DENYING SUPPORT FOR CHINESE AND CHINA-ENABLED AUTHORITARIANISM AND REPRESSION

RISKS OF INTERDEPENDENCE

Technology has enabled disturbing escalations and expansions of China’s authoritarian and repressive policies, prompting American policymakers to step up U.S. tech restrictions in response. Washington’s main concerns are twofold.

First, Beijing has spent years pioneering wholly new kinds of mass digital surveillance and censorship within China—including the Great Firewall, social credit systems, and ubiquitous AI-powered digital camera networks, to name just a few well-known examples. These systems are more fragmented and spottier than sometimes portrayed. Nevertheless, China’s techno-authoritarian innovations have managed to expand the modern frontiers of social control, alarming Americans concerned with Chinese human rights and civic freedoms.\textsuperscript{351} In particular, tech has helped to power Beijing’s worst recent abuses, such as the ongoing campaign to marginalize Uyghurs and eliminate their culture, which Washington rightly calls genocide and crimes against humanity.\textsuperscript{352} Mass facial recognition and biometric collection have become tools of ethnic profiling against Uyghurs, while Chinese drones have helped Xinjiang security forces to manage mass detention operations.
Second, many U.S. policymakers believe that Beijing is proactively exporting this techno-authoritarian model to other countries. For example, Chinese digital surveillance and censorship systems have been sold to repressive regimes like Zimbabwe and Venezuela, with the latter receiving “a commercialized version of China’s ‘Great Firewall.’” Washington fears that a “China model” of techno-authoritarianism will not only spread among authoritarian countries, but may also influence hybrid regimes and illiberal democracies, exacerbating and entrenching the global democratic recession.

Such an outcome would threaten U.S. interests (as well as American values), because Washington derives much of its geopolitical influence from the assumption of like-mindedness among governments and publics in democratic countries. More fundamentally, Biden argues that the fate of America’s own democracy is bound up with that of democracy abroad, and he has rhetorically staked his national security strategy on that premise. This linkage may motivate a broadening of U.S. efforts to combat global techno-authoritarianism, particularly in countries that purchase systems from America’s chief rival, China.

A number of experts dispute the narrative that China purposefully exports techno-authoritarianism. They argue that Chinese foreign tech sales are driven more by the “pull” from governments who demand repressive tools than by any “push” from Beijing. However, the strength of Beijing’s “push” may grow over time, if China (like the United States and other historical great powers) comes to see a network of like-minded regimes as vital to its global interests. Moreover, even a mere “pull” from third countries, when eagerly satisfied by China, can pose challenges to U.S. agendas of human rights and democracy promotion around the world.

Initiatives like the Digital Silk Road help to spread Chinese hardware, software, and services, whose architectures embody Beijing’s preference for a more controllable, government-led internet. Western democracies, in contrast, promote international tech standards and governance models more compatible with free expression and civil society. To be sure, the United States and its allies have also provided substantial technology to friendly authoritarian regimes, from general cloud services to boutique hacking software. Yet multiple democracies are taking tentative steps to reduce this complicity—for example, by cracking down on the reckless proliferation of advanced hacking tools.

The development of Chinese techno-authoritarianism, and Beijing’s more general authoritarian turn under President Xi Jinping, has prompted Washington to revisit its traditionally laissez-faire approach to China’s human rights problems. After the 1989 Tiananmen Square massacre, the United States initially sought to condition the overall bilateral trade relationship on improvements to China’s human rights record. But the Bill Clinton administration “ultimately abandoned this direct linkage” in favor of permanent most-favored-nation status, hoping that economic engagement would open up China politically (while benefiting
America economically). Afterward, for nearly twenty years, the United States dealt with Chinese human rights abuses by levying very targeted punishments that did not jeopardize economic ties. For example, it imposed visa restrictions and sanctions on a handful of Chinese officials involved in the repression of Tibet and Falun Gong. It has also funded civil society and human rights activities in China, including software designed to circumvent internet censorship.

But recent U.S. technology restrictions reflect a tougher policy on Chinese human rights, with more economic bite. The Trump administration punished some of China’s most prominent and successful tech firms, including SenseTime, Megvii, Hikvision, iFLYTEK, and Dahua, for their activities in Xinjiang—the first time that human rights violations had ever been cited in Entity List designations. Likewise, Biden and Congress have cracked down on Chinese imports from Xinjiang, including tech products such as cell phones and solar cells, due to forced labor concerns. The solar cell restrictions, in particular, will have widespread impact across the solar industry. In addition, the U.S. government has announced sanctions and visa restrictions for certain Chinese tech companies and their employees involved in support to the Nicolás Maduro regime in Venezuela and other “regimes engaging in human rights abuses globally.”

