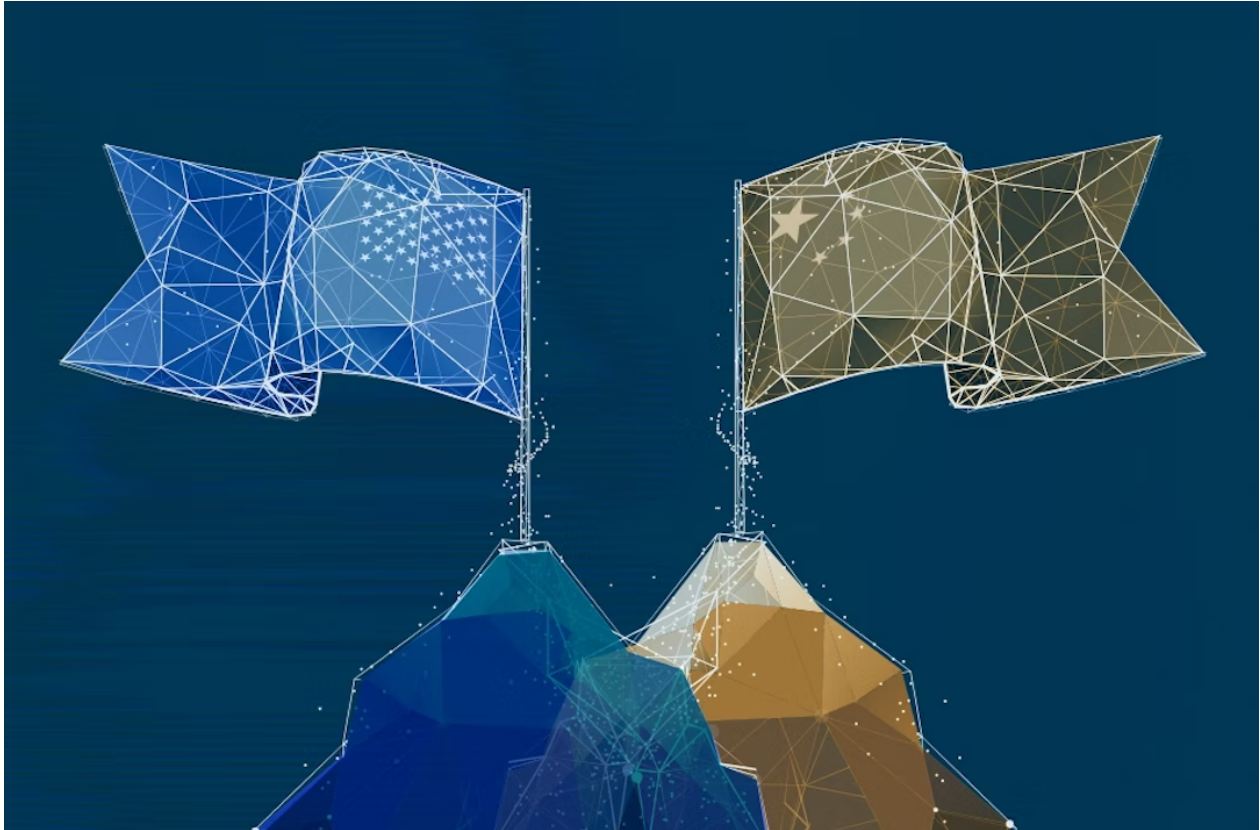


Introducing Third Way's US-China Digital World Order Initiative



Valerie Shen

Vice President for the National Security Program

[@ValerieShen](https://twitter.com/ValerieShen)



Jayson Browder

Visiting Fellow

[@JaysonBrowder](https://twitter.com/JaysonBrowder)

If it wasn't clear three months ago, it is clear now: the next global era will be defined by democracy versus autocracy. In this competition, a new and decisive divide pits America's approach of "digital democracy" against China's approach of "digital autocracy." This great divide places the US and allies on one side and China's unfettered access to sensitive data on the other.

China's digital authoritarianism has been described as "one giant QAnon" and is ubiquitous among the 1.4 billion inhabitants of the country. Moreover, one of the greatest threats to American national security interests is if China prevails in exporting and normalizing its model of digital supremacy. China's global network of surveillance systems is antithetical to liberal democratic values, as it monitors, punishes, and conditions citizens, as well as influences them through automated disinformation campaigns. China's ambition for global digital supremacy is real and supported by aggressive diplomatic efforts and massive financial investments.

