CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

July 27, 2021

China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road

Recorded Future®

This report profiles the growth of China's global digital presence and influence through state-sponsored development of digital infrastructure in foreign countries, cyber espionage enablement, and the export of Chinese surveillance technology. This examination weighs the privacy and security risks associated with Beijing's growing global influence through programs such as the Digital Silk Road Initiative. Data sources include the Recorded Future Platform, academic papers, government reports, and common open-source tools. The report will be of most interest to democratic governments, strategic decision-makers in developing regions such as Latin America, Africa, and South Asia, cyber defense groups, and corporations hosting data in developing regions. Analysis cut-off date: June 22, 2021.

Executive Summary

Through the Digital Silk Road Initiative (DSR), announced in 2015, the People's Republic of China (PRC) is building an expansive global data infrastructure and exporting surveillance technologies to dictators and illiberal regimes throughout the developing world, in some cases trading technology for access to sensitive user data and facial recognition intelligence. Domestically, China uses this type of technology to assert authority over its citizens, censor the media, quell protests, and systematically oppress religious minorities. Now, over 80 countries are enabled to do the same with Chinese surveillance technology.

Many developing countries are vulnerable to the exploitation of their data by corporations and powerful governments due to a lack of direct experience in cyber defense and an eagerness to catch up with competitors through rapid digitalization. The 8 case studies in this report serve as examples from Africa, Latin America, and Southwest Asia. This report explores 3 primary concerns related to China's digital colonialism:

1. China's DSR projects in the least developed regions of the world create a power imbalance between China and the recipient nations, resulting in a high risk for privacy and cybersecurity in those regions.
2. China's export of intrusive artificial intelligence (AI)-enabled technologies and ideologies to illiberal regimes around the world enables authoritarianism and systemic oppression and degrades democratic values.
3. Chinese digital dominance poses both a critical cybersecurity threat to the world and a growing threat to competitors' markets through the assertion of new Chinese-style standards of internet governance.

Digital dominance benefits the Chinese government in several ways. By building out and controlling access to data infrastructure in foreign countries, China is establishing new footholds for the flows of information from new markets. And by hosting foreign companies and government information in data centers, the Chinese government has access to valuable intelligence and intellectual property (IP) if unchecked by the host country. Additionally, China is actively developing exploits for the global internet of things (IoT), giving them an additional layer of access to individual and societal behavior data.

As China builds new global internet infrastructure through the Digital Silk Road, it will co-opt billions of new IoT devices, servers, and foreign resources to its cyber arsenal. We posit that Beijing will conduct extensive influence operations in conjunction with the development of Chinese-style internet governance in participating Belt and Road Initiative (BRI) countries. If left unchecked by both the rest of the world, China will reshape internet governance by replacing democratic values and standards with authoritarian principles.

Key Judgments

China's digital colonialism is a growing threat to democratic values, human rights, and national autonomy, especially in developing regions of the world such as Latin America and Africa.

The export of Chinese digital surveillance technology to developing and security-vulnerable countries poses a critical privacy risk to citizens and businesses alike.

China's development of internet infrastructure in foreign countries opens avenues for Chinese intelligence services abroad and poses a growing risk for cyber espionage intrusion campaigns.

China's growing presence and influence in the developing world will pose challenges for democratic institutions and markets as it co-opts new alliances through coercion and manipulation.

China's intelligence services have unprecedented access to foreign user data and vulnerability research through its fused civil-military research ecosystem. China's dominance in the IoT market ensures continued access to this data, which can be exploited and developed for multiple purposes.

The CCP will increase influence operations and espionage operations globally as the 2022 Winter Olympics in Beijing nears. Its focus will be on modeling the benefits of a surveillance state, crushing pro-democracy movements, and managing the messaging around its minority human rights violations in Xinjiang, Hong Kong, and Tibet.

Background

China's global digital dominance is developing through a program called the Digital Silk Road Initiative (DSR), part of the more widely known Belt and Road Initiative (BRI). Launched in 2015, the DSR is a private-sector agenda that aims to extend China's digital presence abroad, enhancing its commercial and political influence. The DSR receives heavy support from the state. In its initial stages, Chinese companies have answered demands for digital infrastructure and connectivity in Asia, Africa, and Latin America. Data centers, underwater and underground fiber-optic cable, telecommunications networks, smart education, cloud storage, and online surveillance have been constructed, creating a backbone for the flow of data to and from developing regions.

Mirroring its own internal internet controls, China is promoting strict global internet regulation by reinventing the internet, enabling nation-states to take control, and replacing the free, open, and decentralized internet infrastructure that has contributed to shaping the digital experience. In September 2019, Huawei engineers proposed the "New IP [internet protocol] Plan" to delegates from over 40 countries. Suggesting the current internet as outdated and limited, the engineers presented the new plan: a top-down design, enabling nation-states to more efficiently police their digital property and populations.

