Prepared Statement
by
Honorable Eric Rosenbach
Co-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School
Former DoD Chief of Staff; former Assistant Secretary of Defense for Homeland Defense and Global Security

Before the
United States Senate Committee on Commerce, Science and Transportation

Hearing on "China: Challenges to US Commerce"

Chairman Sullivan, Ranking Member Markey, other distinguished members of the sub-committee on security, thank you for calling this important hearing on "China's Challenges to US Commerce" and for the invitation to testify today.

This hearing is important: China is moving very quickly into the Information Age with a strategic approach that bolsters their national interests. The United States, on the other hand, seems to be standing by, beholden to large technology companies focused primarily on connecting more people to generate more data to further bolster their profits. In the absence of a national strategy to protect Americans' data, promote the competitiveness of American firms, and secure our information and technology infrastructure assets, the U.S. risks ceding its leadership role in the future economic, military, and political landscapes.

The Information Age

This is the Information Age. And information is now the world's most consequential and contested geopolitical resource. The world's most profitable businesses have understood for years that data is the "new oil." Political operatives – and, unfortunately, foreign intelligence operatives as well – have shown over the past two presidential elections that data-driven social media is the key to influencing public opinion. Leading researchers in the area of artificial intelligence know that good data, not just algorithms, will allow companies, and nations, to gain a competitive edge.

Data-driven innovation is not only disrupting economies and societies; it is reshaping relations between nations, and there is no better example than the US-China relationship. The pursuit of information power – involving states' ability to acquire, refine, protect, and use information to advance their interests – is changing strategic priorities. In the current US-China trade negotiations, for example, IP theft and state-support for tech companies is on the table next to soybean and automobile tariffs. American policymakers are questioning a long-standing tenet of the US economic system: openness to foreign investment. In short, the pursuit of information power is altering strategic and economic relations between nations.

In the 1990s, America's supremacy in information technologies and the internet seemed unassailable. Unfortunately, as the importance of information as a geopolitical resource has waxed, US dominance has waned. States with authoritarian forms of government – and China in particular – first recognized the strategic importance of information, and have adapted their national laws and policies accordingly. America's economic competitors believe they are locked in a zero-sum competition to create, collect, buy or steal data, and to develop the talent and technology to convert it into strategic advantage.

Data held by both corporate and government entities has more strategic value than ever before because of its importance in developing artificial intelligence. A technical wunderkind is no longer as critical to writing a good AI learning algorithm; instead, what developers most require are troves of high-quality data to train and optimize algorithms over time. As a result, states have a strong interest in developing, accessing or stealing commercial, private and government data necessary to train and optimize AI algorithms.

Indian Prime Minister Narendra Modi, for example, believes that "whoever acquires and controls" data will attain "hegemony." In his recent book *AI Superpowers,* venture capitalist Kai-Fu Lee predicts that China's widening lead in artificial intelligence will not only ensure the "economic balance of power tilts in China's favor," but will tilt "political influence and 'soft power,' towards China," and cement its "cultural and ideological footprint around the globe." Most developed economies now have national "artificial intelligence"strategies. None are more mercantilist than China's "Development Plan for a New Generation of Artificial Intelligence," which aims through a combination of government subsidies and incentives to push China into leading the world in AI by 2030.

The Competitive Threat from China

Over the past decade, China has pursued a national strategy to challenge the United States' global leadership in the Information Age through a conscious strategy of state-backed investment, loose consumer data privacy protections, a centralized AI and technology deployment strategy, and intelligence operations to steal crucial data and intellectual property.

The Chinese government has invested heavily in the research and development of technology that underpins supercomputing, artificial intelligence, broadband networks and big data. Those investments have resulted in genuine achievements. In 2016, for example, China unveiled the world's fastest supercomputer – and announced that it owned more of the top 500 supercomputers than any other nation in the world. Chinese firms and research institutions, nearly always supported with state funds, have made advances in artificial intelligence that some corporate leaders believe will make China the world leader in hardware-based AI.

President Xi has also advanced his nation's strategic plans by developing and supporting firms in key areas of economic power with state-sponsored loans, contracts and research and development. One of the best known of these Chinese "national champions" is Huawei, now the largest telecommunications equipment maker in the world. The significant resources Huawei derives from the backing of the Chinese government puts American and European telecommunications equipment providers at a clear disadvantage, particularly when it comes to

developing and deploying some of the technology necessary for next generation broadband networks.