The effort by the United States and like nations to maintain a peaceful and prosperous world order will require a level of sophistication and commitment unrivaled in our history. China is not only an adversary. It is sometimes a partner whose massive economy is deeply entwined with that of the US and other friendly nations. This is not the zero-sum game of the Cold War conflict, and the hope is that it never becomes so.

Will liberal democracies strengthen and proliferate or weaken and dwindle in the 21st century? The Chinese state intends to shape the global digital order in its image by redrawing technological norms and standards. Ultimately, the US-China national security competition may hinge on who sets the digital world order.

Third Way's US-China Digital World Order Initiative

Third Way's US-China Digital World Order Initiative will raise the alarm and develop the case that it is crucial for US national security to set the digital world order with our values and those of our allies instead of China's. The competition between “digital democracy” and “digital autocracy” is a must-win fight. Free speech, privacy rights, truth, human rights, accountability, and other cherished values of free nations need to form the backbone of how nations are expected to govern cyberspace and apply increasingly powerful technologies. We will form a network of experts in surveillance, disinformation, and advanced technologies to collaborate and help find and amplify solutions. This network will strive to be bipartisan and to seek input from the public sector, private sector, academia, think tanks, foundations, and like-minded partners overseas.



This initiative will emulate the influence of Third Way's groundbreaking nonpartisan Cyber Enforcement Initiative. The Cyber Enforcement Initiative showcased the effectiveness of Third Way's network and model for outsized policy impact, with its ideas finding their way into the Biden Administration, President Biden's Infrastructure Investment and Jobs Act, and the National Defense Reauthorization Act.¹ A first of its kind, this bipartisan initiative will ensure the delicate balance of serving American interests and liberal democracy without jingoism, and be the standard for how a democratic digital world order is developed and exported around the world.

Learning from History

The Cold War competition between the US and the Soviet Union is analogous but vastly different than the 21st century US competition with China. Mark Twain is famously quoted “History Does Not Repeat Itself, But It Rhymes.”² A superpower relationship now will be more complicated and fraught than in the 20th century, but lessons can be extrapolated to make the best policy decisions in this new area. These differences necessitate a new US approach and strategy for success, and it will spill over into digital supremacy competition. More fundamentally, the Soviet Union shared minimal economic and political interests so that damaging and undermining the Soviet Union was almost always in the US national interest.³ This is in stark contrast to the deep interdependence

shared between the US and China in trade and investment, in addition to several mutual national security interests as well as combatting climate change.⁴ China's maladroit endorsement of the Russian invasion of Ukraine will lead to some untethering of the US–China economic ties, but it is unrealistic to believe that the two largest world economies won't remain interconnected.

The US-Soviet conflict was measured by superior traditional weapons and military power—but the decisive weapons of the US-China conflict will be exceptional cyber and information capabilities. The US and Soviet Union rarely engaged in direct open warfare but did frequently battle through consuming and costly kinetic proxy wars such as the Korean and the Vietnam wars (from the US perspective) and Afghanistan (from the Soviet perspective).⁵ With China, it is less likely there will be kinetic warfare operations even by proxy. Instead, the main battlefield will be through non-kinetic, hostile cyber and digital operations. Rather than spreading the economic model of communism to defeat capitalism, China is exporting its authoritarian digital world order which will include its surveillance state model that will weaken and defeat democratic states.

	 Soviet Union 20th century	 China 21st century
Battlefield:	Kinetic proxy wars	Non-kinetic cyber operations
Weapons:	Throw-weights + Kilotons	Terabytes + Bots
Exporting Totalitarian Model:	Communism	Surveillance State
Aggression:	Spheres of influence, destabilize, ideology	Ubiquitous, amassing information, cyber
Narrative:	Capitalism is corrupt and will collapse	Democracy is dysfunctional and will collapse
Economies:	Separate and unequal	Intertwined and large
Mutual Interests:	Minimal	Significant
Economy:	Stagnant	Growing
Outcomes:	Zero-Sum	Non-Zero-Sum
Digital Global Order:	Communism v. Capitalism	Autocracy v. Democracy

Source: Introducing Third Way's US-China Digital World Order Initiative, www.thirdway.org/memo/introducing-third-ways-us-china-digital-world-order-initiative.