The CCP advocates for "cyber sovereignty" (网络主权), the supreme right to govern its own internet, and maintains rigid control over the operation and use of its online infrastructure, its internet-connected devices, and the online behavior of its citizens. President Xi Jinping is attempting to revolutionize international norms and institutions to accommodate the Chinese model of authoritarian governance while insulating itself from global accountability.

Beijing divides the world into friends and enemies. Inside China, friends[1] are those who "uphold the leadership of the [Communist Party] and the socialist cause" through support for its policy agenda. Outside China, the party's friends are "foreigners of influence and/or power who assist China's interests". Those who publicly question how it chooses to exercise power are labeled enemies, whether they are inside China or abroad. The party has developed[2] a sophisticated set of tools and a body of doctrine to maintain unchallenged power by "uniting friends" and "isolating enemies".

This divide-and-conquer strategy not only rewards friends for their support but coerces the party's enemies. Within China, coercive tactics include extralegal detention, limits on public speech, tight control of media messaging and key sectors of the economy, and manipulation of elites by "establishing personal and professional costs for opposing the party". Outside of China, Beijing uses state-sponsored actors to interfere in its enemies' foreign elections, recruit foreign agents for espionage, and disseminate disinformation to isolate its competition.

Publicly, Chinese companies like Huawei claim it would never turn over user data to Beijing. However, the Cybersecurity Law of the People's Republic of China, enacted in 2016, dictates that local data be stored and provided to the state on demand. When Beijing identifies intelligence gaps that they cannot fill with data mined domestically, they covertly fill these gaps through cyber espionage operations. Although espionage is a common nation-state tactic to inform military and policy decisions, Beijing feeds stolen corporate data and intellectual property to Chinese companies as well. Its national "Made in China 2025[3]" (MiC2025) plan, which aims to transform China from a producer of low-cost goods into a high-tech powerhouse, likely feeds collection requirements into its intelligence community. Financial damages from Chinese IP theft are estimated to be as high as $540 billion per year. The US Director of National Intelligence (ODNI) calculated that the US alone is losing approximately $400 billion annually to cyber theft, of which approximately 73% is attributed to Chinese-linked espionage.

Technological development plays a leading role in determining power in our world today. According to the International Telecommunication Union (ITU), globally, only 55% of households have an internet connection. In the developed world, 87% of households are connected, compared with 47% in developing nations and just 19% in the least developed countries. These least developed and developing nations are at a significant technological disadvantage and vulnerability to digital colonialism, defined as "the use of digital technology for political, economic, and social domination of another nation or territory".

[1] http://www.cppcc.gov.cn/zxww/2018/12/27/ARTI1545876942660350.shtml
[2] http://cpc.people.com.cn/GB/64162/64171/65717/65720/4461190.html
[3] http://english.www.gov.cn/2016special/madeinchina2025/

Figure 1: DSR IT infrastructure projects as of December 2018 (Source: International Institute for Strategic Studies)

It encompasses the digitizing of indigenous data without fully informed consent, the theft or exploitation of data, and the use of digital tools for influence and power over a subject.

Many transnational technology organizations are expanding internet access to the least developed countries, which provides opportunities for economic growth as well as access to healthcare, education, and jobs. However, if done in a way that provides unparalleled benefits and power to the offering party, the process begins to mimic colonialistic behavior of centuries past, creating a digital welfare state. In these circumstances, the colonizer incentivizes poor or indigenous populations with goods and services while imposing their values, ideologies, and norms of behavior, as well as extracting and exploiting their personal data. China is fast becoming a "digital dictator", exploiting foreign data for profit and corporate gain.

China's Rise to Global Power

China currently boasts the second largest economy in the world in terms of gross domestic product (GDP), with a GDP of over $13.4 trillion, trailing only behind the US's GDP of $20.49 trillion. When applying purchasing power parity, factoring in the cost of living and inflation differences, China ranks number one, a far cry from where it was just 50 years ago. Its military power ranks third behind the US and Russia by one measure of wartime capabilities and receives a generous 2021 budget of $209.16 billion. With the world's largest population at over 1.4 billion people, China has significant human capital through which to pursue its government's objectives.

Since opening to foreign trade and investment in 1979, China has been one of the fastest growing economies, a pace that the World Bank acknowledged as "the fastest sustained expansion by a major economy in history". The CCP enjoys political singularity and direction, aiming all of its resources at continued growth, sovereignty, and influence. Furthermore, Beijing invests significant resources into overt and covert influence operations, both domestically and abroad to protect its reputation and build support for single-party authoritarianism.

China creates its own rules and pursues its objectives with little regard for democratic values, global standards, or accountability. Its pursuit of national rejuvenation has created fast success through forced technology transfer, stealing proprietary information through cyber espionage, limiting access to its domestic market, and providing state support to its homegrown private sector "champions".

