Brief No. 12.3

THE TECH TROJAN HORSE

China's Strategic Export of the Surveillance State

Michaela Flemming

P | I | P | S

The Tech Trojan Horse
China's Strategic Export of the Surveillance State

APRIL 2020

Michaela Flemming

P | I | P | S
The Project on International Peace and Security
Global Research Institute
College of William & Mary

The Tech Trojan Horse
China's Strategic Export of the Surveillance State

China aspires to be tomorrow's digital hegemon via the strategic export of its surveillance state to developing and autocratic countries. The sale of surveillance equipment, software, and services enables existing regimes to better control their populations, thereby strengthening or facilitating the spread of authoritarian governance. The sale of surveillance technology also increases the dependence of client governments on Beijing for their political survival. This emerging network of technologically dependent authoritarian regimes represents Beijing's digital hegemony in the developing world.

To combat growing Chinese influence in the developing world, the United States should use its resources to encourage the private sector to develop technological solutions to undermine digital authoritarianism and remove dependency on China. Additionally, Washington should work with developing states to build their cybersecurity expertise. Finally, the United States should impose costs on states who practice digital authoritarianism.

Introduction

Recently, countries around the world have implemented predictive policing systems, restricted the content of social media, and used algorithms to rate citizens on their trustworthiness. These cyber tools have facilitated the global rise of digital authoritarianism, or the use of technology to control populations, as a model of governance.[1] China's sale of selling cheap surveillance technology exports its model of digital authoritarianism to developing and authoritarian states. As a result, China's global influence will grow.

Beijing's export of surveillance-capable technology and its digital authoritarian model will make states increasingly dependent on China, while improving the PRC's intelligence capabilities.[2] If client states are dependent on Chinese surveillance technology and services, Beijing in turn will have greater leverage over them. With improved foreign intelligence, Beijing can create more sophisticated propaganda to disseminate in these states.

The United States should respond to China's actions with a multi-step approach. First, Washington can support research into innovative technologies that aim to counter digital authoritarianism. For instance, the private sector is already working on satellites to provide secure internet access to developing countries. Second, the United States can harden developing states against espionage by building their cyber security capacity. Third, the United States can impose costs on countries that practice digital authoritarianism to signal unacceptable uses of technology against populations.

How is China Spreading its Surveillance State?

China's strategic export of surveillance-capable technology poses two main problems for the United States. First, by providing this technology to countries that cannot otherwise access or afford it, China creates a network of client states that are economically and politically dependent on Beijing. These client states rely on China for access to the authoritarian technology, which keeps them in power. Second, surveillance technology captures vast amounts of data, which Chinese intelligence agencies could access. This intelligence gives Beijing greater insight into politics in client states, improving propaganda campaigns.

What is Chinese Digital Authoritarianism?

Chinese digital authoritarianism has two components. First, China is selling surveillance-capable technology to developing and authoritarian regimes, which then use these systems to surveil, repress, and manipulate their citizens.[3] This surveillance state is proliferating rapidly. In 2018, *Freedom on the Net* found that 27 percent of countries surveyed had implemented Chinese surveillance technology.[4] One year later, the share of states had increased to 72 percent.[5] Second, China is spreading cyber-sovereignty, a repressive model of internet governance to client states. Xi Jingping describes cyber sovereignty as "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies."[6] This model emphasizes the role of the state to regulate the internet within its borders. In practice, cyber sovereignty justifies the use of technology, such as surveillance equipment and telecom infrastructure, to repress populations.[7]

Until recently, the global internet rules largely reflected liberal democratic norms with a commitment to openness, privacy, and freedom of speech. By exporting digital authoritarianism, China has changed the rules of the game, eroding U.S. influence. China's core objective is to assert its role in global internet governance and gain coercive leverage over client states. As a result, the United States should expect to see existing authoritarian regimes grow stronger and democratic backsliding in the developing world.

Is China Gathering Data?

As Chinese technology makes up a larger share of the world's digital infrastructure, the Chinese surveillance state is extending its reach. Exporting surveillance-capable technology enables Chinese intelligence agencies to access data from client states.[8] Chinese companies like Huawei and ZTE contend that they do not provide data from their products to the Chinese Communist Party (CCP). However, it is unlikely that these companies could prevent the CCP from obtaining their data. Beijing's national security laws force Chinese companies to comply with the government's demands or be shut out of the Chinese market.[9] These laws mean that any Chinese-based company could be ordered to transfer their data back to servers the CCP controls.

According to Dr. Samantha Hoffman of the Australian Strategic Policy Institute, the CCP "is building a massive and global data-collection ecosystem."[10] For example, Global Tone

Communications Technology Ct. Ltd (GTCOM), a subsidiary of the Central Propaganda Department feeds captured data to the Chinese government.[11] GTCOM embeds its services on platforms offered by Huawei and Alibaba, further broadening its reach.[12] In the future, Chinese technologies in ecommerce platforms, telecom networks, or financial payment institutions could be leveraged to create a wide-reaching espionage infrastructure.[13]

How is it Marketed Abroad?

Beijing markets its digital authoritarian model to developing and authoritarian states through the Belt and Road Initiative (BRI) and state-sponsored training.

- *Who are they targeting?* China is primarily targeting developing and authoritarian states. Developing states want to build digital infrastructure for a number of reasons. In rural areas, online banking can bring people into the financial system, while cheap smartphones can improve communication. However, these technologies often require internet access, which can be prohibitively expensive for developing states to build themselves or procure abroad. On average, 1GB of mobile broadband data in Africa can cost over seven percent of monthly income.[14] Chinese companies are able to keep prices low due to corporate subsidies, government-funded research, and preferential access to the home market.[15] Additionally, China offers cheap financing with fewer conditions than traditional development loans.[16] For the majority of developing states, price is the most important factor. These states tend to prefer lower priced over more secure technology, meaning that they are less persuaded by the United States' argument that Chinese products present a cybersecurity risk.[17]

  Resource-poor authoritarian states want surveillance technology to protect against popular unrest.[18] However, they face credit constraints, which China's cheap authoritarian technology and loans allow them to overcome.[19] While western companies sell surveillance technology to authoritarian regimes, their higher prices and domestic restrictions put them at a disadvantage in this market. As a result, China remains the largest provider of surveillance technology in the world.[20]

- *The Belt and Road Initiative.* China continues aggressively to market surveillance-capable technology via the Belt and Road Initiative (BRI). The BRI is a broad infrastructure investment and aid effort by Chinese government agencies, state-owned enterprises (SOEs), and private sector partners. The BRI is notable for the degree to which these entities cooperate on projects. In Ecuador, for example, Huawei and China National Electronics Import and Export Corporation (CEIEC), a SOE, installed intelligent monitoring systems that send their data to the national intelligence service.[21] This system gives Ecuador's government the tools necessary to track the physical and digital movements of their political opponents.[22] Projects like the Ecuadorian security system demonstrate how both the Chinese private and public sector benefit from the BRI.