The Chinese government has also devoted significant military intelligence capabilities to steal the data and intellectual property needed to fulfill the ambitious goals established for President Xi's "Made in China 2025 Plan." Over the past decade, Chinese intelligence officers from the People's Liberation Army (PLA) have conducted thousands of cyberattacks against both private sector and government targets. The Chinese, for example, were almost certainly responsible for the hacks and the theft of hundreds of millions of Americans' data from the Office of Personnel Management, Marriot, Anthem Health and Equifax. Although the PLA undoubtedly used this for intelligence purposes, it's highly likely that this high-quality data was also used to help the government-sponsored development of AI capabilities.

Over the past decade, Chinese intelligence operatives have been equally aggressive in systematically stealing intellectual property and trade secrets from American organizations essential to national competitiveness. "More than 90 percent of the department's cases alleging economic espionage over the past seven years involve China," deputy attorney general Rod Rosenstein said after an indictment unsealed in December 2018.

The Obama Administration's response to these attacks was slow and initially weak, but by 2015 the Administration finally recognized the need to confront Chinese leadership with explicit attribution, sanctions and improved cyber defenses. These actions resulted in a short-term drop in Chinese cyberattacks against the US. Over the past 18 months, however, Chinese cyber operations have resumed. In the most recent annual national threat assessment, for example, Director of National Intelligence Daniel Coats said that, "China will continue to use cyber-espionage and bolster cyberattack capabilities to support [its] national security priorities." This past December, the FBI's top counterintelligence official asserted that, "Our prosperity and place in the world are at risk."

What Congress Must Do

As the Information Age advances, the United States needs to recognize that data collection and technology deployment are critical both from the perspective of economic competitiveness and national security. Looking over the horizon, adversaries will greatly increase operations to steal sensitive and valuable information in order to advance their strategic and economic advantage over the United States. Given the richness of data held by the largest companies and research centers in the tech, financial and healthcare sectors, it is highly likely that adversary intelligence services will expand their traditional targets to include corporate datasets that could be used to train AI systems and to hone information operations.

US policy responses to these threats should be centered around a few guiding principles:

1. **The Information Age demands a data-centric security and economic strategy:** America needs to develop a data-focused strategy for competitiveness. From a security perspective, a network-centric approach to national security is failing. Focus on the threat of a low probability catastrophic attack on critical infrastructure networks, for example,

has distracted leaders from the reality that we are not defending the nation's most precious resource: information. Likewise, the government has done very little to prioritize the centers of gravity for an economy powered for the Information Age.

2. **The privacy of personal information is a national security and economic priority.** Policies aimed at bolstering US national security and promoting US economic competitiveness must go hand-in-hand with consumer protection. Authoritarian governments may ignore consumer rights in pursuit of acquiring information power, but democracies cannot. Bolstering the global competitiveness of American companies should remain a top priority, but not at the expense of allowing these companies to collect, use, and sell information without user consent or under-invest in cybersecurity measures.

3. **America needs a whole-of-government strategy to improve national competitiveness in the Information Age.** Information geopolitics cuts across all aspects of the economy, society and state security apparatus. Authoritarian governments have adopted a highly centralized, mercantilist approach to protecting, acquiring and using information. Centralization will not be the answer for democracies, but coordination must be. Unprecedented cooperation is required, across economic, social, defense, intelligence, state department and homeland security portfolios. For example, the American government can no silo regulatory decisions about information-related companies separate from foreign policy decisions on cyberspace.

4. **Even further, America needs a whole-of-nation strategy that includes coordination with the private sector.** The US intelligence community needs to share threat information about foreign intelligence organizations with the social media platforms that so directly influence Americans' economic and political decision. Policymakers must be willing to work with private actors to ensure regulatory red tape does not stand in the way of innovation, and that public-private partnerships continue to create incentives to accelerate technology development. At the same time, American technology firms need to understand, and be held accountable for, their role in protecting national security interests.

These principles should be combined with forward-leaning policy action. Specifically:

- **Pass national data security and privacy legislation.** Information is and will be the nation's most import strategic resource for the next century. Yet, even in the face of inadequate data protection practices and damaging data breaches, the US continues to muddle along with a complex web of state-based and industry-specific requirements. American consumers are worse off because their data is unprotected and, in the event of a personally costly data breach, their rights and access to legal recourse are unclear. American companies are left to deal with competing and possibly contradictory requirements, in particular impacting early innovators and small businesses without the resources to navigate this complex environment.

US policymakers urgently need to pass a national law that will protect user data, reduce regulatory complexity, and spur innovation by reconciling differences in state and federal requirements. While Europe's General Data Protection Regulation (GDPR) is by no means a perfect model and in some respects is inconsistent with other US values, it has been effective at driving corporate investment in data protection. Data protection legislation passed in California in June 2018 will need fine-tuning before taking effect in 2020, but it establishes important principles that could serve as the foundation for national legislation.