The Digital Silk Road Initiative

China's DSR project, which falls under Beijing's broader BRI, aims to create next-generation digital connectivity across the globe, including through terrestrial and underwater data cables, 5G cellular networks, data storage centers, surveillance networks, and the launch of global satellite navigation systems.

DSR-branded infrastructure projects are an avenue for Beijing to increase its influence in emerging economies and developing countries as well as an opportunity for domestic technology companies such as Huawei, Alibaba, and Tencent to expand their global business. Through the DSR, China also provides economic aid, political support, and other welfare to recipient states.

Since the DSR's rollout in 2015, China-based companies that initially globalized for purposes of profit have slowly been incorporated into DSR projects. Beijing invests billions of dollars of resources to help its domestic tech champions achieve commercial success overseas and is increasingly supporting the buildout of digital infrastructures such as fiber-optic cable, 5G infrastructure, satellite data, device production, and application-layer software.

By strengthening other countries' reliance on Chinese infrastructure and tools, Beijing gains a valuable mechanism for local political influence. Although this method of exploitation is not exclusive to China, Beijing's disregard for international norms, its increasingly aggressive foreign policy, and its lack of transparency raises concerns for the future of global freedom.

Technology Empowering Authoritarian Regimes

Social media-fueled protests have become the most significant challenge for 21st-century authoritarian regimes. Coups unseated around 9% of the dictatorships that fell between 2001 and 2017. Mass movements led to the collapse of twice as many governments. In addition to movements like the Arab Spring, social media-fueled protests led to the end of dictatorships in Burkina Faso, Georgia, and Kyrgyzstan. The CCP also faces domestic challenges such as pro-democracy movements and criticism from human rights defenders. To counter these threats to its authority, Beijing uses surveillance technology to track the movements and behavior of its citizens, has implemented a social credit system to encourage citizens to conform to laws, and uses surveillance data to identify and apprehend dissenters, journalists, and protesters.

Armed with both experience and tools to counter anti-government activists, China demonstrates to the world how new technology can be harnessed to control populations, manipulate outcomes, and shift power. Government access to vast networks of surveillance cameras, mobile and IoT devices, and private servers is a critical threat to privacy. China has stepped in to offer inexpensive, comprehensive technology packages to nations and regimes that otherwise would not be able to afford them. Furthermore, China teaches governments how to censor, surveil, and manage the data that is collected. In 2020, only 43% of the least developed countries had established data and privacy protection legislation. The security knowledge gap between the seller (China) and the buyer (recipient government) creates a dynamic that unknowingly leaves the buyer in a vulnerable security posture. Selling this type of technology creates a win-win for China: they get access to private data overseas and enable like-minded governments with powerful technical tools, thereby developing important alliances.

Foreign Footholds for Cyber Espionage

China is employing both its private and public sectors to facilitate its vision for a new internet and a world more friendly to its preferences and policies. Cyber espionage operations have been attributed to Chinese state-sponsored threat actors as far back as 2006 and have increased in volume and severity since. These groups have been discovered in hundreds of foreign networks, stealing diverse intellectual properties such as diplomatic plans, medical data, and military technology. We have uncovered several Chinese state-sponsored threat activity groups, including RedDelta, RedEcho, and RedFoxtrot, conducting targeted intrusions against foreign governments and religious organizations.

According to Chinese officials, over 6,000 Chinese enterprises and over 10,000 Chinese technology products have penetrated overseas markets. As China builds new global internet infrastructure through the DSR, it will co-opt billions of new IoT devices, servers, and foreign resources to its cyber arsenal, increasing its global stature, market domination, and cyber-military superiority. This growth will create new avenues and opportunities for cyber intrusions and espionage campaigns.

Digital Infrastructure Projects in Undeveloped Countries

Chinese companies such as China Telecom, China Unicom, China Mobile, GDS, and 21Vianet dominate the data center market, together making up 15.4% of the global market share. The Chinese data center industry is enjoying dramatic growth as a result of a few key factors, including state support through the BRI, DSR, and Made in China 2025 plans; foreign demand for inexpensive goods; a strategic focus on undeveloped regions; and oftentimes coercion to adopt China's technology. These factors have fueled China's own economic and military growth.

China's greatest tech champion, Huawei, is the leading seller of 5G technology and smartphones despite the US decision to ban Huawei technology due to security concerns. Huawei signed a $175 million "smart city" contract with Kenya, a cloud data center contract with Pakistan, and a 4G high-speed wireless internet contract with Canada. In February 2020, Thailand launched Huawei's first 5G testbed in Southeast Asia. In April 2019, Huawei

launched its Cloud and AI Innovation Lab in Singapore, intended to align with its "Smart Nation" Initiative.