  China makes surveillance-capable technology accessible to client states by providing cheap financing. State-supported banks, such as the Chinese Development Bank and the Export-

Import Bank of China, can borrow money at low interest rates, since their bonds are secured by the Chinese government.[23] These savings are then passed on to client states. For instance, a BRI fiber optic cable project in Pakistan was financed at a concessionary two percent interest rate.[24] CEIEC gifted a facial recognition software program to Kyrgyzstan free of charge.[25] China's state-backed financing programs enable credit-constrained client states to purchase surveillance-capable technology. In the future, these states will rely on China as the sole provider of their technologies and services.[26]

- *State-sponsored training.* China also provides training to foreign officials on digital authoritarianism. Training involves seminars on managing public opinion and often are followed by the introduction of laws that fit within China's cyber sovereignty model.[27] Countries that have attended China's information seminars include Saudi Arabia, India, Venezuela, and Nigeria.[28] Other events, such as the World Internet Conference in Wuhan, China, explicitly promote cyber sovereignty.[29] These state-sponsored training programs demonstrate that China is instructing receptive client states on how to carry out digital authoritarianism.

A Transition towards Digital Hegemony

Beijing's efforts to promote cyber sovereignty and Chinese technology indicate that China is asserting its influence online. As a rising power, China seeks to reshape the rules and institutions of the internet to advance its own interests by promoting cyber sovereignty.[30] Through the BRI, China provides access to cheap financing and encourages developing states to buy Chinese technological infrastructure. However, these efforts create dependency on China and allow Beijing to surveil client states. With a web of dependent client states and real-time intelligence on countries worldwide, China's relative power increases.

The United States should be concerned about the proliferation of the Chinese surveillance state. By attempting to upend the U.S.-led status quo and setting new standards of internet governance, Beijing asserts itself as a revisionist power. If China achieves digital hegemony—the ability to set global norms on the internet—it will be at the expense of global democracy and U.S. influence.

Digital authoritarianism promises countries that they can have economic development *and* social control. For many countries, this promise makes digital authoritarianism an attractive alternative to liberal democracy.[31] If the United States does not take steps to counter China's actions, it could face a more hostile global environment populated by authoritarian Chinese client states.

Effects of China selling surveillance-capable technology

The export of surveillance-capable technology will strengthen China's foreign and domestic surveillance capabilities and Chinese client states. However, these clients will become dependent on Beijing for technology, giving China coercive leverage over them. These two effects will enable China to manage public opinion abroad, known as global social management.

Strengthening Chinese Surveillance Capability

China already utilizes surveillance-capable technology to collect data domestically. Data on citizens' identities, movements, and actions online enables the Chinese Communist Party (CCP) to more efficiently control its population. By exporting the surveillance state, China gains the same information on client states' populations. Client governments now risk Chinese intelligence being able to access their digital networks and spy on their citizens.[32] China can use this information as leverage in coercive diplomacy or to improve Chinese propaganda.

- *Domestic Surveillance*. China's international data collection will boost its domestic surveillance capabilities. As the Chinese-made surveillance state goes global, Beijing gains access to more diverse, high-quality data from client states. This data trains Chinese security algorithms to more accurately predict unrest, which enables the CCP to more effectively repress its own population.

  In 2018, Cloudwalk, a Chinese A.I. company, agreed to provide facial recognition software to the Zimbabwean government. As part of the deal, Zimbabwe reportedly handed over its entire national biometric database to Cloudwalk.[33] This data not only improves China's intelligence on Zimbabwe's population, but it also improves the performance of Cloudwalk's algorithms. Facial recognition algorithms are notoriously bad at identifying non-Caucasian faces. Using Zimbabwe's database, Cloudwalk could train its algorithms on a massive set of African faces, making them more accurate overall.[34] Cloudwalk is part of China's security infrastructure in Xinjiang, meaning that their upgraded facial recognition algorithms can be deployed there to more effectively repress citizens. As a result of this agreement, Cloudwalk can develop better tools for the Chinese surveillance state.

- *Improving Chinese foreign intelligence capabilities*. Many countries assert that Chinese-made technology can be used for espionage. For instance, the U.S. government claims that Huawei can spy on consumers through its systems.[35] Additionally, the U.S. military has banned the use of drones made by Chinese drone maker DJI and telecom equipment by Huawei over fears that the data collected while using the technology was accessible to the Chinese government.[36]

  While Chinese SOEs like GTCOM are part of Beijing's data collection network, private Chinese tech companies are also likely feeding data back to the government due to their strong relationship with the CCP. The Chinese government has helped these companies prosper through direct subsidies, a protected home market, and inclusion in the BRI as preferred partners.[37] Private Chinese companies also have a broad global reach. Huawei alone contributes to the surveillance architecture of two thirds of countries employing AI surveillance.[38] In addition, tech companies have the largest proportion of CCP party committees in the private sector.[39] Huawei hosts more than 300 party branches.[40] These committees could pressure private companies to comply with government demands. Finally, China's national security laws require companies to disclose data at the government's request.[41] Consequently, it is likely that data from private technology

companies is accessible to Chinese intelligence. Data gathered from these companies' products could then be used by the CCP to track and respond to threats.

For example, the CCP is concerned about security on its western borders. The Central Asian countries that neighbor China share religious, cultural, and ethnic commonalities with the oppressed Uighurs in Xinjiang. China has provided free or discounted smart city platforms to these states, allowing local autocrats to monitor their populations, while also feeding data back to China.[42] By exporting surveillance-capable technology, Beijing strengthens the pro-China elite and monitors the anti-China movement, thereby securing itself against a potential threat.[43]

- *Espionage at the African Union.* The African Union's IT network was caught transmitting confidential data to Shanghai every night from 2012 to 2017.[44] Huawei built the African Union's IT network, while the Chinese government paid for it. Huawei denied claims of espionage, however, experts commented that it was unlikely that the company was unaware of the daily theft of large amounts of data for five years.[45] The African Union's hack demonstrates how Chinese-made infrastructure could be used by state intelligence agencies for espionage.[46] As a result, the U.S. government labeled Huawei a national security threat.

Authoritarian Regimes Dependent on China are Strengthened.