RISKS AND LIMITATIONS OF DEFENSIVE MEASURES

Unlike past U.S. efforts to punish Chinese human rights abuses, these latest technology controls have had tangible economic consequences, resulting in canceled deals and rerouted supply chains. Still, the recent restrictions represent just a small fraction of the broad-based China tech restrictions that some are advocating in the name of human rights and democracy. U.S. policymakers should understand this slippery slope before they slide much further.

Although recent U.S. government restrictions have focused primarily on Xinjiang, and Washington officially disavows any intent to impose sweeping reforms on China’s larger political order, an emerging and politically diverse strain of thought argues for more expansive and assertive U.S. efforts to liberalize Chinese politics. From the right, leading former Trump administration officials argue that the problem with China is its Marxist-Leninist ideology, and that Washington must therefore wage a Manichean struggle against Beijing’s official thought system. From the left, some human rights promoters believe that America’s economic relationship with China “isn’t worth the moral cost” and that U.S. leaders should mount

An emerging and politically diverse strain of thought argues for stronger U.S. efforts to liberalize Chinese politics. Policymakers should understand this slippery slope before sliding much further.
a “sustained effort” to “[counter] China’s dictatorial apparatus.” From the center, national security voices such as the Atlantic Council’s “The Longer Telegram” have called for the United States to aggravate “internal fault lines of domestic Chinese politics in general and concerning Xi’s leadership in particular”—that is, to help effectuate Xi’s removal from power.

These ideas have growing influence, and they could well push U.S. tech policy down a perilous path. Human Rights Watch, for example, has asserted that “human rights abuses in China exist, and persist, in part because the US and others haven’t insisted on holistic progress, and haven’t imposed a price in response to them.” It therefore signed a letter with twenty-three other NGOs, including Freedom House and PEN America, advocating “a series of escalating actions against technology companies found to be contributing to China's mass surveillance, including by imposing Global Magnitsky sanctions.” But the premise is likely mistaken: the United States probably can’t impose a price severe enough to deter the vast bulk of Chinese human rights violations. As a result, these “escalating actions” would have no clear stopping point.

Much of Beijing’s techno-authoritarianism is a logical outgrowth of the Chinese political system itself—a system the United States cannot change and can barely seem to influence. The Chinese government seeks to preserve the Communist Party’s power at all costs, and the Party stands for a rigid, domineering vision of the Chinese social order. So long as these facts remain true, Beijing will continue developing and employing technologies to achieve its authoritarian ends. Moreover, the indigenous Chinese technology base provides Beijing with ample capability to do so. This means that no amount of U.S. pressure is likely to compel China to relax the basic components of its domestic technological repression. At most, U.S. technology controls can impose modest costs and delays in specific cases where China currently relies on foreign components, such as advanced semiconductors.

Meanwhile, a zealous U.S. campaign against the basic apparatus of Chinese techno-authoritarianism could inflict serious costs on the United States. It would likely devastate bilateral diplomatic ties, making cooperation on global issues more difficult and military conflict more likely. It would also be difficult to contain. Consider that virtually all Chinese tech companies contribute in some way to mass surveillance via the operation of draconian statutes such as China’s Cybersecurity Law and National Security Law. In fact, Beijing’s system of mass surveillance and control is suffused throughout the entire Chinese economic and societal structure. Chinese tech and non-tech companies alike send sensitive data to the state, participate in censorship activities, implement various social credit systems, and generally seek to anticipate and demonstrate allegiance to Xi’s sociopolitical edicts. Aggressive attempts to thwart Chinese mass surveillance, censorship, or techno-authoritarianism may well lead toward technological and economic divorce.

The United States probably has more room to address China’s sales of repressive technologies to foreign governments. Some of these governments are less deeply authoritarian than
China and/or easier for Washington to influence due to specific bilateral relationships. Direct engagement should be tailored to the individual circumstances and motivations of third-country governments. Even then, the U.S. government should expect to encounter strong resistance in any global campaign to roll back techno-authoritarianism. U.S. democracy promotion efforts have historically struggled during periods when they were comingled and conflated with larger geopolitical campaigns, such as the Cold War and the War on Terror.374 American strategic competition with China presents a similar problem for today’s U.S. democracy promoters.

RECOMMENDED POLICIES AND PROCESSES

The United States is right to respond to the novel and serious twenty-first-century challenge of techno-authoritarianism, but it must also avoid embarking on an overambitious crusade with high risks and few rewards. U.S. policy on Chinese domestic techno-nationalism should focus on the most egregious abuses. Rather than waging a quixotic battle against entrenched Chinese policies like mass surveillance and internet censorship, Washington should keep working to punish and stigmatize Beijing’s targeted repression of Uyghurs and other minority groups. Such groups do not benefit from what the Chinese Communist Party considers to be its authoritarian social compact, and they often seek to remain outside of it. In partnership with other countries, U.S. pressure might make some difference on Chinese repression of minorities. But if it does not, America can at least limit its moral complicity.

