of government, including Commerce and State. Although recruiting STEM talent is important, some participants noted that upskilling will only get you so far. Speakers also stressed the need to encourage people who have worked in government to return to the Valley.[3]
- At this point, most technology companies are reacting to great power competition rather than proactively anticipating the attendant risks. Participants suggested that the power of some of these companies can belie their youth. Google just turned 25. Most tech CEOs are under 60, and the average tech worker is even younger. Although they are enmeshed in global markets and supply chains, even the largest players in the

[3] Participants noted that this is already happening at a smaller scale.

private sector have limited experience with geopolitics and are immersed in different cultures and expectations than those working in government. Tech companies are also profit-seeking entities, which are not incentivized to invest time or capital in research that does not directly impact their bottom line. When exchanges with the government and the academy—such as this workshop—do occur, they are usually on industry's free time (and dime).

- Junior academics are not encouraged to work with private companies and may even be penalized for such engagements. Participants also questioned the role of the university in the innovation ecosystem going forward, noting the gravitation of STEM talent to high-paying private-sector jobs and the concentration of certain kinds of research in corporate rather than academic settings. For example, universities do not have access to the computing power needed to build foundation AI models. Proposals, such as creating a National AI Research Resource, might be one way to address questions of access.[4] Participants also discussed the kind of work that would be mutually beneficial for industry, academics, and government. Suggestions included research programs on technology ethics and public policy.

"The AI": Regulation and Governance

The day concluded with a deep-dive on artificial intelligence technologies. Participants discussed the role of AI in strategic competition, as well as various issues pertaining to security, safety, and governance. These conversations were particularly timely, given that the White House had unveiled the Executive Order on "The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" days before the workshop.

The conversation about AI governance is expanding and evolving. Recent attempts to govern AI have emphasized slightly different issues. For example, the EU AI Act primarily focuses on use cases, while the White House's voluntary commitments look at frontier models. The Biden Administration's recent Executive Order takes a more holistic approach, addressing foundation models and downstream effects such as AI-human interactions and post-deployment performance.

- *Although the major AI companies have developed and implemented their own standards for responsible development and deployment, governments and intergovernmental bodies are getting more involved in shaping regulatory best practices and criteria*. Recent developments on this front include the Biden administration's announcement that the Department of Commerce, via the National Institute of Standards and Technology

[4] Others noted factors beyond compute—such as low salaries, job precarity, and inefficient hiring practices—which are driving many young people to pursue jobs in the private sector.

(NIST), will establish the U.S. Artificial Intelligence Safety Institute to spearhead the government's policies on trust and safety and operationalize NIST's AI Risk Management Framework.
- *There may be more creative ways to involve the public in conversations about AI regulation and governance*. Although the public has been largely excluded from these discussions to date, participants discussed various ways to involve end-users in the regulatory process by harnessing tools of deliberative democracy such as public assemblies.

Evaluation is the basis of regulation. Voluntary and mandatory reporting plays a crucial role in various AI safety and governance frameworks, but participants noted that core questions about appropriate standards of assessment, and who is—and should be—doing the evaluation remain unresolved. Participants identified this as a key area for investment and improvement. It is hard to manage what cannot be measured, and participants called for greater transparency and specificity about how emerging capabilities are being used. The speed with which capabilities are evolving amplifies the challenge of measurement. Getting things right will likely be an iterative process.

Experts in the field disagree about what AI safety means and where the greatest risks lie. Discussions touched upon the difference between risks that are framed as existential and the way AI can amplify existing problems such as disinformation, discrimination, and fraud, or democratize access to harm-enabling knowledge. Some participants suggested that it might be useful to disambiguate concepts such as risk, safety, and security. Participants also discussed the value and hazards of information-sharing and the challenge of building institutions that allow companies to be transparent about potential vulnerabilities without compromising national security or enabling insider threats.

Open Questions and Points of Dissensus:

- **How deep is the shift in industry-government relations?** Despite observable changes at the macro-level, some participants cautioned that even today, most companies primarily think about the government in terms of regulatory exposure and financial risk. Technology companies are profit-seeking entities, which focus on issues that are orthogonal to government priorities. Industry-government relations will never be one-track, and private actors that are not selling directly to the DoD are unlikely to prioritize national security, even if they are affected by strategic industrial policy.
- **Are we focusing on the right things?** What is the appropriate balance between developing, acquiring, and fielding exquisite capabilities versus ensuring that the government can scale and mass-produce more quotidian technologies?

- **What are the negative externalities of strategic industrial policies and how can these interventions be improved?** Recent policies such as the CHIPS and Science Act reflect a fundamental shift in industry-government relations, but some participants cautioned that they may have unintended consequences. For example, focusing too much on slowing down the PRC could come at the expense of harnessing and explaining the benefits of emerging technologies to domestic and international audiences. Others suggested that there might be better ways to do strategic industrial policy, for example, developing firmware rather than KPI-based export controls.
- **What bottlenecks should regulators be targeting?** Experts in the field disagree about what technology governance regimes can and should be focusing on. For example, because information and data are difficult to control, many conversations about AI regulation emphasize computing, but some participants cautioned that such regimes may be difficult to verify. Other areas of dissensus included looking at content generation versus the infrastructure of dissemination. And while some problems precipitated by technology may be amenable to technical solutions—for example, watermarking artificially generated content—others might require a more political approach.
- **Where is the frontier between what the government should own and what it should buy?** What are the legal and ethical implications of the DoD relying on private companies for security-critical services? Who owns the problem set when companies provide services that another state might perceive as an act of war?
- **What does successful cooperation between industry, academia, and the government look like in an era of strategic competition?** What would constitute a win-set in terms of analytical outputs?