Due to China's strategic export of surveillance-capable technology, its authoritarian client states are growing stronger. Resource-poor authoritarian states, such as Zimbabwe, are gaining access to technology that they could neither develop nor afford on their own. These technologies facilitate greater social control. For instance, smart city technologies meant to apprehend criminals can also monitor and harass political dissidents. Facial recognition software can track enemies of the state. Restrictive cyber sovereignty-influenced laws allow states to control content online. The control that authoritarian regimes gain from surveillance-capable technology enables them to prevent population mobilization, repress more discriminately, and better control what their citizens can view online. These capabilities strengthen authoritarian regimes.

However, importing Chinese surveillance-capable technology comes at a price—dependence on China. Poor authoritarian states rely on China for the tools that keep their regimes in power, while developing states become dependent on China for basic internet access.[47] Additionally, client states may need Chinese companies to construct, operate, and manage the digital infrastructure purchased from these companies.[48] When states depend on Chinese technology, Beijing gains an advantage. In the future, China could coerce an unruly client state by threatening to remove the client government's ability to surveil or shutting off its internet. For regimes that rely on the internet to remain in power, denying access could be their death knell.

- *Enabling illiberalism.* China is arming client states with technologies necessary to implement a surveillance state. Previously, constructing and maintaining a surveillance state was labor-intensive and expensive. Now China is selling cheap tools to surveil, censor, and repress their populations. Many developing states lack strong institutions and democratic norms to prevent the abuse of this technology by elites. By lowering the barriers

to authoritarian governance and propagating illiberal norms, China enables and encourages client states to become digital authoritarians.[49] In the future, client autocrats will not want to give up the security that Chinese technologies have given their regimes. Consequently, these autocrats will be more vulnerable to Beijing's coercive leverage.

Globally, Chinese companies already facilitate authoritarian governance. For example, Huawei technicians allegedly helped state security forces access a political opponent's WhatsApp account in Uganda.[50] A *Wall Street Journal* investigation found that Huawei was not only supplying technology to monitor communications, but was also training Ugandan personnel on how to use the equipment.[51] Similarly, the Zambian government has enlisted Huawei technicians to spy on opposition bloggers.[52] Other Chinese companies are equally culpable in enabling illiberalism. ZTE helped build and continues to manage a fatherland database for the Venezuelan government that allegedly enables a social credit system via the use of 'smart-citizen cards.'[53] This database holds personal information, medical history, and voting records, and is tied to a 'smart-citizen card' that Venezuelans use to access state services, including food assistance.[54] In 2018, China was coined 'the worst abuser of internet freedom.'[55] These examples demonstrate how China helps foreign governments commit the same abuses.

- *Technological dependence.* Beijing draws developing countries into its sphere of influence by creating China-centric digital infrastructure in these states.[56] China subsidizes costs of digital infrastructure by protecting domestic tech companies and providing foreign aid, concessionary loans, discounts, or payment in other methods, such as data. Additionally, the Chinese government protects domestic technology companies, enabling them to keep prices at a level that few Western manufacturers could sustain.[57] It also would be cost prohibitive for small countries to develop this technology domestically, since Chinese security algorithms will continue to improve using client state data.

  Huawei's role in 5G implementation is an example of such technological dependence. Many countries are looking to upgrade existing 4G networks to 5G. While other companies can build 5G networks, Huawei equipment currently makes up a large part of 4G networks. Current 5G technology is only compatible with 4G equipment from the same company, so changing providers increases the cost of 5G rollout.[58] BT, a UK telecom company, estimated it would cost 550 million pounds to reduce Huawei equipment to 35 percent of BT's mobile network.[59] For many countries, it is cost prohibitive to change providers and fully replace Huawei equipment.

  For poor states, buying Chinese systems creates dependence on China for access to technology. This dependence creates a captive market from which China can mine data, which improves China's intelligence capabilities. This technological dependence also creates coercive leverage for China. If client states rely on Chinese-made or managed digital infrastructure, China could threaten cut service if a client state took actions unfavorable to Beijing.

- *Creating economic and political dependence on China*. The export of the Chinese surveillance state to developing states creates political leverage via an economic power

imbalance. China seeks an asymmetric relationship with client states, using its resources to shape regional economic and political orders to its benefit.

The BRI restructures regional economies to be more China-focused. BRI projects fuel China's economy by shifting excess domestic manufacturing capacity abroad. Some contracts specify that Chinese companies must build and manage critical infrastructure, resulting in continued Chinese influence in these areas.[60] In addition, China gains new markets for its goods and infrastructure to facilitate sale of these goods. Long repayment timelines and easy refinancing for Chinese loans mean that Beijing will remain involved in client states in the near term.

This economic restructuring has political consequences. China's highly accessible loan policy has trapped client states with unsustainable debt. Several of these countries have strategic value to China. Political and economic leverage has enabled the Chinese to extract concessions, such as control over strategically located ports in Sri Lanka and Djibouti or resource rights for oil reserves in Ecuador.[61] In 2011, China wrote off an unknown amount of debt owed by neighboring Tajikistan in exchange for disputed land totaling 11 percent of the country.[62] In the future, countries may find that the aid they receive from China leaves them worse off. Indebted client states are susceptible to Chinese coercion in return for debt relief. Even the threat of calling in loans could give China political leverage over client states. As a result, China will be able to compel client states to advance its own objectives.

Global Social Management

China's policy of social management is going global.[63] In the future, Beijing can leverage its improved foreign intelligence capabilities and client states' dependence on China to respond to international threats. Domestically, Beijing already uses a variety of tools to shape public opinion. However, the globalization of Chinese surveillance state—which strengthens both China's surveillance capability and client authoritarian states—will allow Beijing to manipulate public opinion abroad.

Better foreign intelligence allows the CCP to anticipate and respond to threats from abroad more efficiently. Using the information gathered, China is able to tailor disinformation campaigns through targeted propaganda and censorship. The CCP seeks to present a positive national narrative and counter its negative reputation.[64] Beijing uses cyber tools to promote this narrative abroad. Automated microtargeting algorithms can use artificial intelligence to analyze social media and customize messages for specific individuals.[65] Natural language processing tools can be used to 'score' social media posts, predict the authors' allegiance to the regime, and their likelihood of dissent.[66] These customized disinformation campaigns may be more effective at manipulating foreign public opinion to support the CCP's desired narrative.