The US must champion a digital governance model built on core liberal democratic values that sets standards around the world. The US should lead a global effort to prioritize countering China's ambition to set the digital world order in its authoritarian image—and take major actions as soon as possible. To prevail against China under a long-term peaceful coexistence, the US must once again ensure that its vision of “digital democracy” succeeds against “digital autocracy” in the global arena.

What is at Stake for the Free World

China is executing a detailed plan to become the world's digital superpower. The US is not. As part of the state-driven “China Standards 2035” Project, the Chinese state intends to change the global digital order by redrawing technological norms and standards to outcompete the United States and dominate the free world with its authoritarian model for exportation.⁶ The outcome of this US-

China competition will define the 21st century and have massive implications on US economic, geopolitical, and military strength.

China’s model will enable an information dark age across autocratic nations where whole societies live in a completely distorted version of the world. Current trends point to a stark divide between democratic countries with freedom of speech and press, and authoritarian states with sophisticated disinformation and censorship regimes. Through technologies like the Great Firewall, 1.4 billion people in China alone have already been systematically shunted into state-controlled narratives for understanding the world.⁷ China is perfecting its technology-enhanced authoritarianism for export, and dictators like Vladimir Putin are signing up to better hide horrific truths from their citizens.⁸

China’s digital police state uses mass surveillance technologies and big data to restrain basic freedoms and liberties. Chinese state officials can track its citizens through voice recognizing-social media monitoring, artificial intelligence and facial recognition-enhanced security cameras, and Internet-enhanced neighbor snitching.⁹ This surveillance data is compiled into social credit scores and advanced algorithms to curtail the freedoms of dissidents and “deviants”—including blocking travel for civil rights lawyers, detaining ethnic and religious minority Uyghurs for praying, and punishing journalists for “spreading rumors.”¹⁰

The Chinese government also conducts operations to serve their economic and geopolitical interests by spreading and strengthening Chinese technological authoritarianism.

- **Exporting telecommunications equipment:** China made a billion-dollar market for establishing global digital infrastructure, while also using that same infrastructure to stifle overseas dissent and give similar tools of repression to their allies.¹¹
- **Stealing American intellectual property:** China has been able to supercharge their own tech economy and claim the Chinese state spurs innovation.¹²
- **Banning cryptocurrency and promoting the digital yuan:** China has dismissed decentralized economic power, and instead doubled down on their efforts to make yuan-transactions yet another means of global surveillance, as well as empower the yuan to be a global currency rivaling the US dollar in influence.¹³
- **Hacking into foreign governments:** China degrades the security of democracies through extensive cyberespionage operations. The collected data is used for further political and intelligence operations which target enemies of the Chinese government.¹⁴

The US government is recognizing the national security threat of China’s technological aspirations and cyber operations. In March 2021, the FCC recognized the risks of China’s digital control and designated several Chinese telecommunications firms, including Huawei, as national security threats to US government vendors and are restricted from conducting business with.¹⁵

The annual Office of the Director of National Intelligence’s threat assessment noted, “China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks” and the Chinese government “will work to undercut U.S. influence, drive wedges between Washington and its partners, and foster some norms that favor its authoritarian system.”¹⁶

China’s military buildup strategy also relies on gaining and maintaining the upper-hand in the digital global order. In addition to a traditional military arms race, Xi Jinping has recognized the importance of integrating digital superiority in China’s armed forces. Xi has called for a highly “informatized” military capable of dominating all networks, and to establish next-generation “intelligentized” warfare capabilities using advanced technologies like AI and quantum computing.¹⁷

What’s Next?

Over the next several years, Third Way will push policymakers to establish a comprehensive strategy to secure a democratic digital world order for the 21st century. As we inaugurate this new initiative, Third Way will explore and develop concrete, actionable recommendations that can serve as a realistic roadmap for US leaders to execute. We will develop solutions tailored for legislation in collaboration with our organizational partners and members of Congress. We will establish a non-partisan Advisory Board comprised of leading experts and policymakers on these issues. We will increase public awareness to amplify broad-based political support for the necessary actions to protect US national security.

