The New Big Brother – China and Digital Authoritarianism
Key Findings and Recommendations

Key Findings

- China's efforts to advance and proliferate its ICT hardware and systems, both in China and overseas, represent not only a desire to continually expand its economy, but also a push to establish, expand, internationalize, and institutionalize a model for digital governance that this report describes as "digital authoritarianism."
- If left unchecked, China, not the U.S. and our allies, will write the rules of the digital domain, opening the doors for digital authoritarianism to govern the Internet and associated technologies.
- To CCP leadership, the digital domain is a space that must be controlled by the Party. As such, development of new digitally enabled technologies must operate in line with Party principles. Without such control, CCP leaders fear these technologies could weaken the CCP's hold over its citizens.
- By building out so much of the digital infrastructure in the developing world, China could end up dominating a large portion of the global communications market, positioning it to potentially pressure other governments or conduct espionage.
- At the United Nations, China has played a counterproductive role in efforts to build consensus on a free and fair future of cyberspace. China's behavior echoes its consistent undermining of UN efforts that could highlight its own poor human rights record
- The Administration's current policy is insufficient to combat China's digital authoritarianism, and its alienation of allies has further stunted the United States' ability to influence other countries away from China's digital authoritarianism model.
- The surveillance system in Xinjiang has aided in the detention of possibly more than 2 million Uyghurs, ethnic Kazakhs, and members of other Muslim groups in Xinjiang, according to the U.S. State Department. In Xinjiang, Chinese government and police authorities retain what amounts to near absolute control of the entire ICT domain, and, through that control, have been able to repress and subjugate Uyghurs and other ethnic minorities in the region.
- Foreign technology platforms are restricted from operating in China, allowing Chinese platforms that offer similar services to thrive and expand into new markets. Thanks to this market inefficiency, China now retains some of the most valuable Internet companies in the world by market capitalization, including Alibaba, Tencent, and Baidu.
- The United States currently does not have a domestic 5G supplier for the equipment that makes up the Radio Access Network (RAN) for 5G. Instead, countries seeking viable alternatives to Chinese 5G RAN infrastructure rely on companies such as Swedish company Ericsson, South Korea-based Samsung, or Finnish firm Nokia to build out core components of their layer of the 5G infrastructure.
- The United States could find a future advantage by leading on mmWave technologies, since 1) this band is the spectrum where ultra-fast innovations may arise and 2) a fully actualized 5G network will see devices seamlessly utilize and transition between both the sub-6 and mmWave bands.

Recommendations

- It is critical that the United States government stimulate technological innovation in the United States by increasing government research and development funding, adopting a more extensive industrial policy, developing and attracting superior talent to the United States' technology sector, strengthening bilateral and multilateral technology initiatives with like-minded allies and partners, and ensuring a competitive advantage for domestic companies in overseas markets.
- Create an Industry Consortium on 5G: Congress should create a consortium comprised of leading U.S. telecommunications and technology companies that would be mandated to create the American 5G telecommunications alternative, exploring both cost-effective hardware and software solutions.
- Establish a Digital Rights Promotion Fund: Congress should establish and authorize a Digital Rights Promotion Fund, which will provide grants and investments directly to entities that support the promotion of a free, secure, stable, and open digital domain and fight against the authoritarian use of information and communications technologies. The fund will provide these groups, especially those existing in countries experiencing undue surveillance or other forms of digital authoritarianism, the resources needed to better push back against the spread of digital authoritarianism. Groups able to receive money would include:
    - Local activist organizations promoting a free digital domain and working to counter oppressive surveillance regimes in countries where digital authoritarianism is apparent or on the rise.
    - Nonprofit organizations that advocate for the adoption of international governance standards for the digital domain based on openness, transparency, and the rule of law, including the protection of human rights.
    - Think tanks and other institutional bodies that provide scholarship and policy recommendations for best paths forward to protect against the rise of authoritarian surveillance.
- Establish a Cyber Service Academy: Through legislative action, Congress should establish a new federal service academy similar to our other military service academies, with the specific aim of developing the future of our technology force. In addition to providing students a four year undergraduate education, the academy shall prepare students to become future military leaders in key digital and emerging technology fields, including robotics, artificial intelligence (AI), and cybersecurity.
- Build a Coalition of Likeminded Allies on Critical Technology Issues: The President should lead an international effort, in coordination with our allies and partners, to counter Chinese efforts to develop and proliferate digital domain products, technologies, and services that are not predicated on free, democratic values.
- Establish and Empower New Cyber Leadership within the State Department: Congress should pass the Cyber Diplomacy Act of 2019, or similar legislation, that establishes a new office or bureau of cyber issues at the State Department, which shall report to the Under Secretary for Political Affairs.