- *Pak-China Fiber Optic Cable.* The Pak-China Fiber Optic Cable was intended to provide internet access to Eastern Pakistan and was funded with a concessionary Chinese loan. While loan documents for BRI projects are rarely made public, a leaked draft of the

agreement required Pakistan's media networks to cooperate with Chinese media in the "dissemination of Chinese culture."[67] According to the Council on Foreign Relations, China's prior actions of digital espionage make it likely Beijing will take similar actions when installing fiber optic cables.[68] An enormous amount of data runs over fiber optic cables. If this data was tapped, China would gain valuable intelligence on Pakistan's population, enabling more targeted and responsive propaganda campaigns. Pakistan's discount on the fiber-optic cable may be in exchange for spreading Chinese propaganda and demonstrates how dependent states can be incentivized to promote Beijing's national narrative.

- *Influence in African media*. In 2015, China sponsored a program to provide free satellite TVs to 10,000 rural villages across Africa.[69] StarTimes, a Chinese media conglomerate carried out this program. StarTimes provides cheap access to Chinese news networks, such as China Global News Network (CGTN), while only offering western news on more expensive plans.[70] In Kenya, a StarTimes basic package costs $2.50 per month, compared to $9.50 for a competing plan.[71] Chinese digital media companies, such as Opera News, Scooper, and Vskit are also gaining traction in Africa.[72] In Africa, Chinese news is more negatively perceived than western media, but it is also cheaper.[73]

  Chinese intelligence has the ability to capture the data running over Chinese platforms in Africa to create targeted propaganda delivered directly to local communities. Chinese companies like StarTimes and Huawei provide products and infrastructure that increase the reach of Chinese media. Then media outlets like CGTN disseminate and bolster the CCP's narratives through their pro-China news programs over which the CCP allegedly has editorial control.[74] Consequently, CGTN is required to register in the United States as a foreign agent under anti-propaganda laws.[75] In the future, China can work through Chinese companies and leverage their digital infrastructure towards state objectives. If Beijing can deliver sophisticated information campaigns back over these platforms, China can more effectively influence African public opinion to support its narrative.

Implications for the US

China's geopolitical strategy is a threat to the United States. With more dependent allies, China may be emboldened to adopt a more interventionist foreign policy. If cyber sovereignty gains support, the free and open internet will suffer. Finally, global democratic backsliding results in the proliferation of autocratic regimes, which erodes the U.S. sphere of influence.

China Benefits from Stronger, but More Dependent Allies

Beijing's export of surveillance-capable technology benefits both client states and the Chinese government. For client states, Chinese technology may strengthen their regimes by giving them greater domestic control. At the same time, it also increases their vulnerability to Beijing. Client states will become dependent on China to sustain domestic order. In addition, improved foreign surveillance capabilities allow the Chinese government to directly influence client state

populations. For the Chinese government, access to real-time client state data combined with client states' increased dependence on Beijing gives the CCP leverage over its client states. This leverage could be used to compel or deter client states in a way that furthers Beijing's objectives.

In the future, the CCP could leverage its relationships with Chinese companies to gain strategic advantages.[76] These advantages may be as simple as letting state hackers through back doors in critical infrastructure, cutting service, or even using 5G networks to disrupt and deny enemy communications.[77] 5G has strategic value to the U.S. military; for example, it enables global command and control systems to communicate faster.[78] However, if 5G runs over Huawei's network, China could use Huawei to intercept or deny military transmissions.[79] In Africa, where Chinese companies dominate the current telecommunications infrastructure, securing communications is a major concern for the U.S. military.[80]

Cyber Sovereignty Gains Credence

Cyber sovereignty is gaining global support. Because of emerging cyber security threats, even consolidated democracies realize the necessity of regulating the internet.[81] By promoting cyber sovereignty in international institutions, offering state training, and setting a domestic example, China is actively seeking to influence governing norms around the internet.[82] Cyber sovereignty's growing support challenges the United States' influence online and creates an unfavorable digital environment for U.S. businesses and the government.

Dozens of countries have passed laws in line with cyber sovereignty. After Chinese media training, Tanzania and Uganda enacted laws that gave the state more control over the internet.[83] As more states espouse cyber sovereignty domestically, China can more effectively promote this model in international institutions, such as the United Nations General Assembly. In 2019, China sponsored a UN resolution that would make it easier for countries to cooperatively enforce digital authoritarianism.[84] Beijing was supported by a number of countries that have received its media training.[85] China's leverage over these countries allows Beijing to coerce client states into supporting future Chinese-backed measures. As the number of client states grows, China will gain greater power within multilateral institutions, enabling Beijing to legitimize digital authoritarianism as international law.

Cyber sovereignty reduces the United States' influence in cyberspace. For decades, the United States has used its influence to promote user privacy, freedom of speech, and the norm of minimal government interference online. In contrast, China's model prioritizes state sovereignty and maintaining social stability.[86] As Beijing persuades other countries to adopt cyber-sovereignty, its influence over the rules and norms of global internet increases.

The United States' influence is already shrinking. For instance, Washington has repeatedly declared that Huawei is a threat. However, U.S. allies like the United Kingdom and Germany refuse to ban Huawei from their telecommunications systems. If the United States' online influence continues to deteriorate, it will be harder for the United States to set favorable international norms.

Cyber sovereignty-influenced policies also result in a digital environment that harms the interests of U.S. businesses and the U.S. government. Data localization regulations could raise the cost of doing business by requiring companies to build new servers to keep data within the country of origin. Additionally, data localization policies will make it easier for foreign governments to gain access to intellectual property.

Further Rollback of Democracy

China's export of its surveillance state puts the tools of digital authoritarianism in the hands of client states. For these states, digital authoritarianism is an attractive form of governance. It allows client states to control their populations, while preventing the economic stagnation that has accompanied past forms of illiberal governance.[87] As a result, democracy is eroding worldwide. In 2019, global freedom declined for the 13th consecutive year, while global internet freedom declined for the 9th year.[88]

States' existing regulatory models influence the choices of other states, which shape global internet governance.[89] For example, India, Mexico, Indonesia, Singapore, and Brazil are influential regional powers that have not committed to either the Chinese or American model of internet governance.[90] China targets these states when it promotes cyber sovereignty. Of the top five most influential undecided states, 80 percent have participated in Chinese media training.[91] China increasingly has prompted undecided states to adopt cyber sovereignty influenced practices. For instance, India has built up its surveillance state and used it to repress its citizens.[92] If regional powers like India take up Chinese-style internet governance, it is likely that other states will follow their lead. Consequently, digital authoritarianism will proliferate, and world freedom will continue to decline.

What can the United States do to combat digital authoritarianism?

