TECHNOLOGY:
FINDINGS AND RECOMMENDATIONS

The Penn Project on the Future of U.S.-China Relations presents the following findings and recommendations from its Technology group. The policy papers on which they are based, a video of the October 30th webinar featuring these authors, and additional information can be found on the Project website.

China's Surveillance State at Home & Abroad: Challenges for U.S. Policy

Sheena Chestnut Greitens, University of Texas at Austin

Findings:

1. Under Xi Jinping, China has developed a surveillance state of immense scale and ambition, focused on "prevention and control" of risks to social stability and CCP rule, utilizing technology as a key tool through which the regime's preventive aims are to be achieved.

2. The rise of China's surveillance state has had significant global consequences. Over the past decade, Chinese surveillance and policing technologies have been adopted in more than 80 countries, both democratic and autocratic, on almost every continent.

3. China's supply of, and global demand for, these technologies have fueled their adoption. To craft an effective response, policymakers must address both aspects.

Recommendations:

1. The United States should formulate a coordinated inter-agency strategy that addresses the development and spread of Chinese surveillance technology, to provide an overarching vision, shared lexicon, and reference point for assessing policy tradeoffs. It should also develop a process for tracking and evaluating the spread of Chinese surveillance technology.

2. This inter-agency strategy should tailor messages to particular national circumstances; address the incentives facing subnational officials who decide whether to adopt Chinese surveillance technology; account for the governance challenges that underlie their decisions; and devise a plan for standard-setting in multilateral settings.

Penn Global
UNIVERSITY of PENNSYLVANIA

Penn Arts & Sciences
Center for the Study of
Contemporary China

HENRY LUCE FOUNDATION

3. U.S. strategy should also address cases in which eliminating existing Chinese surveillance technology may not be feasible. In such cases, the U.S. should advance technical and legal safeguards to protect data security and prevent the erosion of democracy.

4. Domestically, the United States must continue to maintain its own edge in technological innovation. It must also pursue an approach to the Chinese diaspora that accounts for the need to recruit and retain global tech talent and simultaneously pursue effective counterintelligence without alienating an important and valuable community through indiscriminate, unfair targeting.

Beyond Huawei and TikTok:
Untangling U.S. Concerns over Chinese Tech Companies and Digital Security

Robert D. Williams, Paul Tsai China Center, Yale Law School

Findings:

1. The growing importance and omni-use nature of technologies such as 5G telecommunications and artificial intelligence magnifies security risks and makes it more difficult to distinguish data security from national security. U.S. policymakers see these risks through a lens that focuses on China's declared strategic ambitions and the weak legal constraints on the CCP's ability to exercise power over Chinese tech companies, among other systemic factors.

2. Chinese tech companies like Huawei and ByteDance/TikTok illustrate the omni-use problem, the complex relationship between national security and data privacy, and the impetus for defensive U.S. policy responses based on assessments of China's governing system.

3. Despite the widespread, multifaceted nature of cybersecurity challenges and related issues posed by Chinese tech companies, U.S. policy has been largely reactive and focused only on a few companies, with Huawei and ByteDance/TikTok the most prominent to date. A more broadly applicable, politically sustainable, and multilateral approach would better serve U.S. interests.

Recommendations:

1. The U.S. should establish a comprehensive data privacy and cybersecurity framework that includes a national privacy law setting high and enforceable standards for data collection and processing. The U.S. also should rationalize its cybersecurity liability regime to better incentivize "cyber hygiene." The U.S. should launch a multilateral digital trade initiative to promote an appropriate balance between concerns of data security and interoperability.

2. Cognizant of escalation risks, the U.S. should find creative means to disrupt and deter malicious cyber operations from countries like China. These include forging a multilateral coalition to enforce norms against commercial cyber-theft and other destabilizing activities.

3. The U.S. should establish an interagency coordinating group with oversight power over prospective technology policies such as export controls, entity listings, supply chain risk standards, immigration policies, and subsidies. This group should work to ensure that federal policies are developed in coordination with multilateral partners where possible, and sufficiently tailored to protect sensitive technologies without cutting off essential flows of data, investment, and human capital.

Shaping Global Technology Governance:
Why the U.S. Must Adopt a Proactive Approach to Technical Standards for Long Term Security

Julia Voo, Harvard Belfer Center for Science and International Affairs

Findings:

1. Technological primacy has afforded the U.S. great *de facto* influence in standards-setting organizations, but this influence can no longer be taken for granted as the capability gap between the U.S. and China closes.

2. China's intention to become a global technology leader will not diminish and its effectiveness in influencing international technical standards will increase. U.S.-China competition on technology is unlikely to subside. Though tensions will continue, a bifurcated system does not serve U.S. long-term interests.

3. China has steadily increased its influence in many standards-setting organizations, including through the cultivation of highly skilled, technical experts who serve in these bodies. The U.S. has not invested the levels of resources necessary to build a similar cohort.

4. The U.S.' emphasis in standards-setting organizations has been "to maintain the status quo." But the global standards development ecosystem is broken, and internet governance remains highly fragmented, duplicative, and inefficient.

Recommendations:

1. The U.S. government should work with industry to develop a strategy to shape global technology governance through the international rules-based order and by seeking a greater share for the U.S. in key markets for technology products.

2. The U.S. should collaborate with China in standards development in certain areas, in order to promote global innovation.

3. The U.S. should promote U.S. university degree programs focused on technical standards in order to cultivate a new cohort of experts on technical standards.

4. The U.S. should develop a vision for global technology governance that would streamline the system for developing global standards.