In 2012, the US House Intelligence Committee labeled Huawei a national security threat and warned that it had stolen intellectual property through backdoors that allowed unauthorized access to sensitive data. US concerns center around the Chinese Cybersecurity Law that the government can use to subpoena sensitive or proprietary customer data from Chinese corporations. Other concerns include the fear of hidden backdoors in Huawei technology, which could subsequently be used to attack US internet infrastructure. In 2019, the US Department of Commerce added Huawei to its "Entity List", restricting it from conducting business with US partners.

Recently, nations such as Australia, Great Britain, and Japan have heeded cybersecurity and espionage warnings from the US, banning Huawei from building their 5G networks. However, many developing countries have opted into expansive DSR contracts with Chinese technology companies in trade for inexpensive internet and trade deals. The following case studies outline security threats developing countries have faced due to DSR deals with China and how Chinese surveillance technology is further enabling pervasive privacy concerns.

Case Study 1: African Union

In January 2017, computer scientists at the African Union (AU) headquarters' IT center in Addis Ababa, Ethiopia, discovered massive amounts of local data being transferred to unfamiliar servers in Shanghai, China every day between 12 AM and 2 AM local time. The AU headquarters building and data center was donated as "China's gift to the friends of Africa" in 2012. The computer systems were delivered turnkey, but with 2 digital backdoors, created by design to allow the free flow of AU's proprietary communications and production data directly to China. This event created a breach of trust between the 2 parties. Although it was quietly resolved at the highest levels of the AU, it also represented a turning point for IT security in the African Union. After the Chinese engineers were dismissed from their roles with the AU, the AU acquired its own new servers and declined China's offer to configure them.

Figure 2: The African Union Conference Center and Office Complex (AUCC), the headquarters of the African Union, in Addis Ababa, Ethiopia

The AU's data traffic was routed through Ethio Telecom, the sole public operator in Ethiopia at that time. Ethio Telecom, a state-owned Ethiopian firm, is also notorious for its cyber surveillance and electronic espionage technology, provided by the Chinese company ZTE. Ethio monitors and controls communications, providing intelligence to the government to silence dissenters, conduct interrogations, target foreign diplomats, and spy on domestic phone calls without warrants.

In July 2017, during the AU's 29th Summit, security inspectors also discovered the conference rooms bugged with microphones, suspected to be Chinese devices, under desks and in the walls. When confronted with this information, AU authorities remarked that this was the cost of being "supported [in] the independence struggle on the continent and [being] helped economically".

Case Study 2: Papua New Guinea

In 2018, Huawei built a data center for the government of Papua New Guinea that was later discovered to be critically vulnerable to cyber espionage by design. A report prepared by Australia's Department of Foreign Affairs on behalf of Papua New Guinea's National Cyber Security Centre detailed multiple security failures, including outdated encryption software and firewalls and insufficient firewall coverage on core switches, meaning remote access by hackers would be undetected. The $53 million data center, sponsored by the Chinese government, was meant to host all of Papua New Guinea's government data, but most departments did not shift to the new center due to a lack of funding for maintenance.

To resolve these issues, Papua New Guinea turned to Australia for financial assistance. When the Australian government investigated the architecture of the data center and commissioned the report, it concluded that a full rebuild would be required to comply with industry standards and requirements, something Huawei adamantly denied. The report also stated that it was a "deliberate effort by Huawei to deploy lax cybersecurity". Australia spent $200 million and took actions to block Huawei from accessing submarine data cables they laid between Papua New Guinea and the Solomon Islands as well as Australia. Huawei has since sold its majority stake in those cables to China-based Hengtong Group, Inc.

With limited cybersecurity training and no counterespionage capabilities, entities like the African Union and Papua New Guinea are at critical risk of compromise, accepting "digital welfare" from China but lacking the ability to sufficiently detect security vulnerabilities designed into its hardware and software.

Telecommunications Projects in Undeveloped Countries

Chinese officials view the construction of next-generation telecommunications infrastructure as critical to gaining a role in internet governance discussion on the global stage. The greater the role that Chinese companies play in the development of fiber optic systems and mobile communications, the greater the role they will have in setting standards for the world. China has also promoted its concept of internet sovereignty among BRI participants by teaching strict data governance, restrictive laws, and oppressive control.

Huawei has a presence in over 170 countries. The majority of current cellular infrastructure in Africa was also built by Huawei. Starting in the 1990s, when 2G and 3G networks were built, Huawei laid the foundation for future technology at steeply discounted prices. Backed by Chinese government loans, Huawei subsidized IT infrastructure throughout Africa, answering demands for more affordable and more available telecommunications infrastructure.