The United States should tailor its policy response based on how states implement Chinese surveillance-capable technology. While developing states typically use Chinese-made surveillance-capable technology to improve internet connectivity or public services, authoritarian states use the same technology to surveil, censor, and repress their populations. The United States should adopt a customized approach for each regime type. Policies should provide states' access to technology for development purposes, while punishing states that use it to repress and censor their citizens.

Create a Framework

Policy makers and academics acknowledge that even highly institutionalized democracies struggle with how to maintain security, while protecting civil liberties.[93] Many scholars have focused on creating a model of democratic digital governance to compete with digital authoritarianism.[94] Additionally, they recommend that the United States establish clear standards on acceptable and

unacceptable uses of citizens' data by both governments and corporations, similar to the EU's General Data Protection Regulation (GDPR).[95] By creating clear standards, the United States also can hold itself and U.S. companies accountable and prevent the export of surveillance-capable technology to dictators.[96] While the United States should reform its own internet governance standards, this will not solve the problem of client states' dependence on China. Until a cost-effective alternative to Chinese digital infrastructure exists, developing client states will continue to be reliant on Beijing.

Spur Competition

The U.S. government should stimulate innovation and competition by incentivizing companies to develop low-cost technical solutions to digital authoritarianism.[97] These solutions involve the production of affordable alternatives to Chinese-made digital infrastructure, such as telecommunications equipment, to combat the problem of dependence. Developing states are often resource-limited—however, they already have a high degree of trust in U.S. technology.[98] This trust means that if U.S companies can make digital infrastructure cost effective, there is likely a market for them in the developing world. For authoritarian states, technical solutions may entail offering tools that protect citizens in digital autocracies, such as VPN access to protect dissenters' identities.

- *Leverage the private market*. Solutions to digital authoritarianism may already exist in the private market. Loon, a subsidiary of Alphabet, has developed stratospheric balloons that supply internet service to remote areas.[99] This technology has already been used to reconnect countries in the aftermath of natural disasters.[100] SpaceX's Starlink satellite network could also deliver low-cost internet access.[101] Advances in these technologies could be competitive with Chinese-made 4 and 5G infrastructure. NordVPN offers free virtual private network services to citizens in authoritarian regimes, enabling them to mask their online activity.[102] Congress is currently debating a bill that could support the global adoption of these solutions. The Utilizing Strategic Allied (USA) Telecommunications Act, which was introduced this year in the Senate by Senator Mark R. Warner, would create a $500 million Multilateral Telecommunications Security Fund to support the purchase of secure equipment abroad.[103] By partnering with companies like Loon, SpaceX, and NordVPN, and using resources appropriated by the USA Telecommunications Act, the United States use options provided by the private market to address a global security problem.

- *Repurpose existing programs*. The United States also could capitalize on existing programs, such as Small Business Innovation Research (SBIR) grants, to develop new technological solutions. SBIR funds research and development at small businesses through grants under $2 million dollars.[104] A similar program, the Small Business Technology Transfer (STTR), brings together private companies and research institutions to encourage innovation.[105] Together, these initiatives have a budget of $2.5 billion dollars, which could be leveraged to develop low-cost digital infrastructure.

> The U.S. government should also look beyond current contract vehicles for innovative solutions. For instance, competitions such as the DARPA Grand Challenge could leverage the human capital of U.S. universities and businesses to encourage the design of low-cost and innovative technologies that could be implemented in developing countries. Additionally, these competitions are extremely low cost with a potentially high reward. The 2007 DARPA Urban Challenge resulted in the creation of the first autonomous vehicles able to navigate an urban environment—despite the fact that the total prize money given out was only $3.5 million dollars.[106]

Some have encouraged the U.S. government to fund its own domestic alternative to Huawei or existing challengers. However, encouraging interoperability between telecommunications systems is a better solution, because it breaks Huawei's monopolistic hold on 5G.[107] In February 2020, the U.S. government announced a partnership with technology companies, including Dell, Microsoft, and AT&T, to create common engineering standards for 5G, resulting in interoperable equipment.[108] If successful, this initiative could reduce reliance on Huawei for 5G networks.[109] The USA Telecommunications Act could also dedicate over $1 billion dollars towards an innovation fund to support research and development into open 5G standards.[110] Supporting interoperability could reduce the cost of digital infrastructure and make western companies competitive with Chinese products.[111]

Build Capacity

The Trump Administration's current alternative to BRI is the Free and Open Indo-Pacific strategy. As part of that strategy, USAID implemented the Digital Connectivity and Cybersecurity Partnership. This program builds partner nations' domestic capacity to combat emerging cyber threats through workshops and training.[112] Currently, the program is limited to Southeast Asia. Chinese cyber-espionage, however, is a global threat requiring a global response. Therefore, the Digital Connectivity and Cybersecurity Partnership should be expanded to developing countries in Eurasia, Africa, and South America to bolster their cybersecurity.

The United States should focus on building cybersecurity capacity to harden targets in the developing world against Chinese espionage. Cybersecurity experts can make an informed calculation of the risks and benefits associated with implementing Chinese surveillance-capable technology. For example, the United Kingdom has refused to ban the use of Huawei equipment, calculating that it has the cybersecurity expertise to safely and securely incorporate it into existing systems. While hardening developing countries does not prevent them from becoming dependent on cheap Chinese technology, it does help protect their citizens' data.

Increase Costs

For poor authoritarian countries that cannot afford western technology, China's offer of low-cost social control is simply too tempting to pass up. The United States should promote the responsible adoption of digital technologies and impose costs on countries that use them to repress their populations.[113] Specifically, these penalties should be targeted at the decision makers in client

states through measures that bring scrutiny to regimes, provide support for pro-democracy opposition forces, or financially constrain elites. By increasing the costs associated with digital authoritarianism, the United States reduces the spread of illiberal governance.

- *Export Controls*. Often sanctions are used to influence the decisions of other states. Currently, agreements, such as the Wassenaar export controls, regulate the sale of dual-use technologies that could enable digital authoritarianism.[114] The United States has chosen not to employ these controls.[115] As a result, U.S. firms supplied 32 countries with A.I. surveillance technology capable of supporting digital authoritarianism in 2019.[116] In the future, the United States can utilize Wassenaar controls to block the sale of American technology to digital authoritarians.

- *Foreign Aid.* The United States can restrict foreign aid to digital authoritarian regimes. Foreign aid is a valuable resource for many developing and authoritarian states. For example, Zimbabwe received $318 million of U.S. foreign aid in 2019, which comprised about three percent of the government's total budget.[117] Imposing restrictions would necessitate creating official standards and definitions for what constitutes digital authoritarianism; however, policy makers can work with the academic community to create these standards. While the United States has the financial might to impose costs unilaterally, it can impose higher costs on non-compliant regimes by operating multilaterally.