To implement this policy, the State Department and the Intelligence Community should collaborate with outside groups to identify Chinese technology systems that support Beijing’s targeted efforts to repress minority groups. The Departments of Commerce and Treasury, and other agencies, could then compile the major ways that these Chinese systems rely on direct or indirect American support, including U.S. exports (of finished technology, raw inputs, or non-technology goods and services) and financing. Regulators would then consider which of these support flows can be feasibly controlled, based on the U.S. government’s ability to trace their movement into and inside of China.

U.S. responses to Chinese “export” of techno-authoritarianism should depend on the “importing” country, the nature of the technology transaction, and the mixture of “push” and “pull” motivations at play.

U.S. responses to Chinese “export” of techno-authoritarianism should look different depending on the “importing” country, the nature of the technology transaction, and the mixture of “push” and “pull” motivations at play. When third countries are specifically seek-
ing out repressive tools and deem Chinese technology to be the best available, Washington can consider using sanctions and other restrictive measures as part of a broader dissuasion campaign aimed at both sides of the transaction—recognizing that the prospects of success will often be low.

When third countries are instead seeking general purpose technologies and the United States is concerned that Chinese products have authoritarian governance models embedded within them, Washington should focus on fostering the development of compelling Western alternatives. The U.S. government could, for example, help its companies better compete with China on costs, or double down on traditional American advantages such as reliability, security, technical assistance, and noncorruption. Restrictive measures could then buy time for these positive efforts to produce competitive alternatives to Chinese tech. Finally, there will likely be countries that pursue hedging strategies—intentionally dividing purchases between Chinese and Western technologies—to maximize their political and economic leverage and autonomy. Hedging countries are difficult to sway; U.S. tech policy might draw insights from other domains, such as arms and civilian aircraft sales, where hedging occurs.375

**CASE STUDIES**

The majority of Trump- and Biden-era technology controls related to Chinese human rights have wisely focused on ethnic repression in Xinjiang. This includes almost all of the Entity List designations of tech companies, for example.

**DJI.** In a few cases, however, the justifications were vague. In December 2020, the Department of Commerce designated four Chinese entities that “have enabled wide-scale human rights abuses within China through abusive genetic collection and analysis or high-technology surveillance, and/or facilitated the export of items by China that aid repressive regimes around the world, contrary to U.S. foreign policy interests.”376 “Abusive genetic collection” may refer to Xinjiang, but the Commerce Department did not say this. Notably, one of the four companies was the drone manufacturer DJI, which was presumably designated for its “high-technology surveillance” in China or its sales to repressive regimes.

DJI supported Xinjiang security operations as of 2017–2019, though publicly available information is scant and somewhat dated.377 By declining to specify what exactly DJI had done (and when) and failing to reference Xinjiang, the Trump administration undermined the strength of its stand and allowed for speculation that human rights may have been a pretext. The U.S. government has many other concerns about DJI, including the potential military and intelligence applications of its products and the company’s dominant market share in a growing industry where American companies have struggled to break through.378
Fortunately, the Biden administration has begun to stake a clearer position on DJI’s human rights record. Its December placement of DJI on the Non-SDN Chinese Military-Industrial Complex Companies List indicated that DJI “has provided drones to the Xinjiang Public Security Bureau, which are used to surveil Uyghurs in Xinjiang.” This specificity helps to give businesses and governments around the world more stable expectations about the intention behind U.S. human rights policy and the planned use of restrictive tools. Ideally, the U.S. government would take the further step of outlining when DJI’s problematic conduct occurred and how the firm could demonstrate reform over time to earn removal from these lists. It may be that DJI and other Chinese companies have no intention of undertaking such reforms or of publicly disavowing human rights abuses that Beijing downplays or denies. However, establishing the general terms of an off-ramp for sanctioned Chinese companies could help Washington clarify its redlines and demonstrate that its human rights concerns are sincere.

**Xinjiang.** The Biden administration should continue looking for and restricting other traceable forms of American support for China’s technological repression in Xinjiang. The newly signed Uyghur Forced Labor Prevention Act is a good first step: it requires importers of goods from Xinjiang to prove those goods were not derived from forced labor, thereby making forced labor less profitable for Chinese companies and the Chinese government. To complement these import restrictions, Washington should further curb the flow of American technologies or tech inputs into Xinjiang. Good candidates for control may include technologies that require significant customization or technical support (including patches and updates), because ongoing vendor-customer relationships can provide a platform to verify Chinese end users and end uses. Other possibilities include enterprise software or heavy “smart” equipment sold to Xinjiang-based entities.