Beijing has positioned itself to dominate technology in all emerging markets, including Latin America, Africa, and the Indo-Pacific. Latin America is an important battleground in which Chinese companies are building infrastructure and setting technological standards. China initially focused on extractive sectors and non-digital infrastructure projects, including the Belt and Road Initiative, which Beijing extended to Latin America in 2017. However, Chinese technology companies such as ZTE and Huawei also made important breakthroughs in the region. Huawei saw a 21.3% increase in revenue from its Latin America operations in its initial year operating in the region. Much of that growth can be attributed to the company's development of telecommunication infrastructure in countries like Mexico, Venezuela, and Brazil. From 2002 to 2018, 62% of China's commercial engagement was through mergers and acquisitions, obtaining energy, telecommunications, and infrastructure.

As of 2019, Huawei was operating in 20 Latin American countries and dominates as the third top cell phone provider in Mexico, Colombia, Peru, and Central America. Earlier this year, chief of US Southern Command Admiral Craig Faller warned Congress that China was conducting "medical diplomacy" to leverage its vaccine supply to negotiate the entry of Huawei 5G and IT infrastructure into Latin American markets.

Case Study 3: Brazil

In January 2021, Brazilian president Jair Bolsonaro agreed to allow Huawei to bid on building out a 5G network in the country after initially opposing it just months prior. Previously, US president Donald Trump pressured President Bolsonaro to oppose the adoption of Huawei's 5G technology in Brazil, but Bolsonaro faced resistance from both industry and his own government, which may have influenced his decision to allow Huawei to make a bid. Of note, China is currently Brazil's largest trading partner, giving China significant influence in decisions related to industry partnerships in the country. Huawei has been present in Brazil for 22 years and has already conducted 5G tests with all the wireless companies in Brazil.

Huawei has been expanding its digital influence in Brazil, opening an internet-of-things lab in the state of São Paulo in partnership with the Institute of Technology, a research entity founded in 2003 and accredited by the Ministry of Science, Technology, Innovation, and Communication. Huawei also supports an internet-of-things center with Telefónica and a separate partnership with the Pontifical Catholic University of Rio Grande do Sul on a smart public lighting system.

Case Study 4: Uruguay

In August 2019, the Uruguayan government signed a memorandum of understanding with Huawei to deepen cooperation on emerging technologies, such as 5G networks, artificial intelligence, the internet of things, and cloud computing. The bilateral agreement also expands cooperation in agriculture, clean energy, communications, mining, manufacturing, and finance through the Belt and Road Initiative. Former Uruguayan president Tabaré Vázquez developed a strong political alliance with Chinese President Xi Jinping while he was in office and had, since 2016, offered explicit support to the One-China policy and backed China's reunification with Taiwan. President Vázquez also stressed that Uruguay was ready to play a leading

role in advancing Latin America-China relations and "enhance coordination on international and regional issues". Uruguay will likely play an important role in influencing other Latin American governments toward cooperation with China.

Access to the Global Internet of Things

China poses a grave threat to global privacy and security as its state-sponsored surveillance apparatuses are accessing internet-of-things (IoT) data well in excess of accepted international norms. According to a study by global market research firm International Data Corporation (IDC), the Chinese IoT market will reach $300 billion by 2024, putting it ahead of all competition. No other government in the world has this level of IoT market domination and access to the IoT data of foreign consumers. The collection and exploitation of IoT data is regarded by the CCP as an economic and technological "strategic high ground". The data is fed into a fused civil-military research ecosystem involving PRC intelligence and military actors who will have access to breakthroughs in IoT vulnerability research. Additionally, China's increased effort to influence and set international IoT standards is a critical part of its ambitious state-directed plan to achieve dominance in the IoT industry.

Chinese companies can access IoT data in 5 main ways:

1. At the user level, Chinese companies can access user data simply from sales and use of their IoT products, including abusive terms of service and usage agreements.
2. Device-level access through device manufacturing and design vulnerabilities and backdoors open up opportunities for outside entities to collect information at scale.
3. At the corporate level, Chinese companies can acquire foreign IoT companies and the data they have accumulated through their products, or buy foreign data through a third-party vendor.
4. The Chinese government can subpoena private data at will from foreign businesses (in China) through its Cybersecurity Law.
5. Collection of user data, human behavior, and device information from Chinese-made applications used worldwide, including social media, games, IoT firmware, and business software.

Unauthorized access to IoT devices has already resulted in physical consequences, including attacks on industrial machinery and power grids around the world. The widespread use of Chinese IoT devices and components suggests that the aggregate negative consequences of unauthorized access to Chinese devices may be proportionally larger than for devices from other countries. For example, the 2016 Mirai botnet attack was largely enabled by vulnerable devices produced by Chinese manufacturer Hangzhou Xiongmai Technology. The company acknowledged that its DVR and internet-connected cameras were created with weak default passwords and security vulnerabilities.