TOPICS

US-CHINA DIGITAL WORLD ORDER 10

ENDNOTES

1. Peters, Allison, and Michael Garcia. "A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?" Third Way, 12 November 2020, <https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here#law-enforcement-personnel-and-capacity>. Accessed May 25, 2022; Clarke, Aaron, and Tom Klein. "2021 Year in Review: The Biden Administration's Efforts on Cybersecurity." Third Way, 25 January 2022, <https://www.thirdway.org/report/2021-year-in-review-the-biden-administrations-efforts-on-cybersecurity>. Accessed May 25, 2022; Garcia, Michael. "The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act." Third Way, 5 April 2021, <https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act>. Accessed May 5, 2022.
2. "History Doesn't Repeat Itself, but It Often Rhymes" – Mark Twain." Ohio Wesleyan University, Fall 2018, <https://www.owu.edu/alumni-and-friends/owu-magazine/fall-2018/history-doesnt-repeat-itself-but-it-often-rhymes/#:~:text=%E2%80%9CHistory%20Doesn't%20Repeat%20Itself,It%20Often%20Rhymes%E2%80%9D%20%E2%80%93%20Mark%20Twain>. Accessed May 25, 2022.
3. Li, Wei. "Why do we need to revisit the Cold War?." *China International Strategy Review*, 1–13. 28 Jul. 2020, doi:10.1007/s42533-020-00047-7, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7385715/>. Accessed May 25, 2022.
4. Lewis, Joanna. "The U.S.-China Climate and Energy Relationship." Center for Strategic and International Studies, 22 Sep. 2017, <https://www.csis.org/us-china-climate-and-energy-relationship>. Accessed May 25, 2022; Meltzer, Joshua; Shenai, Neena. "The US-China economic relationship: A comprehensive approach." The Brookings Institution, 28 February 2019, <https://www.brookings.edu/research/the-us-china-economic-relationship-a-comprehensive-approach/>. Accessed May 25 2022; *U.S.-China Counterterrorism Cooperation: Issues for U.S. Policy*, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 8 Jul. 2010, <https://sgp.fas.org/crs/terror/RL33001.pdf>. Accessed May 25, 2022; USIP China-North Korea Senior Study Group. "China's Role in North Korea Nuclear and Peace Negotiations." U.S. Institute of Peace, 6 May 2019, <https://www.usip.org/publications/2019/05/chinas-role-north-korea-nuclear-and-peace-negotiations>. Accessed May 25, 2022.
5. Blakemore, Erin. "What was the Cold War – and are we headed to another one?" *National Geographic*, 23 Mar. 2022, <https://www.nationalgeographic.com/culture/article/cold-war#:~:text=Multiple%20proxy%20wars%20stood%20in,all%20considered%20Cold%20War%20proxies>. Accessed May 25, 2022; Li, Wei. "Why do we need to revisit the Cold War?." *China International Strategy Review*, 1–13. 28 Jul. 2020, doi:10.1007/s42533-020-00047-7, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7385715/>. Accessed May 25, 2022.

6. Central Committee of the Communist Party of China and the State Council. "National Standardization Development Outline" 10 Oct. 2021, http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm. Accessed May 25, 2022; Gargeyas, Arjun. "China's 'Standards 2035' Project Could Result in a Technological Cold War." *The Diplomat*, 18 September 2021, <https://thediplomat.com/2021/09/chinas-standards-2035-project-could-result-in-a-technological-cold-war/>. Accessed May 25, 2022; Sheehan, Matt; Blumenthal, Marjory; Nelson, Michael. "Three Takeaways From China's New Standards Strategy." The Carnegie Endowment for International Peace, 28 Oct. 2021, <https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678>. Accessed May 25, 2022.
7. Wang, Yaqui. "In China, the 'Great Firewall' Is Changing a Generation." Human Rights Watch, 1 Sep. 2020, <https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation>. Accessed May 25, 2022; Yuan, Li. "China's Information Dark Age Could Be Russia's Future." *New York Times*, 18 March 2022, <https://www.nytimes.com/2022/03/18/business/chinas-russia-information.html>. Accessed May 25, 2022.
8. Yuan, Li. "China's Information Dark Age Could Be Russia's Future." *New York Times*, 18 Mar. 2022, <https://www.nytimes.com/2022/03/18/business/chinas-russia-information.html>. Accessed May 25, 2022.
9. Hvistendahl, Mara. "How a Chinese AI Giant Made Chatting—and Surveillance—Easy." *Wired*, 18 May 2020, <https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/>. May 25, 2022; Anderson, Ross. "THE PANOPTICON IS ALREADY HERE." *The Atlantic*, September 2020, <https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>. Accessed May 25, 2022; Page, Jeremy. "In Sign of Resistance, Chinese Balk at Using Apps to Snitch on Neighbors." *Wall Street Journal*, 29 Dec. 2017, <https://www.wsj.com/articles/in-sign-of-resistance-chinese-balk-at-using-apps-to-snitch-on-neighbors-1514566110>. Accessed May 25, 2022.
10. "How China Tracks Everyone." Youtube, *Vice News*, <https://www.youtube.com/watch?v=CLo3e1Pak-Y&t=360s>. Accessed May 25, 2022; Reilly, Jessica; Lyu, Muyao; Robertson, Megan. "China's Social Credit System: Speculation vs. Reality." *The Diplomat*, 30 Mar. 2021, <https://thediplomat.com/2021/03/chinas-social-credit-system-speculation-vs-reality/>. Accessed May 25, 2022; Buckley, Chris; Wang, Vivian; Bradsher, Keith. "Living by the Code: In China, Covid-Era Controls May Outlast the Virus." *New York Times*, 30 Jan. 2022, <https://www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html>; <https://www.rfa.org/english/news/uyghur/eid-prayers-07302021163133.html>. Accessed May 25, 2022; Yuan, Li. "A Generation Grows Up in China Without Google, Facebook or Twitter." *New York Times*, 6 Aug. 2018, <https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html>. Accessed May 25, 2022; Brzeski, Patrick. "'Friends' Re-Released in China, But LGBTQ Storylines Get Censored." *The Hollywood Reporter*, 14 February 2022, <https://www.hollywoodreporter.com/tv/tv-news/friends-rereleased-china-lgbtq-storylines-censored-1235093754/>. Accessed May 25, 2022.