Conclusion

China's promotion of digital authoritarianism threatens the United States' interests on and offline. By selling surveillance-capable technology and championing cyber sovereignty, China gains greater global influence. This effect has implications for the U.S. global leadership. First, the United States may face a stronger and more aggressive Chinese government. Second, cyber sovereignty threatens to turn cyberspace into a hostile environment for U.S. businesses and security interests. As a result of the United States' declining global influence, China's actions facilitate global democratic backsliding.

To counter the proliferation of digital authoritarianism, the United States must take action. While the United States should codify its own standards of acceptable behavior online, it should go further. The United States should leverage its domestic human capital through initiatives that spur market competition in surveillance-capable technology. Additionally, the State Department should expand current cybersecurity training initiatives. Finally, the United States should impose costs to autocratic states.

Acknowledgements

The author would like to thank Elsa Kania, Jimmy Zhang, Professor John Lombardini, Professor Claire McKinney, Professor Fiona Shen-Bayh, and Ranjani Parthasarathy for providing integral feedback in the developmental stages of this project, as well as Dr. Daniel Markey and Justin Sherman for taking the time to discuss their research and offer feedback which became pivotal in shaping the policy solutions section of this paper. The author thanks the U.S. Army Mad Scientist Team and the U.S. Joint Forces Staff College for the opportunity to present her work. The author would also like to thank Professor Amy Oakes, Professor Dennis Smith, LtCol John L. Gallagher, IV, USMC, Rose Olwell, M. Nina Miller, Major General Mark Matthews, USAF (Ret.), CDR Daniel Orchard Hays, USN, and an anonymous review for their support and editorial assistance throughout the entire process. The author also thanks the Global Research Institute at William & Mary for financial support.

[1] Digital authoritarianism is commonly defined as the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations. This definition comes from "Exporting Digital Authoritarianism: The Russian and Chinese Models", by Alina Polyakova and Chris Meserole.
[2] I define surveillance-capable technology as any technology that collects data from users and that data could potentially be misappropriated by the state. This technology includes smart city systems, mobile payment applications, camera systems, telecommunications infrastructure, WIFI networks, etc.
[3] Alina Polyakova and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Brookings* (August, 2019).
[4] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 2.
[5] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 2.
[6] Adam Segal. "When China Rules the Web: Technology in the Service of the State." *Foreign Affairs* 97, no. 5 (September, 2018).
[7] "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." *Council on Foreign Relations* (September 26, 2019).
[8] Emily Dreyfuss. "The Internet Became Less Free in 2018. Can we Fight Back?" *Wired* (Dec 12, 2018).
[9] Arjun Kharpal. "Huawei Says it would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice." (March 4, 2019).
[10] Samantha Hoffman. "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." (October, 2019): 3.
[11] Samantha Hoffman. "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." (October, 2019): 12.
[12] Samantha Hoffman. "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." (October, 2019): 4-5.
[13] "China Accused of using Belt and Road Initiative for Spying." *Financial Times* (Aug 16, 2018).
[14] Kieron Monks. "Africans Face most Expensive Internet Charges in the World." (Oct 22, 2019).
[15] Tom Hancock and Yizhen Jia. "China Paid Record $22bn in Corporate Subsidies in 2018." *Financial Times* (May 28, 2019); Anil Gupta and Haiyan Wang. "How China's Government Helps and Hinders Innovation." (Nov 16, 2016); James L. Schoff and Asei Ito. "Competing with China on Technology and Innovation." *Carnegie Endowment for International Peace* (Oct 10, 2019).
[16] "How Will the Belt and Road Initiative Advance China's Interests?" *China Power* (Oct 18, 2019).
[17] Elsa B. Kania. "Why Doesn't the U.S. have its Own Huawei?" *Politico* (Feb 25, 2020); John Handel. "The 5G World: What People Care About." *Politico* (Feb 25, 2020).
[18] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright. "The Digital Dictators: How Technology Strengthens Autocracy." *Foreign Affairs* 2020, (March).
[19] Nicholas Wright. "How Artificial Intelligence Will Reshape the Global Order." *Foreign Affairs* (July 10, 2018).
[20] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 2.
[21] Paul Mozur, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State." *The New York Times,* April 24, 2019.
[22] Paul Mozur, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State." *The New York Times,* April 24, 2019.
[23] "How Will the Belt and Road Initiative Advance China's Interests?" *China Power* (Oct 18, 2019).
[24] James M. Dorsey. "Double-Edged Sword: China and Pakistan Link Up with Fiber-Optic Cable." *Eurasia Review* (July 19, 2018).
[25] Bradley Jardine. "China's Surveillance State has Eyes on Central Asia." *Foreign Policy* (Nov 15, 2019).
[26] Scott N. Romaniuk and Tobias Burgers. "How China's AI Technology Exports are Seeding Surveillance Societies Globally." *China Power* (Oct 18, 2018).
[27] Adrian Shahbaz. "The Rise of Digital Authoritarianism." *Freedom on the Net* (October, 2018): 8.
[28] Adrian Shahbaz. "The Rise of Digital Authoritarianism." *Freedom on the Net* (October, 2018): 9.
[29] Samuel Woodhams. "How China Exports Repression to Africa." *The Diplomat* (February 23, 2019).