**Surveillance sector.** A handful of U.S. human rights–oriented tech restrictions have not focused on Xinjiang or other particularly egregious Chinese abuses. Biden’s version of the Non-SDN Chinese Military-Industrial Complex Companies List allows designation of companies operating in China’s “surveillance technology sector.” This undefined term could conceivably cover an enormous range of Chinese companies. The Treasury Department did try to clarify that it “expects to use its discretion to target” three kinds of Chinese companies: those supporting surveillance “that occurs outside of the PRC,” those enabling “surveillance of religious or ethnic minorities,” and those “otherwise facilitat[ing] repression or serious human rights abuse.” While the first two categories make sense, the final catch-all requires narrowing and clarification. For example, the Treasury Department’s initial designations—of Hikvision and Huawei—failed to cite any specific human rights abuses or even explain which enforcement category they fell under. (Subsequent designations of SenseTime, DJI, Megvii, and several other Chinese tech companies did provide relevant details on the firms’ involvement in targeted surveillance of Uyghurs.)
Without more clarity on the intent behind this authority, the U.S. government may find itself adding an ever-larger and more diverse set of Chinese companies to its restrictive lists. Consider that in 2019, the House of Representatives voted 407 to 1 to require sweeping export controls of virtually all technologies “critical” to Chinese social control, surveillance, and censorship. The Senate version of the bill that eventually became law omitted this provision. Still, the initial House vote indicates broad support in Washington for an expansive and potentially costly campaign against China’s entire techno-authoritarian model—not just the worst abuses.

**Summit for Democracy.** During the Summit for Democracy in December 2021, the Biden administration announced several new initiatives related to technology and human rights. While the initiatives were generally sound, they nevertheless demonstrated a continued reluctance to clarify U.S. policy objectives in this area. First, the United States joined with Australia, Denmark, and Norway to launch the Export Controls and Human Rights Initiative, aimed at “prevent[ing] the proliferation of software and other technologies used to enable serious human rights abuses.” The meaning of this initiative depends entirely on how “serious human rights abuses” is interpreted—a term that Washington has so far not defined.

Second, the White House announced a series of “grand challenges” to spur innovation in what it called “democracy-affirming technologies.” These technologies include censorship circumvention software, which the United States has long supported. Still, it is odd to brand such software as “democracy-affirming” rather than, say, “counter-authoritarian”: its primary users are seeking to elude their own authoritarian governments, not “affirm” democratic ones. The new language has the effect of masking a major U.S. policy dilemma: is Washington content simply to “affirm” existing and emerging democracies, with these governments’ partnership and consent? Or does the United States seek actively to subvert and weaken authoritarian regimes? The latter goal, while instinctually appealing to many in Washington, could be disastrous if applied to China and should not be used to justify significant bilateral tech restrictions.

**Is Washington content to “affirm” existing and emerging democracies with their partnership and consent? Or does it seek actively to subvert and weaken authoritarian regimes?**

**KEY OFFENSIVE POLICIES**

Washington retains a variety of traditional tools for addressing China’s authoritarianism and repression, to include démarches, advocacy in international forums, and moral and material support for Chinese dissidents (especially those living abroad), in addition to targeted sanctions against companies and officials involved in the worst abuses. While these are unlikely
to deter Beijing’s domestic techno-authoritarianism to any large degree, they are sometimes
the best options available.

There is more the United States can do to combat techno-authoritarianism at a global level,
including in places where China supplies repressive technologies. First, the U.S. govern-
ment could further crack down on America’s own witting and unwitting transfer of poten-
tially harmful technology products, services, and know-how to human rights abusers.
For example, Washington could be more parsimonious in licensing the export of advanced
hacking services; better monitor the conduct of U.S. companies granted such licenses; and
place postemployment restrictions on former U.S. government officials and contractors
who have had access to classified American cyber operations techniques. Second, the
United States could more intensively press its allies on their sale (as with Israel, Italy, and
Germany) or use (as with Saudi Arabia and the United Arab Emirates) of authoritarian
technologies, whether sourced from China or elsewhere. The recent Entity List designation
of Israel’s NSO Group was a long-overdue step in this regard and has already had some
positive effects.

And third, America can better model pro-democracy, pro–human rights technology poli-
cies at home, thus earning the credibility to serve as a global leader on these topics. For
example, U.S. federal agencies could hold transparent and inclusive discussions with civil
society groups and other affected communities on difficult emerging issues such as law
enforcement use of facial recognition. The White House Office of Science and Technology
Policy recently announced a broad initiative along these lines, aimed at developing a “Bill
of Rights for an Automated Society.” The practical impact of this “Bill of Rights” will
depend on its successful implementation in federal rulemaking and legislation.
DENYING SUPPORT FOR CHINESE AND CHINA-ENABLED AUTHORITARIANISM AND REPRESSION