- **Promote competitiveness of American firms:** China undeniably has an advantage in data collection, by virtue of its large population and weak data privacy protection policies. While data is an important input, it is not the only determinant of competitiveness in the information age. China's authoritarian system also gives it a deployment advantage, but the US can do a lot more to reduce regulatory red tape, attract top talent, and create other incentives to spur innovation.

    - ***Ensure regulation supports competitiveness of American firms in critical sectors.*** A key driver of the information age has been the exponential growth of high-speed wireless broadband infrastructure around the world. American firms are currently locked in a tight competition with Chinese powerhouses to determine who will dominate this important area. The US government – and the FTC in particular – should make sure that regulations designed to protect consumers and competition don't inadvertently undermine the competitiveness of American firms relative to Chinese national champions like Huawei.

    - ***Reduce regulatory red tape to expedite deployment of next-generation broadband infrastructure.*** Nationwide 5G deployment is a massive effort requiring equipment installation and associated permits and approval processes across thousands of localities. Yet without this foundation, the US risks falling behind in the next generation of wireless-enabled technologies. Policymakers must drive toward regulation that standardizes and fast-tracks local approvals, while giving local authorities the opportunity to provide implementation guidance.

    - ***Continue public-private partnerships that support advanced technology development.*** Within the framework of robust national data privacy and security laws, the US government should promote more partnerships with civilian companies and academic institutions to make progress on high-priority AI initiatives. For example, the Defense Innovation Unit - Experimental (DIUx), established by DoD for this purpose, provides a model for incentivizing the private sector to develop technologies with direct national security applications.

    - ***Win the race for talent.*** The US has a history of prizing and nurturing openness, creativity, and innovation. Our university system is a springboard for raw talent; our legal and government institutions allow new businesses to thrive; and our

sophisticated financial system enable the best ideas to be successful. To maintain a competitive edge, the US needs a foundation of policies and practices that continue to attract top talent, like the heads of AI at Apple, Facebook, Microsoft, and Google's cloud computing division, who were all born outside the US. The visa program is a good place to start -- at minimum, Congress should ensure that more highly skilled workers are able to obtain H-1B visas. Policymakers should further consider special programs for students and experts in the AI and broader set of STEM fields.

- **Protect American information and infrastructure assets:** Good offense that promotes US economic competitiveness must be coupled with good defense that bolsters the US system against foreign attacks and takeovers.

    - ***Incentivize use of strong encryption.*** Making America the world leader in encryption technology could advance both economic and national security interests. Protecting the nation's most important resource will require a significant expansion in the use of encryption. The nation's defense and security agencies have relied on encryption to protect its most precious secrets for many decades – DoD, in fact, is the largest user of encryption in the world. The US must both clarify the legal questions around encryption and develop real incentives to promote the use and growth of encryption products and platforms that allow individuals and organizations to protect their data.

    - ***Limit foreign ownership and provide resources to support firms in key information sectors.*** Over the past decade China has systematically targeted investment in and ownership of firms developing technology, such as AI, that will drive strategic advantage in the Information Age. Congress took encouraging action by reforming and passing legislation that increased limitations and oversight of foreign ownership and involvement in data-rich sectors. This was important, but should be supplemented with new sources of incentives to sustain American tech firms whose technology does not have an immediate commercial application.

- **Deter Chinese actions to steal our national resources by defending America's interests in cyberspace:** Our response to Chinese cyber-attacks that steal personal data and intellectual property has been weak, resulting in the perception by China that an attack on the American economy will not incur costs. The US needs a strong national response to demonstrate that interference with American information and infrastructure assets in any manner is unacceptable. We have to raise the cost of attacks and decrease the benefits that our adversaries seek.
    - ***Publicly attribute attacks to raise costs to adversaries.*** The increased willingness of the Intelligence Community, DHS, and FBI publically to attribute Chinese cyber attacks through indictments is crucial and positive first step.

- ***Develop precise and legal offensive cyber operations that change the current dynamic of America simply sitting back and absorbing the blows of adversarial actions***. Good defenses are important, but defense will not alone mitigate the threat of foreign attacks. To complement defensive measures, the U.S. government, led by the Department of Defense, needs to bolster its capabilities to disrupt and degrade Chinese cyber operations before they succeed.

- ***Improve intelligence sharing with the private sector.*** The Intelligence Community should also strive to share as much intelligence information as possible about Chinese cyber operations. In the past, the government has too often watched important intellectual property or data flow out of the country without warning impacted organizations.