Digital Repression and the Export of Surveillance Technologies

The world is facing a deepening recession in democratic freedom for the 15th consecutive year. In 2020, the COVID-19 pandemic, economic and physical insecurity, and violent conflict shifted the international balance away from democratic values and in favor of tyranny. Last year, nearly 75% of the world's population resided in a country that faced deterioration of freedom. China and Russia both strengthened anti-democratic narratives and used the COVID pandemic to criticize the handling of the disease by democratic nations. Beijing countered criticism of its handling of the COVID-19 outbreak with an intense global disinformation campaign and domestic censorship. Authoritarian regimes around the world are evolving to embrace the internet, social media, and AI to counter their greatest threat — mass anti-government protests. At least 18 countries are currently using Chinese surveillance and censorship technology, and more than 36 governments have held Chinese-led training on "new media" or "information management".

China is exporting digital authoritarianism en masse to reinforce and enhance political repression under the guise of building "safe cities" projects that use tracking devices, video cameras, and other surveillance technology to enhance law enforcement and military capabilities. This activity shows up predominantly in the Southern hemisphere, where adoption of authoritarian-style surveillance technologies in the name of public safety will create both repression of human rights and privacy in those countries, and vulnerability of personal data to Chinese interception and exploitation. In Africa, for example, China is implementing facial recognition technology and using the data to advance its capabilities on dark-skinned individuals.

While this advancement may serve to improve recognition of individual faces of all different colors and shapes, human rights groups point out that Chinese surveillance companies are programming the technology to recognize and categorize groups of minorities for purposes of monitoring, detaining, and repression. These groups, called "sensitive peoples" by Chinese technology company CloudWalk, include the Uyghur Muslim population of Xinjiang, of which the CCP is conducting systematic and widespread human rights violations.

This confluence of factors, including the availability of this technology to repressive regimes, the established use of this surveillance technology for repression of minority groups, and the advancements in grouping individuals by appearance, has serious implications for minorities and repressed peoples around the world.

Africa

Chinese companies are aggressively targeting African markets with facial recognition surveillance technology under the guise of promoting "safe cities". However, the push into African societies is concerning because China aims to advance facial recognition capabilities on dark-skinned individuals. According to Human Rights Commissioner Edward Santow, facial recognition technology is less accurate when used on people with darker skin and presents challenges in diverse societies as dark-skinned individuals could be excessively targeted or excluded from surveillance activities. More accurate differentiation between dark-skinned faces has led to increased political targeting of individuals within African countries and could lead to increased racist persecution around the world. The Chinese technology influence in Africa involves several companies:

- Chinese telecom giant ZTE provides the infrastructure for the Ethiopian government to monitor its citizens' communications.
- Huawei employees embedded in Zambian cybersecurity teams intercepted encrypted communications and used cell data to track political opponents.
- In 2015, Hikvision opened an office in Johannesburg. Hikvision, a leading provider of surveillance cameras, is based in Hangzhou, Xinjiang, the heart of the persecuted Uyghur population. Hikvision technology is notorious for being vulnerable to cyberattacks.

As of January 2021, 41 African countries have signed memorandums of understanding to join China's Belt and Road Initiative. Of those, 13 have acquired advanced surveillance capabilities, and 9 of those — Botswana, Côte d'Ivoire, Ghana, Kenya, Mauritius, Morocco, South Africa, Uganda, and Zambia — are implementing "safe city" systems, all produced by Huawei.

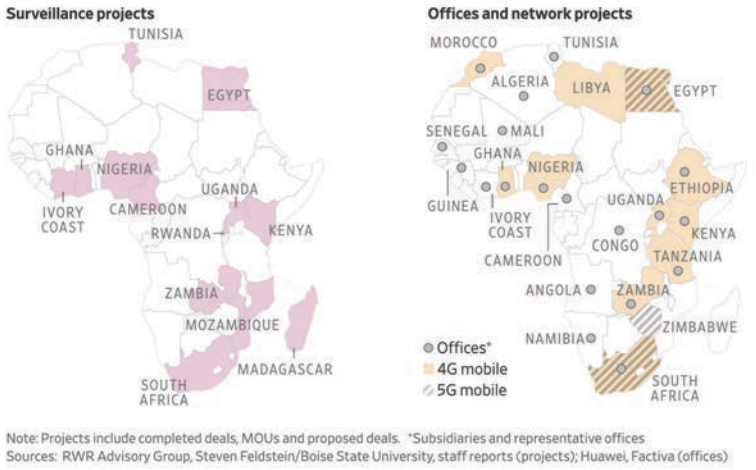


Figure 3: Huawei projects in Africa, 2019 (Source: Wall Street Journal)

In Africa, 5 countries are direct beneficiaries of Digital Silk Road investments totaling $8.43 billion: Angola, Ethiopia, Nigeria, Zambia, and Zimbabwe. The following case studies serve as examples of how Chinese surveillance technology is enabling authoritarianism, human rights violations, and diminishing democratic values throughout the developing world.