11. Anderson, Ross. "THE PANOPTICON IS ALREADY HERE." *The Atlantic*, Sep. 2020, <https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>. Accessed May 25, 2022; Mozur, Paul; Kessel, Jonah; Chan, Melissa. "Made in China, Exported to the World: The Surveillance State." *New York Times*, 24 April 2019, <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>. May 25, 2022; Mozur, Paul; Xiao, Muyi. "A Digital Manhunt: How Chinese Police Track Critics on Twitter and Facebook." *New York Times*, 31 Dec. 2021, <https://www.nytimes.com/2021/12/31/technology/china-internet-police-twitter.html>. Accessed May 25, 2022.
12. Department of Justice, Federal Bureau of Investigation. "Responding Effectively to the Chinese Economic Espionage Threat." 6 February 2020, <https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat>. Accessed May 25, 2022; "China still steals commercial secrets for its own firms' profit." *The Economist*, 11 November 2021, <https://www.economist.com/china/2021/11/11/china-still-steals-commercial-secrets-for-its-own-firms-profit>. Accessed May 25, 2022; Allison, Graham; Klyman, Kevin; Barbesino, Karina; Yen, Hugo. "The Great Tech Rivalry: China vs the U.S." Belfer Center for Science and International Affairs, Harvard Kennedy School, Dec. 2021, https://www.belfercenter.org/sites/default/files/GreatTechRivalry_ChinavsUS_211207.pdf. Accessed May 25, 2022; Xinhua. "China Focus: China spurs digital economy as new driver of growth." *Xinhua*, 25 May 2022, http://www.xinhuanet.com/english/2021-08/04/c_1310107393.htm. Accessed May 25, 2022.
13. Fanusie, Yaya, and Emily Jin. "China's Digital Currency." Center for New American Security, Jan. 2021, <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Chinas-Digital-Currency-Jan-2021-final.pdf?mtime=20210125173901&focal=none>. Accessed May 25, 2022; Ho, Fong Tak. "China's Cryptocurrency Ban Comes as Government Rolls Out Digital Yuan." *Radio Free Asia*, 28 Sep. 2021, <https://www.rfa.org/english/news/china/ban-09282021111710.html>. Accessed May 25, 2022.
14. "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying." *NPR*, All Things Considered, 26 Aug. 2021, <https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying>. Accessed May 25, 2022.
15. Shepardson, David, and Reuters. "Five Chinese companies pose threat to U.S. national security - FCC." *Reuters*, 12 Mar. 2021, <https://www.reuters.com/world/us/five-chinese-companies-pose-threat-us-national-security-fcc-2021-03-12/>. Accessed May 25, 2022.
16. Office of the Director of National Intelligence. "Annual Threat Assessment of the US Intelligence Community." Feb. 2022, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf>. Accessed May 25, 2022.
17. Department of Defense. "Military and Security Developments Involving the People's Republic of China." 3 Nov. 2021, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>. Accessed May 25, 2022.