[30] John Ikenberry. "The Rise of China and the Future of the West: Can the Liberal System Survive?" *Foreign Affairs* (January 2008).
[31] Nicholas Wright. "How Artificial Intelligence Will Reshape the Global Order." *Foreign Affairs* (July 10, 2018).
[32] Wesley Rahn. "Will China's 5G 'Digital Silk Road' Lead to an Authoritarian Future for the Internet?" *Deutsche Welle* (April 26, 2019).
[33] Amy Hawkins. "Beijing's Big Brother Tech Needs African Faces." *Foreign Policy* (July 24, 2018).
[34] Amy Hawkins. "Beijing's Big Brother Tech Needs African Faces." *Foreign Policy* (July 24, 2018).
[35] Bojan Pancevski. "U.S. Officials Say Huawei can Covertly Access Telecom Networks." *The Wall Street Journal,* Feb 12, 2020.
[36] Frank Fang. "US Department of Homeland Security Warns about Threats Posed by Chinese Drones." *The Epoch Times,* May 22, 2019; Neil Vigdor. "U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning." *The New York Times,* Jan 4, 2020.
[37] Andrew Grotto and Martin Schallbruch. "The Great Anti-China Tech Alliance." *Foreign Policy* (Sept 16, 2019).
[38] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 9.
[39] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. "Mapping China's Tech Giants." *Australian Strategic Policy Institute* (April 18, 2019): 7.
[40] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. "Mapping China's Tech Giants." *Australian Strategic Policy Institute* (April 18, 2019): 7.
[41] Arjun Kharpal. "Huawei Says it would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice." (March 4, 2019).
[42] Bradley Jardine. "China's Surveillance State has Eyes on Central Asia." *Foreign Policy* (Nov 15, 2019).
[43] Bradley Jardine. "China's Surveillance State has Eyes on Central Asia." *Foreign Policy* (Nov 15, 2019).
[44] "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts." *Council on Foreign Relations* (Mar 7, 2018).
[45] Danielle Cave. "The African Union Headquarters Hack and Australia's 5G Network." *Australian Strategic Policy Institute* (Jul 13, 2018); Salem Solomon. "After Allegations of Spying, African Union Renews Huawei Alliance." *Voice of America* (June 7, 2019).
[46] Keith Johnson and Elias Groll. "The Improbable Rise of Huawei." *Foreign Policy* (April 3, 2019).
[47] Steven Feldstein. "China is Exporting AI Surveillance Technology to Countries Around the World." *Newsweek* (April 23, 2019).
[48] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 14.
[49] Paul Mozur, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State." *The New York Times,* April 24, 2019.
[50] Joe Parkinson, Nicholas Bariyo, and Josh Chin. "Huawei Technicians Helped African Governments Spy on Political Opponents." *The Wall Street Journal* (Aug 15, 2019).
[51] Joe Parkinson, Nicholas Bariyo, and Josh Chin. "Huawei Technicians Helped African Governments Spy on Political Opponents." *The Wall Street Journal* (Aug 15, 2019).
[52] Joe Parkinson, Nicholas Bariyo, and Josh Chin. "Huawei Technicians Helped African Governments Spy on Political Opponents." *The Wall Street Journal* (Aug 15, 2019).
[53] Angus Berwick. "How ZTE Helps Venezuela Create China-Style Social Control." *Reuters* (Nov 14, 2018).
[54] Angus Berwick. "How ZTE Helps Venezuela Create China-Style Social Control." *Reuters* (Nov 14, 2018).
[55] Adrian Shahbaz. "The Rise of Digital Authoritarianism." *Freedom on the Net* (October, 2018).
[56] "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." *Council on Foreign Relations* (September 26, 2019).
[57] "Do Chinese Suppliers Set the Competitive Landscape for Video Cameras?" *Memoori* (July 24, 2017).
[58] Ferry Grijpink, Alexandre Ménard, Halldor Sigurdsson, and Nemanja Vucevic. "The Road to 5G: The Inevitable Growth of Infrastructure Cost." *McKinsey & Company* (February, 2018).
[59] Mark Sweney. "Huawei Ruling Will Cost Us £500m, Says BT." *The Guardian* (Jan 30, 2020).
[60] "How Will the Belt and Road Initiative Advance China's Interests?" *China Power* (Oct 18, 2019); Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. "Mapping China's Tech Giants." *Australian Strategic Policy Institute* (April 18, 2019): 10.
[61] John Hurley, Scott Morris, and Gailyn Portelance. "Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective." *Center for Global Development* (March, 2018).

[62]John Hurley, Scott Morris, and Gailyn Portelance. "Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective." *Center for Global Development* (March, 2018).
[63] Samantha Hoffman. "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." (October, 2019): 7.
[64] Merriden Varrall. "Behind the News: Inside China Global Television Network."*Lowy Institute* (January 16, 2020).
[65] Richard Fontaine and Kara Frederick. "The Autocrat's New Tool Kit." *Wall Street Journal* (March 15, 2019).
[66] Richard Fontaine and Kara Frederick. "The Autocrat's New Tool Kit." *Wall Street Journal* (March 15, 2019).
[67] James M. Dorsey. "Double-Edged Sword: China and Pakistan Link Up with Fiber-Optic Cable." *Eurasia Review* (July 19, 2018); James M. Dorsey. "One Belt, One Road: A Plan for Chinese Dominance and Authoritarianism." (May 18, 2017).
[68] Andrew Chatzky and James McBride. "China's Massive Belt and Road Initiative." *Council on Foreign Relations* (Jan 28, 2020).
[69] Aubrey Hruby. "In Africa, China is the News." *Foreign Policy* (Aug 13, 2019).
[70] Jenni Marsh. "How China is Slowly Expanding its Power in Africa, One TV Set at a Time." (July 24, 2019).
[71] Aubrey Hruby. "In Africa, China is the News." *Foreign Policy* (Aug 13, 2019).
[72] Celine Sui. "China Wants State Media to Peddle its 'Soft Power' in Africa, but Tech Platforms are a Better Bet." *Quartz Africa* (Oct 29, 2019).
[73] Celine Sui. "China Wants State Media to Peddle its 'Soft Power' in Africa, but Tech Platforms are a Better Bet." *Quartz Africa* (Oct 29, 2019).
[74] Paul Mozur. "Live From America's Capital, A TV Station Run by China's Communist Party." *The New York Times* (February 28, 2019).
[75] Jenni Marsh. "How China is Slowly Expanding its Power in Africa, One TV Set at a Time." (July 24, 2019).
[76] "The Overlooked Military Implications of the 5G Debate." *Council on Foreign Relations* (April 25, 2019).
[77] "The Overlooked Military Implications of the 5G Debate." *Council on Foreign Relations* (April 25, 2019).
[78] "National Security Implications of Fifth Generation (5G) Mobile Technologies." *Congressional Research Service* (Feb 24, 2020).
[79] "The Overlooked Military Implications of the 5G Debate." *Council on Foreign Relations* (April 25, 2019).
[80] "Gen. Joseph Votel, Gen. Thomas Waldhauser, and Acting ASD for International Security Affairs Kathryn Wheelbarger at HASC Hearing on U.S. Military Activities in Middle East and Africa." *United States Africa Command* (March 11, 2019).
[81] Justin Sherman. "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" *Council on Foreign Relations* (Oct 30, 2019).
[82] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. "Mapping China's Tech Giants." *Australian Strategic Policy Institute* (April 18, 2019): 8.
[83] Amy Mackinnon. "For Africa, Chinese-Built Internet is Better than no Internet at All." *Foreign Policy* (March 19, 2019).
[84] Justin Sherman and Mark Raymond. "The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom." *The Washington Post* (Dec 4, 2019).
[85] Justin Sherman and Mark Raymond. "The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom." *The Washington Post* (Dec 4, 2019).
[86] Andrew Grotto and Martin Schallbruch. "The Great Anti-China Tech Alliance." *Foreign Policy* (Sept 16, 2019).
[87] Nicholas Wright. "How Artificial Intelligence Will Reshape the Global Order." *Foreign Affairs* (July 10, 2018).
[88] Adrian Shahbaz and Allie Funk. "Freedom on the Net." *Freedom House* (2019): 1; "Freedom in the World 2019: Democracy in Retreat." *Freedom House* (2019).
[89] Robert Morgus, Jocelyn Woolbright, and Justin Sherman. "The Digital Deciders: How a Group of often Overlooked Countries could Hold the Keys to the Future of the Global Internet." *New America* (October 23, 2018).
[90] Robert Morgus, Jocelyn Woolbright, and Justin Sherman. "The Digital Deciders: How a Group of often Overlooked Countries could Hold the Keys to the Future of the Global Internet." *New America* (October 23, 2018).
[91] Adrian Shahbaz and Allie Funk. "Freedom on the Net." *Freedom House* (2019): 9; Robert Morgus, Jocelyn Woolbright, and Justin Sherman. "The Digital Deciders: How a Group of often Overlooked Countries could Hold the Keys to the Future of the Global Internet." *New America* (October 23, 2018).
[92] For example, the controversial Aadhaar national database has centralized biometric information on over 1 billion Indians, which the government has used to strip minorities of their voting rights, welfare benefits, and citizenship. Guatam Bhatia. "India's Growing Surveillance State: New Technologies Threaten Freedoms in the World's Largest Democracy." *Foreign Affairs* (Feb 19, 2020).