Case Study 5: Uganda

In 2018, Uganda's President Yoweri Museveni ordered his cyber-surveillance intelligence unit to intercept encrypted online communications and cell phone calls of a "popstar turned political opponent" named Bobi Wine. According to an investigation by the Wall Street Journal, when the regime's intelligence agents tried for days to hack Wine's WhatsApp and Skype accounts and failed, they requested assistance from Huawei, the top digital supplier in Uganda. Within 2 days, the Huawei engineers were allegedly able to successfully breach Wine's WhatsApp account using spyware. Museveni's regime then used the access to sabotage the opponent's political rallies and arrest Wine and hundreds of his supporters.

Figure 4: Huawei headquarters in Kampala, Uganda (Source: Wall Street Journal)

Beijing has been conducting the same activity domestically to monitor, censor, and control its own population for decades through its "Great Firewall" and state-sponsored "law enforcement" programs. According to the investigation, Huawei employees not only played a direct role in government efforts to intercept the private communications of opponents, but they also encouraged Ugandan security officials to travel to Algeria so they could study Huawei's "intelligent video surveillance system" operating in the capital city of Algiers. Uganda later agreed to spend $126 million on a similar facial recognition surveillance system from Huawei.

Case Study 6: Zimbabwe

In March 2018, the government of Zimbabwe agreed to a strategic partnership with Guangzhou-based CloudWalk Technology to develop facial recognition programs in the country. As part of the deal, Zimbabwe agreed to share all facial recognition data from its local databases to CloudWalk for further analysis. Yao Zhiqiang, strategic director of CloudWalk's research and development center, expressed that "in order to make a breakthrough with [facial recognition] technology, deep learning needs to be exploited", referring to the AI gaps in analyzing dark-skinned faces.

Surveillance tools such as CCTV, AI projects, and facial recognition are also transforming Zimbabwe's ability to track citizens, political opponents, monitor dissent, counter-protests, and consolidate political control. However, Zimbabwe's government remains under targeted sanctions from the US, meaning there are reputational and legal risks for western companies attempting to sell sensitive digital equipment to its government. CloudWalk has stepped in to fill that void, directly supporting an oppressive government that willingly and violently subdues its population. The deal is built on a long relationship between former President Robert Mugabe's regime, considered an ideological ally by Beijing. In 2016, Mugabe publicly expressed his desire to emulate Chinese-style social media censorship. The current president, Emmerson Mnangagwa, took office after a 2017 military coup ousted Mugabe after 37 years of repressive rule, but activists are skeptical of any significant progress being made on the human rights front.

Latin America

Case Study 7: Venezuela

In 2008, Venezuelan president Hugo Chávez sent a Justice Department envoy to Shenzhen, China to explore the Chinese social credit system and its national ID card system. During their visit, they were taken to the headquarters of Chinese telecom giant ZTE Corp., where they learned how China was developing a system to track social, political, and economic behavior through a national ID card. President Chávez expressed immediate interest in the idea but opted to use a Cuban firm to make millions of ID cards for $172 million. When the Venezuelan delegation's technical advisor, Anthony Daquin, later expressed concerns over privacy overreach to the Venezuelan government, he was detained, beaten, and extorted by Venezuelan intelligence agents, prompting him to flee the country.

In 2017, with the Maduro regime in power, Venezuela contracted with ZTE on a $70 million government effort to build a national ID card, payment system, and "fatherland database" to track individuals' transactions, personal information, and social media accounts. Now, a team of ZTE employees is embedded in a special unit at Cantv, the Venezuelan state telecommunications company that manages the database, which is housed on ZTE servers. Information retained on Venezuelan citizens through the system includes PII such as dates of birth, family information, employment and income, property owned, medical history, state welfare benefits received, presence on social media, membership of a political party, and voter history.

Figure 5: Venezuelan president Nicolas Maduro holding a fatherland ID card (Source: ABC News)

Since the project was initiated, President Maduro has upgraded to a larger version of the system, aiming to add 30,000 cameras and payment applications. Su Qingfeng, the head of ZTE's Venezuela unit, confirmed that it has sold the Venezuelan government servers to host the system's data and to host new Chinese mobile payment applications.

Despite protests from concerned citizens and human rights activists, the program is being mandated across the country. The government requires citizens to enroll in order to receive public benefits including health care and pension payments, leaving the poorest populations vulnerable to data collection and exploitation.