[93] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 10.
[94] Alina Polyakova and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Brookings* (August, 2019): 11.
[95] Helen Dixon. "Regulate to Liberate: Can Europe Save the Internet?" *Foreign Affairs* (Oct, 2018).
[96] Rebecca Mackinnon. "Internet Freedom Starts at Home: The United States Needs to Practice what it Preaches Online." *Foreign Policy* (April 3, 2012).
[97] Elsa B. Kania. "Why Doesn't the U.S. have its Own Huawei?" *Politico* (Feb 25, 2020).
[98] John Handel. "The 5G World: What People Care About." *Politico* (Feb 25, 2020).
[99] Amrita Khalid. "Loon's Autonomous Balloons are Bringing the Internet to Rural Peru." *Quartz* (Nov 21, 2019).
[100] Amrita Khalid. "Loon's Autonomous Balloons are Bringing the Internet to Rural Peru." *Quartz* (Nov 21, 2019).
[101] SpaceX's Starlink satellite network successfully launched its first sixty satellites in late May of 2019. Since then, "a second batch of satellites [were launched into orbit] in November 2019," followed by "a third in January 2020." Elon Musk "expects to begin broadband internet service by the end of 2020," and has plans to continue launching satellites. SpaceX has been granted permission by the U.S. Federal Communications Commission to launch 12,000 satellites, and potentially up to 30,000 satellites in the future. Currently, "only about 2,000 artificial satellites" are orbiting Earth, "and only 9,000 have ever been launched in all of history." Musk's plans for SpaceX's Starlink satellite network could connect the globe in an unprecedented measure, paving a new future for internet freedom. Adam Mann. "Starlink: SpaceX's Satellite Internet Project." (Jan 17, 2020).
[102] "Emergency VPN: Fighting Internet Censorship in Authoritarian Regimes." *NordVPN* (June 17, 2019).
[103] "National Security Senators Introduce Bipartisan Legislation to Develop 5G Alternatives to Huawei." (Jan 14, 2020).https://www.warner.senate.gov/public/index.cfm/2020/1/national-security-senators-introduce-bipartisan-legislation-to-develop-5g-alternatives-to-huawei
[104] "About SBIR." https://www.sbir.gov/about/about-sbir.
[105] About STTR." https://www.sbir.gov/about/about-sttr.
[106] "DARPA Urban Challenge." (2007). https://archive.darpa.mil/grandchallenge/.
[107] Tom Wheeler. "Moving from 'Secret Sauce' to Open Standards for 5G." *Brookings* (Feb 18, 2020).
[108] Bob Davis and Drew FitzGerald. "U.S. Pushing Effort to Develop 5G Alternative to Huawei." *Wall Street Journal* (Feb 4, 2020).
[109] Bob Davis and Drew FitzGerald. "U.S. Pushing Effort to Develop 5G Alternative to Huawei." *Wall Street Journal* (Feb 4, 2020).
[110] Drew FitzGerald. "Senators Urge $1 Billion Plan to Loosen China's Grip on 5G." *Wall Street Journal* (Jan 14, 2020).
[111] "The Status of Open Source for 5G." (February, 2019). https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_White_Paper_The_Status_of_Open_Source_for_5G_Feb_2019.pdf
[112] "Advancing Digital Connectivity in the Indo-Pacific Region ." *USAID*. https://www.usaid.gov/sites/default/files/documents/1861/USAID_DCCP_Fact_Sheet_080719f.pdf
[113] Naazeen Barma, Brent Durbin, and Andrea Kendall-Taylor. "Digital Authoritarianism: Finding our Way Out of the Darkness." *War on the Rocks* (Feb 10, 2020).
[114] The Wassenaar Arrangement is an arms-control agreement meant to regulate the export of dual-use technology. The United States, Russia, and Japan are all part of the 41 members . However, China is not a member of the Wassenaar Arrangement; Robert Morgus and Justin Sherman. "How U.S. Surveillance Technology is Propping Up Authoritarian Regimes." *The Washington Post* (Jan 17, 2019).
[115] Robert Morgus and Justin Sherman. "How U.S. Surveillance Technology is Propping Up Authoritarian Regimes." *The Washington Post* (Jan 17, 2019).
[116] Steven Feldstein. "The Global Expansion of AI Surveillance ." *Carnegie Endowment for International Peace* (September, 2019): 2.
[117] "U.S. Relations with Zimbabwe: Bilateral Relations Fact Sheet." *U.S. Department of State* (Jan 17, 2020). https://www.state.gov/u-s-relations-with-zimbabwe/;"Citizen's Budget: A Citizen's Guide to the 2019 National Budget." *Parliament of Zimbabwe* (2019). https://www.unicef.org/zimbabwe/media/1931/file/CITIZEN'S%20GUIDE%20TO%20THE%202019%20BUDGET.pdf