In 2016, the US Department of Justice determined that ZTE violated its sanctions on Iran by selling American "controlled items" to the country as part of a surveillance technology package used to monitor its citizens. As a result, a settlement was made between the Chinese corporation and the US government: pay a $1 billion penalty, put $400 million in escrow with an American bank, overhaul its leadership, and allow a team of compliance monitors to be installed inside the company for 10 years.

On November 30, 2020, the US Department of the Treasury added the Chinese surveillance company China National Electronics Import and Export Corporation (CEIEC) to its list of Specially Designated Nationals and Blocked Persons for its role in supporting the "illegitimate Maduro regime" and "undermining democracy in Venezuela". The US Treasury stated that CEIEC provided "software, training, and technical expertise to Venezuela[n] government entities, which was then used against the people of Venezuela". The press release detailed that CEIEC has enabled Maduro through technology and training to repress political dissent, conduct malicious cyber efforts since 2017, censor independent media, and manipulate votes by censoring social media.

Case Study 8: Ecuador's ECU-911

In February 2011, Ecuador signed a deal with Chinese tech giants CEIEC and Huawei to install an extensive surveillance system financed by Chinese loans. Inspired by the 2008 Beijing Olympics, Ecuador purchased over 4,300 surveillance cameras to collect footage of citizens and transmit it to intelligence services, calling the project ECU-911. The surveillance project includes capabilities to monitor emails and phone calls, as well as to bug vehicles with hidden microphones. In order to help facilitate the rollout of ECU-911, Beijing sent military attachés from the embassy in Quito to assist in the installation and setup of the equipment.

In exchange for ECU-911, Ecuador agreed to provide one of its main exports, oil, to China. However, the deal quickly became a point of concern for the Ecuadorian government. In exchange for the technology that totaled more than $19 billion, Ecuador signed away large portions of its oil reserves, leaving the country in debt to China and in a vulnerable position economically. Following this deal, Chinese infrastructure projects in the country increased, including the construction of a hydroelectric dam and oil refineries to maximize outputs demanded by China.

Outlook

China is playing a direct role in the expansion of authoritarian rule around the world. With global democracy in decline for the 15th consecutive year, it will become increasingly important for the free world to counter China's influence in the developing world. Illiberal and hybrid regimes throughout Asia, the Middle East, Africa, and Latin America will invest in the next generation of Chinese-style autocratic technologies to enable population control, surveillance, and censorship. The authoritarian tools that Beijing is selling will continue to spread around the globe if liberal democracies do not cooperate better with developing nations and present a cost-effective alternative.

Beijing will continue to dominate the construction and management of telecommunications, data, finance, and IoT. Furthermore, they will continue to push new technical standards for the next generation of the internet and will leverage their political and economic influence over "friends" to gain this power. Established political alliances between China and BRI partner countries such as Uruguay, Zimbabwe, and Venezuela will likely play a part in strengthening partnerships between respective neighboring countries and China.

As the world's democratic leaders and the G7 step up to this challenge with plans such as the Build Back Better World (B3W) initiative, we expect Beijing to increase their efforts proportionally, using the entire autocratic toolkit to influence, coerce, and sponsor the adoption of Chinese technology and ideology throughout the world. As Beijing gains access to new markets and human-driven AI data, it will also improve its capabilities for influence operations in those societies, drawing them closer to China and encouraging a push away from the US and its allies. China is set to host the 2022 Winter Olympics in Beijing and will likely use the event as a platform to display the effectiveness of its domestic surveillance and policing. Leading up to the Olympics, China will likely crack down on pro-democracy protests and will ramp up its control of the Muslim minority population — and the way the media portrays it.

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cybercriminals — individuals and groups — from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

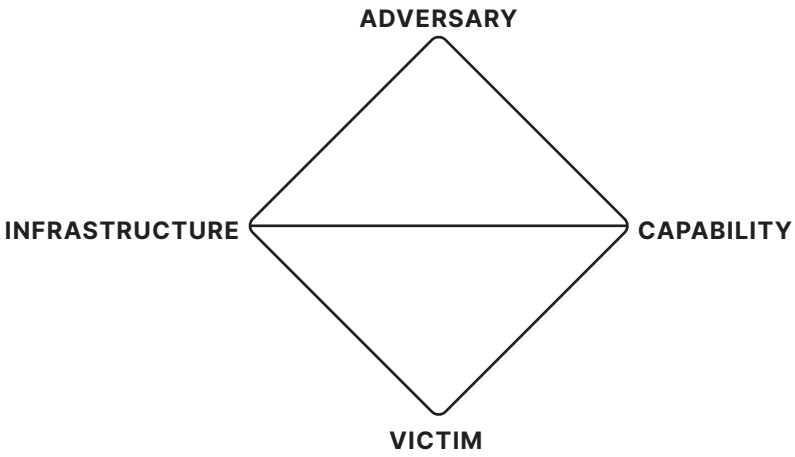
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-21 where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group. We tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely used or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.